

**BUSINES-TO-CONSUMER ELECTRONIC COMMERCE  
SURVEY OF STATUS AND ISSUES**

**ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT**

**Paris**

**64201**

**Document complet disponible sur OLIS dans son format d'origine**

**Complete document available on OLIS in its original format**

**Copyright OECD, 1997**

**Applications for permission to reproduce or translate all or part of this material should be made to:**

**Head of Publications Services, OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France**

## TABLE OF CONTENTS

INTRODUCTION .....	4
I. THE EMERGING MARKET IN ELECTRONIC COMMERCE .....	5
The nature of electronic commerce .....	5
Current status and prospects .....	7
Key aspects of the electronic commerce market .....	11
Conclusion .....	12
II. ISSUES SURROUNDING ELECTRONIC COMMERCE.....	14
Conducting business-to-consumer electronic commerce .....	14
The key issues .....	17
Current status and prospects .....	38
CONCLUSION.....	44
A closer look at the economic impact.....	44
Industry-specific issues .....	45
General issues .....	45

### Tables

Table 1. Electronic commerce overview .....	46
Table 2. Electronic commerce market forecasts1 .....	46
Table 3. Emerging industry sectors .....	47
Table 4. Reasons for using Web sites .....	50
Table 5. Future use of Internet .....	50
Table 6. Internet user profil .....	51
Table 7 Households with PC/modem and growth of the WWW .....	52
Table 8. Issues involving electronic commerce .....	53
Table 9. Various payment methods .....	54
Table 10. Characteristics of the various payment systems .....	55

### Figures

Figure 1. Growth in commercial Web sites .....	47
Figure 2. Distribution of monthly sales generated by Web sites .....	48
Figure 3. Profitability of Internet commerce activities .....	49

## **INTRODUCTION**

Electronic commerce between businesses and consumers is rapidly developing into a major economic activity. It may create new market opportunities not only in information and communications industries but in almost all industries involving commercial transactions with consumers. However, this raises many questions about existing forms of economic activity. In the light of rapid developments in technology and industry activities in the private sector, various groups of experts are currently discussing a number of issues concerning electronic commerce. Given the diversity of concerns expressed, an overall view of the issues would appear useful. This paper thus seeks to survey and analyse the issues in the various areas of concern regarding electronic commerce between businesses and consumers.

On the basis of information gathered as of late 1996, the first part looks at the economic potential and the prospects for electronic commerce; the market potential, the nature of the market, and issues related to industry activities are described. The second part looks at institutional issues that are becoming important for commercial transactions on open global electronics networks, notably the Internet. It covers information, also available as of late 1996, on issues, views and actions.

This report has been declassified by the Committee for Information, Computer and Communications Policy (ICCP).

## I. THE EMERGING MARKET IN ELECTRONIC COMMERCE

This section discusses the potential of electronic commerce and surveys the start-up market environment for both merchants and consumers. Particular attention is paid to business-to-consumer categories and to electronic commerce activities on Internet.

### **The nature of electronic commerce**

#### *Overview*

Electronic commerce is not new, and it involves various types of transactions conducted over electronic networks. As Table 1 shows, electronic commerce can be categorised by the types of parties involved and the nature of the networks over which the transactions are made.

Business entities use various types of electronic transactions, especially over proprietary networks. Bank-to-bank fund transfers, such as bank point-of-sale (POS) or automatic clearing house (ACH) transfers, or certain business transactions, such as electronic data interchange (EDI), are examples. Proprietary networks are managed exclusively for the designated participants or members and for the specific purposes which they have defined among themselves.

Transactions between business entities and consumers are also possible. Various on-line shopping services are already available on proprietary networks such as America Online, CompuServe, or Minitel. In these cases also, transactions are conducted according to a pre-arranged manner among members who join the network and agree to those arrangements or terms of transactions.

An emerging category of electronic commerce involves electronic transactions over the open network, such as the Internet, between parties that do not necessarily know one another in advance or have agreed to certain arrangements. On the open network, technologies such as the World Wide Web (WWW) make it possible to conduct both business-to-business and business-to-consumer transactions.

In the following sections, discussion will focus on this emerging category and particularly on business-to-consumer transactions over the Internet in light of its growth potential and its impact on economic activities and society. Following a brief review of the nature of the Internet, the discussion turns to market dynamics and the possible impact of electronic commerce.

#### *The Internet*

Using the Internet as a transaction network for electronic commerce provides at least a few benefits for all participants in commercial transactions. One is the lower cost of network transactions as compared to other network services. Owing to the Internet's rapid growth, the cost of access and use has been dropping. A major cost to Internet users is fees to the service providers that provide connectivity,

but these have been decreasing. Also, because of technological developments, the network can transmit, fairly easily and without significant additional cost, not only text but also other forms of information, such as pictures, sound, and video, both to and from users. For the transmission of various forms of electronic information to and from users -- typically needed for commercial exchanges -- Internet can be the most cost-effective option.

Another aspect of the Internet is its global coverage. Almost all countries can be accessed. One source estimates that, world-wide, over 90 million people can be reached through the Internet ([www.netree.com/netbin/internetstats](http://www.netree.com/netbin/internetstats)). Technically, home pages put up on the server in one country can be accessed and viewed from anywhere in the world. Thus, it is technically possible for a single Web site to make a commercial offer that is available throughout the world, and all consumers accessing that site can, again technically, place orders for goods and services from their home or office PC, however distant the server being accessed. This implies that there are practically no country borders on the Internet.

The “open” nature of the Internet, which connects many different networks world-wide, technically enables consumers and merchants anywhere to conduct commercial transactions over the network. Theoretically, such transactions can be instantaneous. Because information concerning a transaction is transmitted and processed electronically, transactions can take place far faster than through the mails or other means of trading at a distance. Ordering, payment, and even, in the case of goods or services that can be transformed into digital electronic signals (software, information, music, and videos), delivery can be instantaneous. When used for commercial transactions, the nature of the Internet influences market dynamism.

### ***Changes in market dynamics and potential impact on industry***

As the Internet potentially gives both consumers and businesses world-wide access, an Internet marketplace would be more comprehensive than any marketplace in history. The relatively minor cost of establishing home pages that offer goods or services attracts both existing merchants and newcomers. Theoretically, anyone who opens or accesses a Web site can enter the market.

The benefits for both consumers and industries of conducting trade over the Internet may trigger dynamic market changes. Consumers can expect more choice, convenience, and probably cheaper prices. They can “search” Web sites that offer goods and services. Already, various search engines or directory services<sup>1</sup> are available to Internet users and help them find Web sites containing the information they seek among the more than 200 000 Web sites world-wide. Consumers can compare information from various commercial sites in order to find the offer that best fits their needs. Moreover, in terms of convenience, the Internet is accessible 24 hours a day, seven days a week and can be accessed from home or office. Finally, consumers may be able to group their purchases; this might give them greater negotiating power and allow them to deal more effectively with suppliers.

Merchants, for their part, gain direct access to consumers (see Box 1), thereby avoiding the need to go through various intermediaries to reach them. This may make it possible for them to avoid certain intermediary costs, such as distribution inventories and the maintaining of expensive retail shops. As already mentioned, entering the market is theoretically easy, and the way business is conducted will change as the organisational structures become more flexible.

### **Box 1. One-to-one marketing: Trends in marketing and selling**

To succeed in the intensely competitive global marketplace, marketing strategies are shifting to a new paradigm. From the 1950s to the 1980s, leading businesses in North America, Europe, and Asia made advances in mass production, mass communication, and mass distribution to establish world markets for their products and services. During the 1980s, mass marketers began using new technologies and analytical techniques to define targeted markets in order to reach the customer groups most likely to buy their products. The trend towards greater specialisation has continued, with many marketers using new tools for targeted marketing and new delivery media, such as direct mail and telemarketing.

The concept of one-to-one marketing is a marketing trend of the 1990s. It involves a systematic, interactive approach to developing and managing a detailed knowledge base that integrates individual customers' product and business requirements, personal preferences, and purchase histories with traditional demographic statistics. This information provides the foundation for businesses to offer customers individually tailored products, services, information, incentives, and transactions. By focusing on individual customers and one-to-one marketing, business managers seek to establish relationships with customers that maximise customer satisfaction, develop customer loyalty, and contain the high costs associated with acquiring new customers.

With the emergence of the Internet's World Wide Web, businesses have the opportunity to implement one-to-one marketing and selling on a mass basis. The proliferation of inexpensive, easy-to-use Web browsers and affordable Internet access services has made the Internet easy to navigate, accessible to millions of homes and businesses, and readily adaptable to a broad range of business, entertainment, education, commerce, and marketing applications. As Internet use has grown, industry experts have described Web sites as ideal places to develop individual customer relationships. Whether a Web site is designed primarily for delivering content, promoting a brand, or conducting transactions, it offers businesses an opportunity to extend front-office services directly into the homes and businesses of customers and to initiate and maintain an ongoing relationship on-line. By recognising the relationship-building potential of the Web -- in particular, its ability to capture Web site visitor profiles, observations, and feedback, and to micro-target useful information to visitors on the basis of this data -- business managers can use advanced Internet technologies to engage in personalised dialogues with millions of customers on a one-to-one basis.

*Source:* <http://www.hotwired.com/wired/4.03/features.html>, Don Peppers and Martha Rogers, "The One-to-One Future: Building Customer Relationships One Customer at a Time", Doubleday, 1993.

## **Current status and prospects**

### ***Market size and growth trends***

Currently, Internet commerce is quite small, representing at most about US\$ 500 million world-wide.<sup>2</sup> However, every source of market research forecasts significant growth in market size over the next three years. The most conservative forecasts expect growth of at least ten-fold for three to four years, and the most optimistic foresee about US\$ 780 billion in 2000 (Killen and Associates). The latter figure would represent about 10 per cent of the overall retail and wholesale market.

Distance trade in general, which includes mail orders, TV shopping, etc., is estimated to represent about US\$ 600 billion for 1994 and is expected to reach US\$ 2 150 billion in 2000. On the basis of the optimistic scenario, Internet commerce would account for more than 30 per cent of this market (Killen and Associates) (Table 2).

### ***Active market sectors***

A range of market sectors appear suitable for electronic commerce on the Internet. Based upon France's experience with Minitel services, travel services, information services, home banking, public services, and shopping are strong candidates. User surveys have already shown the potential of ticketing and travel services and trade in goods, including computer equipment, software and music CDs (Forrester Research, June 1995) (Table 3).

### ***Companies engaged in Internet commerce***

It is unclear how many firms are participating in Internet commerce, but there are indications that the number is already significant and growing fast. About 250 000 US corporations are estimated to be using Web sites for commercial purposes (*Nikkei Shimbun*, 7 October 1996), although they are not necessarily offering commercial transactions on their home pages; some are simply using them for public relations or advertising. A Massachusetts-based software firm, Open Market, has released a directory of registered commercial Web sites. The firms numbered over 47 000 as of late November 1996, and were increasing by 800 to 900 a week (Figure 1).

According to Active Media, 80 per cent of the commercial Web sites have monthly sales figures of less than US\$ 10 000, and many of these firms do not yet seem to be making money from electronic commerce.

An October 1996 Japanese survey (*Weekly Diamond Magazine*) indicates that 60 per cent of the 64 Japanese firms conducting electronic commerce on the Internet are not making a profit, as against 29 per cent that say they are. However, among those making a profit, some commented that this is because they regard the investment as almost nil, while others said that the revenue is too small to justify hiring a person full-time. (Figure 2 & 3). The survey indicates some of the reasons. One is the mismatch between consumer profiles and the products offered. Women appear to be poorly represented among Internet users, and this is considered a problem for market expansion since most shopping is usually done by women. Also, the cost of publicising a Web site address, for example in magazines or other media, is quite high. On the positive side, there were no claims of problems with transactions.

### ***User and consumer profiles***

Accurately describing Internet users is difficult. Because of its dynamic growth and the absence of a central management organisation, it is almost impossible to give a complete picture of Internet users. As mentioned above, estimations suggest, however, an Internet population of 90 million people. One survey indicates that the number of users grew at a rate of around 50 per cent per half year in 1996 and that Internet Web sites are becoming a fast-growing marketplace for commercial transactions (Commerce Net/Nielsen Internet Demographics Survey).



“Selling and purchasing” are already recognised as major activities of the World Wide Web. According to a recent US survey, 30 per cent of Internet users use the WWW to purchase products, and 16 per cent to sell products (Commerce Net/ Nielsen Internet Demographic Survey of August 1995 and March 1996 -- [http://www.commerce.net/work/pilot/nielsen\\_96/exec.html](http://www.commerce.net/work/pilot/nielsen_96/exec.html)). According to Project 2000 (and based on the August 1995 Commerce Net/ Nielsen Internet Demographic Survey), an estimated 1.51 million people have made a purchase using a Web site. The American Internet User Survey of November and December 1995 (FIND/SVP) indicates that 30 per cent of Internet users see “buying and selling” as a future value of the Internet (<http://etrq.findsvp.com/internet/highlights.html>) (Table 4 & 5).

In Japan, with an estimated over 7 million Internet users as of January 1997 (according to a survey by the Network Wizard Inc.<sup>3</sup>), awareness of electronic commerce is high among Internet users<sup>4</sup>, particularly distance sellers. A survey conducted by the Electronic Commerce Promotion Council (ECOM) of Japan on 4-6 September 1996 indicates strong interest in electronic commerce on the Internet among those with experience of direct marketing, 14 per cent of whom have already made purchases over the network. Among those interested in distance selling, 97 per cent expressed willingness to use on-line electronic media to purchase goods. Another survey done more recently by Infocom Research, Inc. in December 1996 indicates 39 per cent of Internet users already have experience in on-line shopping.

The profile of Internet users is still quite different from that of the general public. Owing to the rapid growth in the number of users, however, differences are becoming less marked. The typical Internet user is male, highly educated, with a relatively high income, significant computer experience, and a managerial or professional job. Many are married and have children. While this remains true for both Europe and the United States, the situation is changing. For example, in 1995, female Internet users accounted for 7 per cent in Europe and 10 per cent in the United States, but for 1996, the figures are 15.2 per cent and 34.2 per cent, respectively.<sup>5</sup> Educational and occupational backgrounds are becoming more diversified. The share of new US users with university degrees is 39 per cent, while it is 56 per cent among long-time users (Table 6).

Commercial use of the Internet for buying and selling is becoming more popular. New users are more interested in this aspect. Based upon 1996 US survey figures (Commerce Net/ Nielsen Internet Demographic Survey, March 1996), 75 per cent of users indicate that they use the Internet to obtain product information. Moreover, 30 per cent regard purchasing products as the reason for using Web sites, while 16 per cent indicate selling products. The populations that use Web sites for purchasing products grew to 87.5 per cent over a six-month period, and those using them to sell products grew to 118.2 per cent over the same period. These growth figures are significantly higher than those for growth in the overall user population in the same survey. The American Internet User Survey (FIND/SVP, November-December 1995) confirms that the future of the Internet lies in its commercial exploitation. It indicates that 30 per cent of users expect the Internet to be used for buying and selling and 39 per cent for advertising and marketing (see Table 4, 5 & 6).

### ***Price and cost trends***

Internet commerce may be able to achieve better market performance, for example by providing consumers with more choice and lower prices and merchants with lower costs for reaching consumers and supplying products (see Box 2). The potential benefits are different types of products. Since Internet commerce has just emerged, it is difficult to determine whether this is happening or not. Data and information reported so far indicate that such possibilities exist and there is some indication that they are being realised.

### **Box 2. Small and medium-sized Web enterprises**

A Web-site-based book seller called “Amazon.com” claims itself as the largest book seller on the Internet (or in the world). Its sales are estimated at US\$ 17 million, and its inventory is more than five times that of Barnes & Noble, a large chain of traditional booksellers. Because it does not need shops, clerks, or inventory and can take advantage of centralised inventory and purchasing, it discounts list prices by 10-30 per cent. Amazon’s sales are rising by 34 per cent a month, with hundreds of thousands of visitors to their Web site shop each day.

Another example, the Internet Shopping Network, founded in 1994, has become the largest virtual shopping mall on the Internet. In 1995, it became a division of the Home Shopping Network and now carries a selection of 35 000 computer hardware and software products from over 1 100 manufacturers.

Individual, Inc., founded in 1989, is a leading provider of personalised information services for hundreds of thousands of readers world-wide. Using its proprietary information retrieval, filtering, and delivery technologies, Individual provides customised news and information services for end-users, new electronic publishing outlets for its Information Partners, and relevant marketing opportunities for its advertisers. Individual’s news delivery services use Individual’s proprietary agent technology SMART to search, filter, and deliver a daily customised interactive news service based on over 700 information sources and 20 000 articles. In 1996 it earned US\$ 6.1 million and is growing at an annual pace of 39 per cent. Its clients numbered 425 000 at 30 September 1996.

*Source: Business Week, 23 September 1996; Fuji-Keizai, “Internet Electronic Commerce Service Business”, April 1996.*

In some cases, consumers can purchase at the best price, as a *Fortune* article on purchasing insurance policies and books has noted (“The Birth of Digital Commerce”, 9 December 1996). In terms of costs, some factors push prices down and others push them up. Among factors that push them down, at least four have been mentioned (for example, in the *Fortune* article cited above and in *Business Week*’s “Making Money on the Net”, 23 September 1996). First, as suppliers do not have to have or operate physical “shops” involving real estate, shop clerks, displays, etc., retailing costs can be significantly reduced. Second, merchants can access consumers without resorting to “middlemen” whose margins add costs to final prices. Third, by managing customer orders directly, they may be able to reduce inventory stocks in intermediate channels, while the electronic network can help locate products more efficiently.<sup>6</sup> Fourth, technology that allows consumers to “find” and “compare” offers made world-wide is now becoming available. In addition to search engines, so-called “intelligent agent software”, which automatically visits relevant Web sites, checks information, and selects the best offer, is beginning to be used.<sup>7</sup> Such software helps promote competition.

Other factors affect costs or prices of products or services. First, it is unclear what the cost of making sales will be. Merchants, intermediaries, and governments will be taking steps to deal with some of the issues discussed below, such as the protection of privacy and reduction of the risks of buying and selling on the Internet. Some of these measures will increase selling costs. Second, delivery costs to individual customers may not be negligible, especially for goods that must be physically transported from warehouses to consumers. Unlike traditional systems, where delivery costs are shared by many orders, individual handling of packaging, shipping and paperwork may result in higher delivery costs to customers. For international shipping, handling costs for customs clearance and other paperwork can add

additional cost. These and other costs will be important in determining where and to what extent electronic commerce will exert downward pressure on prices. Currently some on-line providers charge prices equal to those in traditional markets or even higher. It is unclear what this means. It could be that although their costs are for different inputs than those purchased by traditional sellers, their total costs are the same. Alternatively, if costs to electronic commerce merchants are lower, it may be that consumers are willing to pay a premium for the convenience of shopping on the Internet, and that there is not yet enough competition among sellers on the Internet to drive their prices down to their cost level. Until there is full competition among electronic commerce firms, as well as between electronic commerce and non-electronic commerce firms, the full benefit of electronic commerce will not be realised.

Price trends are an excellent indicator of overall market performance and dynamics, but when looking at price trends, it is necessary to hold quality constant, and in the distribution sector convenience is a major aspect of quality. It would be necessary to follow these trends in order to analyse the economic impact of electronic commerce.

### **Key aspects of the electronic commerce market**

The economics of electronic commerce is an important issue. It includes areas such as the accessibility of such markets for consumers and merchants, possible friction with existing trade practices and regulations, and the role of intermediaries. Policy questions involving specific industry regulations and competition policies may be arising.

#### ***Accessibility***

Is the market easy for consumers to access? Although the population with access to the WWW is growing rapidly, it still represents less than 20 per cent of the population of the major OECD countries, and the profile of this population is still quite different from that of the general public. Penetration of equipment and services has not yet reached a mature state, and new users may find using the Internet difficult. For many consumers, the barriers to Internet commerce may appear even greater. Increasing accessibility for consumers is an important factor for realising the potential benefits of electronic commerce.

For merchants, it is clear that putting up Web pages to open an Internet shop is significantly less costly than traditional retailing. Technically, of course, the Web can be accessed from all over the world through the Internet. However, to become known and make a profit requires promotion, and in this respect incumbents with well-known names and brands are in a better position than new entrants, who would need significant capital to advertise. Traditional media, such as magazines, newspapers, and TV, have advantages as advertising tools until more users have become more accustomed to using search engines or agent software, and these can greatly exceed the cost of setting up the Internet shop. Of course, new entrants are in some respects in a better position than incumbents, not only because of lower costs, but also because they may be better able to make quick changes in response to changes in consumer demand. Some new entrants will fail, others will be bought by large firms that want their "know-how", and others will become large firms. The low cost of entry and marketing in electronic commerce can be the source of the new competition.

### ***Customary practices and regulations***

Internet sellers must also consider the regulations and customary practices observed by their industry sectors. In some sectors, it is an established practice to use intermediaries, and direct selling to consumers will be a competitive threat to traditional intermediaries (retailers and wholesalers), as well as to producers with large investments in a traditional distribution system. In the United States, direct mail order selling prompted some traditional sellers to become more efficient, while others sought to prevent the new competition through the use of collusive action. Enforcement of competition law was necessary to permit the market to develop in an efficient manner. Similar possibilities exist in relation to the Internet. In Japan, alcoholic beverages, pharmaceutical products, and music CDs are areas where strong customary practices exist, and selling alcoholic beverages over the network might infringe regulations that control the retailing of alcoholic beverages (*Nikkei Shimbun*, 19 September, 1996). There is also some dispute, between the industry and the regulatory body, over whether existing regulations allow the sale of pharmaceutical products over the network. If CDs are allowed to maintain fixed prices, discount sales of music CDs also raise problems. Moreover, among countries or regions, practices and regulations may vary. The international nature of the Internet raises serious questions about their harmonisation and practical implementation.

### ***Intermediaries***

It has been argued that, in the absence of intermediaries, merchants would find it more difficult to access customers directly.<sup>8</sup> For electronic commerce, various intermediary functions are already being performed by search engines and agents, which help consumers find information on products or merchants. By selecting shops and products, Internet shopping malls could act as intermediaries by, in effect, endorsing the selected products and services and thus raising consumer confidence and offering support to merchants. Various payment schemes, including credit cards, also serve an intermediary function, as merchants accepted by major payment schemes are regarded as legitimate sellers and may be more readily accepted by consumers. Internet merchants also usually have to rely on third parties for delivery services. There will be various intermediary functions for Internet commerce, and acceptance by such intermediaries can be crucial to merchants seeking to operate on the Internet.

The emerging intermediary functions may therefore play an important role for competition in the Internet marketplace. Moreover, competition among intermediaries also influences the competitive nature of Internet commerce.

### **Conclusion**

Business-to-consumer electronic commerce has just emerged as a new marketplace with significant growth potential. Its economic impact may be far greater than its projected near-term market size. It will draw new entrants and enhance competition in various markets. Consumers' purchasing behaviour is likely to be drastically affected. Existing rules and customary practices in specific markets may require review and modification. In general, consumers can expect to see lower prices and better quality. The dynamics of electronic commerce may affect traditional markets in many ways.

These developments have extensive policy implications. Government regulations may need to be reviewed to ensure that unnecessary regulations are not impeding electronic commerce's contributions to consumers' welfare. To avoid constraining the development of this new market, it is important to monitor the market dynamics or the actual effects of electronic commerce carefully. Cross-border trade rules and regulations may also require attention. As a result, it is very important to undertake further research on market developments in electronic commerce.

## II. ISSUES SURROUNDING ELECTRONIC COMMERCE

While commercial activities already exist on the Internet, an environment for conducting business-to-consumer electronic commerce was not yet well developed as of late 1996. The environment for Internet transactions is different from shopping at department stores or through mail order or telephone. For both technical and institutional reasons, Internet transactions still carry some risk for both consumers and merchants. Uncertainties about government policies or jurisdictional rules may significantly affect the market environment.

This section first examines the electronic commerce transaction process and identifies the problems that must be addressed to provide a better environment. It then turns to the key issues for electronic commerce and discusses the current status of the technology, industry activities, and on-going debate. The key issues are: authentication, rules for establishing businesses and effective electronic contracts, handling of content, privacy, payment systems and electronic money, consumer protection, impact on taxation, and security.

### **Conducting business-to-consumer electronic commerce**

One way to identify the issues involved is to examine the steps in a commercial transaction over the network. First, to conduct a transaction, the business establishment must exist in cyberspace (step 1). Then, to sell its products or services, the company must make marketing efforts (step 2). Next or concurrently, goods or services are produced (step 3). When a customer shows interest, buyer and seller negotiate and make a contract (step 4). Then, payment and delivery take place (step 5). If something is wrong with the product or service, cancellation may occur (step 6). At some point, either afterwards or at the establishment of the business, taxes must be paid (step 7). In addition, various other issues arise that concern consumers, companies, or governments (Table 8).

### ***Establishing the business***

When establishing the business entity, for instance, the issue of trademarks may arise. While the Internet makes it possible for all Web sites to be connected to and viewed by Internet users world-wide, there are no well-established rules for protecting trademarks that appear on the sites. Trademarks or company names registered in one country may also be used in other countries. In the physical world, no conflict may occur, but on the Internet, a search engine would find both sites, and the companies concerned may enter into a dispute.

## ***Marketing***

Thanks to advanced information technology, marketing activities in cyberspace can be effective and massive. On the Internet, there are various ways to gain information on individuals, such as demographic information, buying patterns, and topical interests. For instance, it is technically possible to obtain an individual's record of visits to Web sites from access servers. With such information and interactive network functions such as e-mail, so-called "one-to-one" marketing is conceivable.

Such marketing may be more convenient for consumers and increase market efficiency. However, it may cause problems of protection of privacy if it is "excessive", and thus raise privacy issues.

## ***Production***

Most obviously in the case of digital publication, copyright can be a serious problem. Technically, the transfer of digital content from the original server to the end user's computer usually involves numerous copies. Various intermediate servers make mirror and proxy files, and end users browse the Web site. To do so, they technically copy information to their own computer's hard disk. It is questionable whether all these copies receive permission from the copyright holders.

Also, there is uncertainty about enforcement of intellectual property rights (IPR) in an environment where almost all countries are connected and transactions can take place. Not all countries have the same system of protection and enforcement of IPR, so that IPR protection can be a issue for companies.

An important issue is digital content that is considered harmful or illegal in some countries but can be legally put up on the Web site in others. Since a controversial Web site can be accessed worldwide, this raises the issue of the handling of such content.

## ***Negotiation and contracting***

When conducting a negotiation or making a contract, it is very important to identify both sides of the table. On the Internet, however, it is not easy at present to be certain that the Web site or e-mail correspondent really represents the name given. Technically, it is not very difficult to pretend to be someone else on the network. Unlike the physical world, the Internet does not yet have an established and widely used identification system. The authentication issue, i.e. finding legitimate merchants and legitimate consumers, can be a major problem for both buyers and sellers.

Also, there is some uncertainty about the effectiveness of electronic contracts. It is not easy to create a "physical" signature in an e-mail exchange on the network. Moreover, it is not clear whether e-mail can replace contract documents in all countries involved in electronic commerce.

### ***Payment***

Payment over the network can be very convenient for consumers and will stimulate electronic commerce. However, some technical problems must be overcome, and some institutional issues must be addressed. The system of payment must be widely available and used, and, economically, it must make sense to use it. The transactions must be secure. As in many cases in a digital environment, technology plays an important role in resolving difficult issues here.

It is technically possible to create a “cash” substitute for circulation in cyberspace. There are projects for developing and using such technology as a means of payment. Electronic money creation can theoretically affect monetary or financial policies of governments. Another issue is the danger that the development and circulation of such instruments might be used for money-laundering activities.

### ***Nullification or cancellation***

For cyberspace transactions, consumer protection policy is not yet established. When a consumer is dissatisfied with the products delivered, it is questionable whether in all cases money can be returned in exchange for the products. It is not yet clear whether the policy that applies for physical market transactions also applies for electronic transactions. Individual firms have the incentive and the ability to offer money-back guarantees, but it may be necessary for industry self-regulation and/or government regulation providing for rules on nullification, cancellation and cooling off applicable even to cross-border transactions may be necessary to ensure consumer confidence and realise healthy market growth.

In this respect, it is also necessary to clarify the liability of the bodies involved in transactions. Merchants, network service providers, payment system operators, and consumers may have to have rules for sharing responsibility in the case of damages due to the transactions.

### ***Payment of taxes***

The issue of calculating VAT for cyberspace transactions, for example, is complex. For instance, the consumer may be located in a European country but purchase from a company legally located in the United States, while the goods are located in another European country and the server that does the contract is in Asia. Who should collect and pay VAT? What rules should apply for income tax purposes?

Taxation rules on Internet transactions remain unclear. The business can be scattered over different countries and even change physical base frequently without notifying cyberspace customers. By their very nature, these transactions raise many issues about the application of existing rules of taxation, and clarifications is needed.

### ***Horizontal issues***

Other issues arise that affect the entire transaction. Protection of privacy and security are such issues.



Information on an individual can be produced and handled throughout the transaction process. Thus, it may be necessary to establish basic rules or principles concerning the protection of the individual's privacy. The intrusion of unwanted information into an individual's private space would need to be controlled. Information should be held confidential. An individual should have control over his/her information. These issues are examined below.

Security is also a fundamental issue. Technically, the system must be reliable, and, most fundamentally, the network infrastructure needs to be able to support very high growth in commercial transactions over the next several years. The system must also be technically able to protect against fraud and crime. The impact of electronic commerce on law enforcement and national security should be examined. Institutional agreements or rules such as liability sharing are also fundamental to the security of electronic commerce.

## **The key issues**

### *Authentication issues*

When one makes a purchase at a cybershop, one runs the risk of dishonest merchants. They may be trying to steal money or credit card numbers and may pretend to be well-known merchants that they are not. For their part, merchants need to know if the customers are legitimate. They may need to know whether the customer actually exists and is not pretending to be someone else. In some cases, merchants may need to know that they will not be selling goods, such as liquor, to minors or selling other products that required qualified purchasers. If the amounts of money involved are large, the merchant must avoid forgery or other problems. In these respects, authentication is the key issue. Efforts have been made to develop new technologies or services for authentication, and some are already commercially available. However, these efforts have only begun, and the issues are not solely technological.

This section describes the current status of authentication issues, which include: finding legitimate merchants, finding legitimate consumers, and preventing forgery. It also reviews current technological developments and new services, as well as concerns of various parties.

### *Current technologies and systems for providing authentication*

#### Technology trends

A cryptography technology based on a public key algorithm which was developed in the mid-1970s has recently become a focus of attention. Rather than sharing one secret key, this new design uses two keys: a "public key" that is disclosed to the public and used to encrypt data, and a corresponding "private key" that is kept secret and used to decrypt the data. An important application of public key cryptography is "digital signatures", which can be used to verify the integrity of data or the authenticity of the sender of the data. In this case, the private key is used to sign a message, while the corresponding public key is used to verify a signed message. Public key cryptography offers the benefit of confidential transmissions and digital signature in an open network environment in which parties do not know one another in advance.

Commercial activities that provide authentication services using public key technologies already exist. For example, Verisign, Inc. (<http://www.verisign.com>), in the United States has been working with telecommunication operators, credit card companies, and software companies to develop digital identification (ID) services. Digital IDs with various levels of security are being issued for use with e-mail, on-line transactions, or electronic banking involving large sums. The digital ID consists of the public key, an expiration date, documentation binding it to the user's organisation, and the digital signature of its issuer.

In April 1996, Union Credit in Japan, one of the top five Japanese credit card companies (founded by Fuji bank, Dai-ichi Kangyo Bank, Sakura Bank, etc.) established an authentication system using the SET protocol.<sup>9</sup> It is currently operating this service on a trial basis. This is the first authentication facility activated on the Internet for credit cards used for electronic commerce. Although companies such as Verisign have provided the technology<sup>10</sup>, they have not yet established a specific authentication facility for credit cards. Electronic commerce experiments are underway in France as well. They are based on the combination of the SET protocol and Smart Cards, hence offering a high level of security, in particular with regard to authentication. One of those experiments will rely on the European initiative C-SET (Interoperable Chip-Secured Electronic Transaction) project, currently undertaken within the framework of the programme "Information Society Initiatives in Standardization" of the European Commission.

First Virtual is another example of a commercial authentication service. It does not use public key technology. First Virtual was established in 1995 and started to provide credit-card authentication services for on-line purchases. This service only uses e-mail for confirming transactions to sellers and buyers. It works as follows. Users must become members by registering and furnishing the required information. When a member buys something from a member merchant, the merchant sends this information to First Virtual. On this basis, First Virtual sends a confirmation e-mail to the users, in order to ensure that they are the parties concerned and that the contract is that agreed upon by both parties. The service periodically reviews the transaction record and eliminates members who are the source of frequent complaints. By doing so, they seek to maintain the legitimacy of users and merchants. Payment transactions are forwarded periodically to credit card companies to settle accounts. Besides providing authentication services, First Virtual allows individuals to accept credit-card payment through First Virtual.

#### Initiatives for consumer education and protection

In addition to using the new technology, some industry associations take initiatives to raise consumer consciousness. Through Web sites, the Direct Marketing Association (DMA) in New York and the Japanese Direct Marketing Association (JADMA) in Tokyo draw attention to the importance of careful Internet trading procedures. They set guidelines for users (confirm the merchant's address, save the order forms, etc.), and provide a hot-line service. Magazines published in the field have been warning Internet users about the risks of forgery or data hacking, especially for payment, and the importance of verifying the legitimacy of merchants before making contracts. For example, *Impress's Internet Magazine*, Japan's largest magazine for Internet users, carries reports on on-line shopping in every issue. Off line, direct marketing associations authorise legitimate merchants, set guidelines for legitimate trading procedures, and operate the No Ads List database, which member merchants agree to use so that consumers who do not want their names on mailing lists will not receive advertisements through the mail. On-line business can be expected to develop the same kind of self-regulation.

In some countries, direct marketing industry associations regulate their industry, with the aim of ensuring its sound development, winning consumer confidence, and protecting against severe government regulations that might restrict fair business activities. Their guidelines generally include a code of ethics with rules for describing the quality of products or services, for fair pricing, and for appropriate trading procedures such as cancellation. They also define rules for protection of personal data, which are based on the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and related OECD documents. These associations generally have action lines (hot lines) for assisting consumers who have unresolved problems involving a direct marketing transaction. These associations have recently started discussions on direct marketing (or trading) via the Internet.

### **Box 3. Policy and the treatment of keys in cryptography**

Although cryptography can be used for authentication, some governments express concern about their use, for reasons of security and protection of privacy, among others. The following paragraphs present current policy issues involving the use of encryption technologies and the treatment of keys in cryptography technology.

In some cases, cryptography technology is closely linked to military technologies, and, in many countries, commercial applications or transactions involving cryptography technology are under government control. For instance, the US government controls the export of strong cryptographic products, such as public key cryptographic software using more than 56-bit key length; its permission must be obtained to export commercial cryptography products above a certain level of sophistication. Also, some European countries consider that commercial use of cryptography technology should be under governmental control. Cryptography policy guidelines have been discussed at the OECD since March 1996, and their establishment would help achieve the formulation of a co-ordinated policy among OECD countries. Some governments are proposing and considering key escrow systems or trusted third party systems as options for managing the commercial use of cryptography technologies to ensure public safety and national security.

#### **Key escrow systems**

A key escrow<sup>11</sup> cryptography system (or, simply escrowed cryptography system) is a cryptography system with a backup decryption capability which, under certain prescribed conditions, allows authorised persons (users, officers of an organisation, and government officials) to decrypt ciphertext with the help of information supplied by one or more trusted parties who hold special data recovery keys. These keys are not normally those used to encrypt and decrypt the data, but rather provide a means of determining the data encryption/decryption keys.<sup>12</sup>

#### **Key recovery system**

In July 1996, the US government announced that it would examine introduction of the key recovery system, by means of which a trusted party (in some cases, within the user's organisation) would recover the user's confidentiality key, for the user or for law enforcement officials acting under proper authority. Access to keys would be provided in accordance with destination country policies and bilateral understandings. No key length limits or algorithm restrictions would apply to exported key recovery products. Some software or hardware vendors, such as Trusted Information Systems, Inc., have already presented products for this system.

## Public key authentication framework

In July 1996, Standards Australia released a new draft standard for a public key authentication framework (PKAF) for Australia. Certification authorities will have to have acceptably strong evidence of identification in order to certify that a particular physical/legal person is identified with a particular public key. In Japan, MITI and MPT formed consortiums in 1996 with private sector entities, such as credit card companies, telecommunication companies, and so on to conduct experiments on an authentication centre using public key methods.

## Digital signature

In August 1996, the American Bar Association (ABA) issued digital signature guidelines. These discuss the need for a third party CA and indicate the requirements for the CA.<sup>13</sup> In Japan, the initiative to issue Certification Authority Operating Guidelines<sup>14</sup> was taken by ECOM, in April 1997. These guidelines are planned to provide the basic principles for issuers of digital certificates to operate the CA services.

### *Maintaining legitimacy through industrial and governmental effort*

In itself, cryptography technology does not necessarily guarantee the legitimacy of consumers and merchants. It can reduce the chances of someone pretending to be someone else, of forgery, or of obtaining private data, but it alone cannot prevent swindles or minor problems. Such problems may be more serious on the Internet, owing to the lack of physical constraints, such as postal or telephone costs, etc. Therefore, certain countermeasures should be considered.

For example, mechanisms should be available to prosecute illegitimate merchants or swindlers and disclose information about them to users (consumers and merchants), through hot lines, lists of cases, etc. In addition, guidelines for legitimate merchants should be set and means of authorisation established, as has been done for the mail order and telephone order (MOTO) industry in some countries through industry associations such as the direct marketing associations, as discussed above. Finally, it is important to encourage digital identification movements in order to avoid both major and minor problems.

Because consumers can easily contact foreign merchants on the Internet, and because merchants can locate their servers or business facilities anywhere, legitimacy problems can be world-wide in scale. In addition, as mentioned above, policies or guidelines may differ among countries or regions, so that such measures should be considered at international level. Management of “keys” for cryptography systems may also need to be considered at international level.

### *Rules for establishing businesses and effective electronic contracts*

Electronic commerce is conducted differently from traditional trade, and it is not clear whether or not traditional trade practices or systems can be applied effectively. Among the relevant issues are trademarks, the effectiveness of electronic contracts, and intellectual property rights (IPR).

### *Problems with trademark rights*

Domain names used to be simply identification names on the WWW servers. However, as electronic commerce and search engine technologies become popular, domain names have come to represent a corporate identity similar to existing trademarks. In each country or region, domain names are assigned by a third party: Inter NIC (Inter Network Information Center ) in the United States, RIPE NCC (Réseaux IP European Network Communication Centre) in Europe, and APNIC (Asia-Pacific Network Information Center) in the Asia-Pacific region are the major actors. Each tries to avoid overlapping domain names, but so far, no formal action has been taken to determine whether domain names resemble existing trademarks.

In the United States, lawsuits have arisen because domain names were used without the permission of the trademark owner. For example, the US Trademark Registration Law gives the registered trademark owner exclusive rights to use the trademark and prohibits others from using it. If someone starts a service using a domain name that resembles an existing trademark, the disputes concerning the application of trademark law arise. In early 1994, the Princeton Review, a famous test preparation firm, registered a domain name, kaplan.com. However, "Kaplan" is the Stanley H. Kaplan Educational Center, the Princeton Review's largest competitor, and the Princeton Review used the address in an advertisement which compared their services. Kaplan brought a lawsuit against Princeton Review for infringement of a registered trademark, false identification of source, as well as unfair advertisement, unfair competition, and deceptive trade practices. The conciliation result supported Kaplan's petition and ordered Princeton Review to give up the domain name (see MITI, "Issues to be examined concerning electronic commerce", August 1996).

In 1996, the International Telecommunications Union (ITU) and the World Intellectual Property Organisation (WIPO) began discussions on the registration process for assigning Internet domain names, as a way of dealing with trademark disputes. In June 1996, at an OECD conference held in Dublin, the current status of trademark issues was reported (<http://www.oecd.org/dsti/iccp/dublin.html>).

### *Issues surrounding the effectiveness of electronic contracts and the validity of electronic documents*

To permit consumers and merchants to take advantage of the potential benefits of contracting via the Internet, it may be necessary to examine or reconsider certain laws governing commerce. Questions have been raised, by governments and by experts, over whether electronic data can be used as evidence and whether electronic communications can be taken as official. Such questions are in addition to issues of digital signature or authentication, which are addressed elsewhere in this report.

One example related to the effectiveness of electronic contracts concerns rules on when and how contracts become enforceable when using electronic mail for acceptance of an offer. Whether the traditional "mailbox rule" (see Box 4) applies or not is not yet clear.

#### **Box 4. The mailbox rule**

Acceptance of an offer (or similar services) by mail creates a contract at the moment of dispatch, provided that the letter is properly addressed and stamped. Otherwise, the acceptance becomes effective when the letter is received by the offering party. This is known as the “mailbox rule”, and it applies only to acceptances. The rule has some limitations. For example, the offering party can explicitly state that acceptance will not become effective until it is received. Also, in the event that the offeree first sends a rejection and then sends an acceptance, whichever arrives first is determining. If the offeree sends an acceptance first and then a rejection, the acceptance is effective unless the offering party receives the rejection first and relies on it. At first blush, the mailbox rule may seem to be a little rule written by lawyers to ensure the need for their services. If the reasons behind the rule are examined, however, it seems to be a logical way to regulate such activities. The question of whether the mailbox rule applies to e-mail is one that the courts have not yet answered. Its applicability seems to depend on whether e-mail is deemed to be more like instantaneous communication than like traditional mail services. Unlike real time chat e-mail, however, it is probably not instantaneous in the sense of this rule.

*Source:* Edward A. Cavazos and Gavino Morin, *Cyberspace and the Law*, Chapter 3, “When Acceptance Becomes Effective: The Mailbox Rule, The Mailbox Rule Revisited, The E-mailbox Rule?”

Other issues include the validity of electronic documents. In some countries, specially enacted laws and regulations require persons involved in trade to submit certain documents subsequent to contracts to purchase or sell. For example, in Japan, as in many other countries, for instalment sales or door-to-door sales, written documents are required. For electronic contracts, however, electronic data might easily be altered, without leaving a trace. This issue is one that should be discussed along with that of the effectiveness of digital signatures. MITI has pointed out that electronic documents are generally valid for legal procedures, commercial transactions, and administrative requirements, but that there are cases where special laws or measures require written documents (MITI, “Issues to be Examined concerning Electronic Commerce”, August 1996). The MPT study group’s report has also pointed out the necessity for further study on the legal frameworks regarding the digital signatures and the Certification Authority (CA) services (“Cryptography Policy and Electronic Money”, April 1996). Following those reports, the ECOM of Japan, the industry consortium for electronic commerce, is working on developing a model contract in electronic commerce for both consumers and merchants<sup>15</sup>.

To avoid hindering commercial Internet activities, governments may need to review rules such as those requiring written documents. At present, some governments oblige companies to keep paper, not electronic, copies of contract information. However, they should look into the possibility of reducing the burden on merchants that such duplication involves, while giving attention to consumer protection and to technologies such as technologies for screening and saving electronic documents and authentication or identification of information on the network.

#### *Protection of IPR*

The Internet is dramatically changing the distribution of digital content products, which are sold in packages and can be directly distributed to users’ PCs through the network. Music “broadcast” on the Internet can be downloaded to users’ PCs and replayed. As mentioned in Section 1, the Internet is used for information gathering and software purchases. Consequently, the market for products with intellectual

property rights has significant growth opportunities. The many “radio stations” opened on the Internet in 1996 are an indication of this trend (see *Nikkei Multimedia*, 1996, No. 6). Most have contracts with the associations or companies that manage the copyrights, such as ASCAP and BMI (United States) and JASRAC (Japan). However, these new technologies and new commercial activities may increase the risk of illegal copying and in fact challenge the traditional notion of “copying”. The new treaties adopted at WIPO in December 1996 may help clarify the situation.

Also, an international initiative may be necessary to establish co-ordinated rules for treating legal aspects of electronic contracts or other legal documents, given the high potential for cross-border electronic commerce on the Internet. The initiative taken by the United Nations Commission on International Trade Law (UNCITRAL) for EDI constitutes an example of a successful initiative in this context.

### Copyright infringement

Digitalisation of content and the greater penetration of networking increase the risk of illegal copying, as consumers can make copies easily and pass them to others through the network. Copyright enforcement is becoming more and more difficult. This is an important issue that must be addressed.

Moreover, the traditional sense of “copy” raises other important issues. For example, it could be argued that the information that the browsing software brings up from the network onto the user’s PC is a “copy” of an original on the server, as technically it is. It could be argued that a “copy” is made when one downloads information from the original server to the mirror server or when one downloads sound or pictures from the Web site to the user’s PC to hear or see them. Such basic Internet activities could be interpreted as copyright infringement, as it is traditionally understood.

If all such activities are regarded as copyright infringement and if every such activity needs to obtain the copyright holder’s consent, this would be very difficult, at least at present, especially for non-music content, as handling copyrights for visual sources is generally quite complicated. In the digital publishing industry, the complexity of copyrights for visual sources and the high handling costs involved are a large concern for publishers of CD-ROMs. In many cases, though, these concerns may be largely theoretical, and examples do exist of established methods of obtaining consent and clearing permission for the use of copyrighted material working well. As the plethora of content available from a diversity of electronic publishers attests, new technological methods are being developed which facilitate the process.

### Initiatives addressing IPR issues

Initiatives have been taken by many groups to address these issues. Prime among these is the successful conclusion of two new treaties at the WIPO Diplomatic Conference in December 1996. Prompt ratification and implementation of these pacts by as many countries as possible may be the single most constructive step in ensuring a global environment for intellectual property rights, and the rapid and healthy development of electronic commerce. In July 1995, the European Commission issued a Green Paper on copyright and related rights in the Information Society. It is preparing to introduce Community legislation in proprietary areas, such as the legal regime applicable to digital transmissions and the scope of reproduction rights. It is also going to seek to establish appropriate minimum standards of protection at international level. In mid-1996, the Commission proposed to link the Community trademark registration system to WIPO’s international trademark system. This would enable European companies to make a single application to register their trademark both within the EU and in the non-EU countries that are members of the Madrid Protocol (“E-commerce over the Internet”, *EITO 1997 Yearbook*,

December 1996). The US Copyright Clearing Center set up the Electronic Rights Management Group to consider this problem. It will also follow closely the activities of the European Commission. Many initiatives from the technological point of view have been taken to protect intellectual property rights in the distribution of digital content over networks. In Japan, for instance, MITI has been supporting R&D in rights management technology to enable the greater distribution of content over networks and launched pilot projects on content distribution using rights management technology in the spring of 1997. In France, as well, a new system based on a single gateway, called SESAM, has been set up for the management of rights in the multimedia sector. In addition, technological initiatives spearheaded by the private sector -- for instance, the Digital Object Identifier initiative -- are aimed at facilitating voluntary licensing systems that copyright owners may choose to employ to manage access to their intellectual property in the networked environment more efficiently and at lower cost to consumers.

### *Handling content*

The Internet allows users to send and receive data easily from anywhere in the world, and this has greatly contributed to the progress of science and industry. However, it can make and has made information which some consider objectionable widely available: slanderous or malicious messages, controversial literature, pornography, and information that may be used by organised crime or terrorist groups. Such information can cause significant social problems, which are primarily dealt with in two ways, in addition to self-regulation by the industry: government regulation and user blocking. In the United States, for example, a law intended to regulate indecent information was ruled unconstitutional by the Supreme Court. Many Asian and European countries have pushed similar legal restrictions, but these offer little promise of solving the problem. The second approach relies on user-controlled filtering systems which block out information that users do not wish to see or that supervisors wish to keep from others.

This section first gives examples of such issues and governmental actions concerning the handling of content, then introduces technology developments and self regulation of controversial content, and concludes by discussing policy implications.

### *Governmental actions for handling of content*

Until 1996, this issue was not widely discussed except in countries such as Singapore or Islamic countries. In 1996, however, OECD countries took various actions aimed at regulating Internet content. These regulations have three general objectives:

- to protect public order and morality: for this purpose, some adult-oriented content or advertisements (for tobacco or alcohol, for example) which are considered inappropriate for all users have begun to be regulated;
- to protect human rights: for this purpose, guidelines or bills that forbid slander or attacks on specific individuals over the Internet have been set or proposed;
- to protect national security: for this purpose, there are discussions on regulating content that encourages or accelerates terrorism or discrimination.

More specifically, in 1996, the German government directed CompuServe, one of the largest US on-line service providers and one of the world's largest Internet access service providers (IAP), to shut



down communication to the neo-Nazi propaganda site on the server in the United States. As it was impossible to disconnect only this site, communication to many other sites was also shut down, so that many unrelated people and sites were affected as well. Currently, Germany's Justice Minister is preparing a new law to make firms that offer a link to the world-wide computer network liable to punishment if they discover that illegal material, such as pornography or unlawful propaganda (e.g. neo-Nazi), is available through their service and take no action to remedy the situation (Reuters Information Service, Bonn, 29 March 1996). In November 1996, CompuServe announced plans to move their European operation to another country.

In 1996, France had envisaged setting in place a text specifying existing laws with regard to the responsibilities of IAPs. This regulatory modification did not take place, but the French authorities are still considering this issue. The Swedish government has also submitted a bill that regulates IAPs' connections to controversial sites (<http://www.dsv.su.se/~jpalme/SOU-1996-40-eng.html>).

In 1996, the US Congress passed the Communications Decency Act, which may allow the government to censor or restrict content shown on Web sites. Implementation of this law has, however, been held up by a court order, and was appealed to the Supreme Court where parts of it were found to be unconstitutional. At the state level, many acts have been introduced that regulate unethical on-line activities.

In Australia, at the state level, the New South Wales government announced that people arrested for transmitting or advertising pornographic material on the Internet will face a maximum penalty of one year in prison or fines of A\$ 10 000. Under the new legislation, it will be illegal to transmit, advertise, permit access to, and retrieve pornographic materials on line. The new law also covers computer games that include violent and/or sexual activity (UPI, March 1996).

In February 1996, in co-operation with MITI, the Japanese industry association Electronic Network Consortium (ENC) made available "General Ethical Guidelines for Running On-line Services" and "Recommended Etiquette for On-line Service Users", both of which cover content management. Though the guidelines do not have force of law, it is said that a large number of the grey sites have since disappeared. In 1996, the law enforcement agency investigated the IAP BEKKOAME, claiming that it transmitted problematic content over the network. In this case, as in Germany, not only the information provider but also the IAP was called to account. In December 1996, MPT released a report concerning the handling of content on the Internet which points out the effectiveness of filtering technologies and rating systems. ENC (Electronic Network Consortium) started promoting the filtering technologies and rating systems based upon PICS and RSACI in November 1996. MPT and Yokohama City are jointly conducting the project for content filtering technology development in 1997.

Among non-OECD countries, the Singapore government takes a firm attitude towards controlling content on the WWW. It directs IAPs to disconnect sites which the government judges inappropriate. In China, the Ministry of Posts and Telecommunications announced that they strengthened regulation of Internet communications in 1995 (*Kyodo*, 21 June 1995).

## Advertising on the Internet

As advertising has come to play a more important role for Internet business, deceptive advertising, as well as advertising of products, such as tobacco or alcohol, are also becoming an issue. Reports from the Federal Trade Commission (FTC) in the United States and the OECD draw attention to the issue of cross-border advertisement (FTC, *Consumer Protection Policy in the New High-tech, Global Marketplace*, 1996; OECD, *A Global Marketplace For Consumers*, 1995).

### *Industry self-regulation*

The industry has proposed various censorware, filtering software, parent control products, and rating mechanisms to enable users or supervisors to block access to inappropriate material. In 1995, SafeSurf introduced an Internet rating system as part of an effort to create a safe “cyber-playground” for children. Soon after, an industry effort called PICS (Platform for Internet Content Selection), asked SafeSurf to assist them in designing and establishing an Internet protocol for labelling content. SafeSurf has now expanded their original rating standard to comply with the PICS protocol. The PICS protocol provides software and browser companies with a common method for reading all rated content. As the result of these efforts, parents, for example, will be able to block access to inappropriate sites or to designate viewing levels according to their children’s age and their personal standards. By early 1996, Microsoft, Netscape, SurfWatch, CyberPatrol, and other software vendors had also announced PICS-compatible products. America Online (AOL), AT&T WorldNet, CompuServe, and Prodigy now provide free PICS-compliant blocking software. In May 1996, CompuServe announced that it will use PICS-formatted RSAC labels based on RSAC and SafeSurf vocabularies to label all Web content it produces (<http://www.safesurf.com/>, 28 February 1996). The distribution of information is restricted not at the source but at the users’ premises. Ratings are done by the publishers or by third parties such as CompuServe or industry associations.

In October 1995, the Network Working Group of the US Internet Engineering Task Force (IETF)<sup>16</sup> provided a set of guidelines on Internet use, the Netiquette Guidelines. These cover ethics in one-to-one communication, including mail and talk, in one-to-many communications, including mailing lists and NetNews; and information services, including file transfer protocol (ftp), WWW, WAIS, Gopher, MUDs (multi-user domain, multiple user dimension, multiple user dungeon, or multiple user dialogue) and MOOs (MUD, object-oriented). In Japan, the Electronic Network Consortium, in co-operation with MITI, also issued a set of guidelines, as previously mentioned. The Telecom Service Association, an entity of telecommunications companies including Internet Access Providers, is studying the adoption of self-regulating guidelines regarding the treatment of the content on the Internet. In addition, various publications on network ethics and etiquette have sought to raise awareness of users and providers.

### *Policy implications*

It may be argued that existing laws should apply to regulation of content or use of the Internet. However, the characteristics of the Internet can make implementation of such laws difficult. The Internet is perhaps the first truly global communications medium based on the Internet Protocol (IP), so that communication is relayed through various routers and servers, etc., seamlessly which may enable global commerce more than anything has done previously. Some of the issues for discussion are raised below.

Is it broadcasting or not?

Regulations are imposed on radio and TV broadcasting, because they use public infrastructures and are available in public places and in the home. The issue is whether it is possible to consider Web sites as broadcasting. If they are regarded as sources of private communication, few regulations can be imposed. A user can view a site without disturbing those who do not want to see it; at the same time, the site can be reached by many people at once, as is also true for radio and TV. However, anyone can put up a Web site at relatively small cost and with little difficulty as compared to broadcasting via TV or radio. Some Web sites, in particular those published by individuals, can therefore be regarded as an expression, or a publication, of people's ideas, views, or opinions. In terms of regulations, the definition of the Internet may be crucial and important to governments.

Who is in charge of what?

In the case of CompuServe in Germany and BEKKOAME in Japan, the IAPs were ordered to disconnect sites and were investigated by the law enforcement agency, respectively. Many countries have proposed bills requiring IAPs to take responsibility for what they carry. Unlike existing media, such as magazines, newspapers, TV or radios, Internet communication involves various steps and various parties, i.e. the information providers (or content creators), the IAPs that rent space on their servers to them or who connect the information providers' servers, other IAPs that relay the connection, backbone network providers (usually telecommunication companies), the IAPs that connect to users, the users who access the information providers, and the browsers that search the latter, etc. In the case of CompuServe in Germany, the IAP that provided the connection to users (CompuServe) was called to account. So far, it is not clear whether third parties who are neither information providers nor receivers but relayers of information are responsible for content or not, and still less how IAPs are to control access to controversial content. It may be necessary to discuss the responsibility of IAPs from various aspects, such as technical capabilities, economics and legal requirements.

Cross-border advertising

Recently, Internet activities, such as providing browsing software or operating sites, have tended to depend heavily on advertising, which is becoming more and more personalised (see the following section on privacy issues). Currently, TV and radio advertising is subject to certain regulations regarding time, accuracy, goods, terms, etc. If governments try to apply such regulations to the Internet, it is expected that it will be much more difficult to accomplish than for Web sites or chatting boards.

Importance of international co-operation

The most difficult problem in controlling Internet content is that the content often originates in other countries. Assuming that a country or state can control users' access by regulating IAPs, are the regulations applicable to IAPs operating under other jurisdictions but providing access to users in that country or state? Are they applicable to foreign IAPs with access points (servers) in the country but no sales activities or corporate entities? Because the world of the Internet is not restricted by borders, there will be many issues to resolve at international level. In October and November 1996, the governments of France and Belgium proposed that the OECD start multinational discussions including content issues. International co-operation is likely to become more and more necessary for regulating information providers and IAPs or rating content through censorware.

## *Privacy issues*

Through electronic commerce, it is easy for third parties to obtain individual profiles or transaction histories. When users log on to Web sites they often give their domain name or a profile. Such information, as well as users' transaction histories, can be stored in databases maintained by system operators (which manage on-line services, IAPs, electronic bulletin boards, conferencing systems, or WWW servers such as AT&T WorldNet or America Online) or search engines.

Typical "privacy" issues can be discussed from three different viewpoints. These are: *i*) preventing the intrusion of unwanted information into one's private space and prohibiting excessive collection or tracing of personal information; *ii*) guaranteeing confidentiality (non-disclosure to others) of such information; and *iii*) ensuring that the individual can eliminate and correct personal information.

From the perspective of law enforcement, it is important to be able to trace individual transaction data for the purpose of preventing or exposing crime or tax evasion. However, some parties fear excessive censorship or abuse of power. Not only governments but enterprises such as gateway service providers (on-line shopping malls, payment services) that can get individual transaction data may present a threat to privacy.

In discussing how electronic commerce affects privacy issues, this section presents information on trends in on-line advertising and marketing, as well as measures being taken by the industry and government.

## *Recent industry trends and sources of dissatisfaction*

In terms of the economics of marketing, marketers are moving from mass to targeted marketing, a trend that seems to be facilitated by the Internet, as marketers can more readily acquire information on individuals and send e-mail ads more cheaply (see Box 5).

### **Box 5. The rise in direct interactive marketing**

Rapid development of networks and information processing makes it possible for large quantities of personal information to be acquired, exchanged, stored and matched very quickly. Not only for electronic commerce but for off-line trading as well, credit-card companies, direct mail/marketing companies, or other retailers can use personal information stored in databases for marketing. For example, American Express increased its European revenue by 20 per cent through its relationship billing service (*Nikkei Business*, 1995). It encloses, in the bills of cardholders who have purchased from certain merchants, a leaflet from those merchants. American Express receives a fee from the merchants for this service.

For some Internet service providers, advertising revenues are becoming an important revenue source in addition to subscription fees and access charges. Because of strong price competition on the consumer front, growth in revenues from users is not expected to be high; advertising or marketing support revenues from advertisers are increasingly replacing revenues from users.

In the United States, companies such as Free Ride, Inc., have provided free Internet e-mail accounts since 1995. Instead of obtaining subscription or access fees, they send users e-mail advertisements and receive a fee from advertisers. Agents, Inc., is operating sites that provide users with personalised information on music and obtain revenue from personalised advertisement services.

This kind of business is gaining ground in Japan as well. In July 1996, Hypernet communications started to provide free Internet access with advertising (see Box 6) and had acquired more than 100 000 subscribers by October. Using personal information, some companies are expanding their business to marketing support services, such as consulting services or sales agent business, etc.

#### **Box 6. Free access for reading advertisements**

When users subscribe to this type of service, they get a “viewer”, a small window on the side of the browser. On the basis of the user’s profile, interests or transaction history, the service provider posts ads, which sometimes contain a personalised message; alternatively, the provider posts ads on the user’s e-mail. Internet advertising is said to be shifting from the “banner type” to the personalised “one-to-one” ads (*Weekly Diamond*, October 1996), a trend which is facilitated by the fact that companies can send personalised messages at low cost, and by advances in database functions for computers, such as database marketing software. Both advanced marketing systems and direct mail by e-mail are becoming popular. In the United States, many direct mail companies already use e-mail.

Certain software technologies make it possible to record individual Internet behaviour. Technologies such as the cookie function (Box 7) or BroadVision’s One to One application were invented for creating personalised home pages, ads or marketing. However, they may also make it possible to record information on user behaviour and transmit it to companies that use the technologies without notifying users. Again, the private sector has begun working to resolve this issue through technological means.

#### **Box 7. Cookies**

Netscape 3.0 or Microsoft’s Net Explorer 3.0 have what is called a “cookie function”. This function registers user access and sometimes even information such as user ID, password or credit card numbers (this information represents the “cookie”) for each Web site every time users access it. (When users shop in a shopping mall, the cookie function stores information on purchases made at each shop. This allows users to pay for all of their purchases when they exit the mall, instead of at each shop.) However, as the cookie is automatically sent to each Web site when users log on, Web servers can observe user behaviour. Unlike access logs, cookies are said to be easy to store and the database easy to manage; hence, it is possible for a Web site to use personal information improperly for their business or to exchange personal information with other Web sites.

As commercial activities develop, the issue of privacy vs. personalised advertising is coming to the fore. According to Jupiter Communications (*Business Week*, 23 September 1996) Web site advertising activities were expected to generate US\$ 312 million in 1996 and to reach US\$ 5 billion by 2000 in the United States alone. However, along with these growing market expectations, there are many complaints related to on-line commercial activities and the use of personal information. On 27 September 1996, for example, the largest US on-line service provider, American Online (AOL) announced it would block e-mail ads from Cyber Promotion, Inc. AOL has been receiving more than 100 claims a day from users complaining that they were receiving too many e-mail ads, mainly from Cyber Promotion, Inc., through AOL (*Philadelphia Inquirer*, via Knight-Ridder/Tribune Business News, 30 September 1996).

### *Issues for discussion and current status*

#### Preventing invasion of privacy

In the off-line world, direct marketing activities are sometimes considered excessive. Some consumers receive what they view as too much direct mail. As the technology that enables one-to-one marketing can increase the information or advertisements sent to individuals very efficiently, consumers may receive large numbers of e-mail marketing messages from advertisers or firms. If consumers do not wish to receive such information, they may want to have some control over what they receive.

Self-regulation by the software industry has already begun. In October 1996, the Software Publishers Association (SPA) stated that software companies should consider users' privacy and encouraged them to handle users' profiles and transaction histories carefully when developing new programmes.

Some governments have started discussions on regulations concerning personal information and privacy. The OECD has been working on privacy issues in order to establish world-wide consensus and an international framework for privacy and individual autonomy (freedom of movement, freedom of assembly, and fundamental human rights) in the information infrastructure. The 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* have been adopted by all OECD Member countries as the foundation for protection of privacy. These were followed by the 1985 *Declaration on Transborder Data Flows*.

In 1995, the OECD began to hold meetings on the subject of cryptography technologies and policies in which principles involving the privacy aspects of data and lawful access to data are discussed. The process of drafting guidelines for cryptography policy began in March 1996, under an ad hoc group of experts, which is working to achieve internationally comparable criteria for cryptography policy making. In May 1997, OECD Ministers agreed the guidelines.

The United States uses a mix of approaches to personal privacy, including sectoral legislation, private sector codes of conduct, and other forms of self-regulation and voluntary privacy standards. While the United States and Japan do not regulate collection of personal data in the private sector through one single means, the European Union issued, in 1995, the European Privacy Directive, which presents principles for processing personal data fairly and lawfully (*Privacy Law & Policy Reporter*, 1995, 2 PLPR 81).

In the United States, The Center for Media Education and Children's Advertising and the Council of Better Business Bureaus have suggested that collection of information from non-adults should perhaps be restricted. In 1996, a bill aiming to control the collection of personal data from children, the "Children's Privacy Protection and Parental Empowerment Act of 1996", was introduced to Congress.<sup>17</sup>

In Japan, MITI has set a goal for providing appropriate protection of personal data through the presentation of guidelines. In March 1997, it adopted the revised version of the guidelines concerning the protection of computer processed personal data in the private sector. For the purpose of promoting the guidelines, MITI has encouraged the development of a system for granting marks to enterprises instituting appropriate protection of personal data; a consumer consultation service for general complaints or inquiries related to the protection of personal data; and a supervising system to study measures of enterprises concerning the protection of personal data and to push for improvements in enterprises providing inadequate protection. The main points of the amendment on the guidelines are as follows:

- (i) prohibition on the collection of personal data leading to social discrimination;
- (ii) clarification of the conditions under which personal data are collected, used and disclosed;
- (iii) clarification of the right to request access to correction and deletion of personal data and methods by which that right may be exercised;
- (iv) clarification of the proper management of personal data and the implementation of accountability;
- (v) guaranteeing confidentiality (non-disclosure) of personal information.

Technology is increasing the ability to gather and handle information about individuals, such as basic identification but also individual preferences, buying behaviour, or opinions on specific subjects. Much of this information may be confidential and thus require careful handling in terms of disclosure to other parties. It may be necessary to establish rules for guaranteeing the confidentiality of private information and disclosure of such information to others, though rules already exist regarding the confidentiality of private information (e.g. the OECD 1980 Guidelines on Privacy) which may suffice.

Self-regulation has also begun in this area. The mail order and telephone order (MOTO) industry has been taking the initiative. In the United States and Japan, the direct marketing associations have set guidelines for member companies on the use of personal information. In July 1996, the US DMA presented "Privacy Protection Principles on the Net" at a workshop held by the Federal Trade Commission. The ECOM of Japan has also been preparing guidelines on the handling of personal data collected by electronic and other means, which were published in spring 1997.

There are in fact regulations concerning confidentiality of personal information in the communication industry. Telecommunication companies or CATV companies are generally obliged to maintain the confidentiality of users' transaction data under laws such as the US Video Privacy Act of 1988, the Cable Television Consumer Protection and Competition Act of 1992 (which protects users from disclosure by CATV companies of their viewing preferences), and the Electronic Communications Privacy Act. However, it is unclear whether system operators and search engine providers have such obligations.

## Ensuring the individual's access to personal information

Once personal information is obtained by a third party, with or without an individual's consent, the issue arises of the possibility for the individual to update or eliminate such information or to know how such information is used. Protection of personal information would involve the individual's control over such information. It is argued that individuals should be able to correct or ask for elimination of information or to ask institutions holding such information to disclose how it is used.<sup>18</sup>

In terms of an individual's ability to refuse direct mail and to eliminate private information from commercial databases, the MOTO industry is ahead of the on-line industry. DMAs in some countries, such as the United States and Japan, maintain lists of consumers who do not wish to receive direct mail. Member MOTO companies must check this list before sending direct mail and cease sending mail to those who register on the list. Discussions concerning e-mail ads have started recently.

### *Policy implications*

As commercial activities, e-mail ads, and information gathering on the Internet easily cross borders, to what extent should these and other issues be left to the marketplace, where firms can be expected to compete in part by offering consumers the privacy they desire, and to what extent is it necessary or desirable to have industry self-regulation, national government regulation, or some international regulation or international co-ordination to answer questions such as:

- For what purpose and under what conditions are companies or institutions allowed to collect personal information?
- Under what conditions can public authorities (the courts, the legislature, or law enforcement agencies, etc.) use key escrow to trace individual transactions? Compared to off-line transactions, would official control over key escrow pose a greater threat to privacy?
- For what purpose and under what conditions can companies or institutions use personal information? When and how can they transfer (including through sale) personal information to other parties?
- Do companies or institutions that can access personal information (system operators, payment system providers, mall operators) have a responsibility to keep personal information they obtain confidential?
- What kind of action should the industry (which can access and use personal information) take to guarantee individuals the ability to access, correct and eliminate such information?

### *Payment systems and electronic money*

This section first defines and categorises new payment methods and then describes each of them. Next, related government and industry concerns and attitudes are discussed.

Electronic "payment" involves a number of issues which arise from the basic requirements for payment systems: minimising transaction costs, ensuring certain levels of security, and convenience. Some of the issues to be addressed are:



- Is it possible to develop a “cash-like” electronic device (electronic money<sup>19</sup>) for on-line payment?
- Is it economical for consumers, merchants and issuers?
- Can it be made available to both consumers and merchants?
- Is it important to standardise the payment systems?
- Is it necessary for governments to set qualification standards for issuing e-money? Is international co-operation necessary?
- Is there any impact on the money supply?
- Does electronic money facilitate “money laundering”?

Besides electronic money systems used for network payment transactions, such as e-cash or CyberCash (described below), e-money systems focusing on off-line trading, such as MONDEX or Visa Cash, are also being developed. The two movements have different backgrounds, interests, objectives, and economics. Hybrid systems such as the new electronic money system that NTT invented in September 1996 can be used not only for network payment transactions but also for off-line transaction.

#### *Current efforts*

Currently, over 30 systems and technologies, which use cryptography technologies for carrying out secure electronic payment transactions, are being proposed and tested. The various types of payment systems are here divided into four groups<sup>20</sup> on the basis of the timing of the payment and the anonymity of the transactions: credit-card-like; debit/money transfer or cheque-like; cash-like; and prepaid (see Tables 9 and 10).

#### Pay before engaging in the transaction

- Prepaid: This system uses electronic prepaid value. Users have the right to ask issuers to settle outstanding payments. Some proposed prepaid value systems do not guarantee that holders can convert value into real money. Examples are Avant and Danmont.

#### Pay at the time of transaction

- Cash-like payment system: This system involves issuing electronic cash that can be converted into physical currency and transferred without a detailed transaction record held by third parties (i.e. anonymously). Examples are MONDEX, e-cash and NTT’s new money system.

#### Pay after the transaction occurs

- Credit card-like payment system: Here, the seller’s bank account is credited the amount of the sale before the buyer’s account is debited (e.g. First Virtual, CyberCash secure Internet payment service, etc.).

Debit<sup>21</sup> money transfer/cheque-like payment system: Here, the buyer's account is debited at the time of payment. Debit-card-based systems, such as Carte Bleue in France, fall into this category. In this report, cheque-type e-money systems are viewed as realising almost real-time checking transactions or money transfer.<sup>22</sup> The transaction involves third parties, such as banks (Box 8). Examples are FSTC (Financial Service Technology Consortium) and SFNB Security First Network Bank in the United States, and NetCheque. This system transmits "payment instructions", initiated by buyers over the network, which are processed by banks. The choice of system or technology standard seems to be led by industry competition for the *de facto* standard, and complex and dynamic alliances have been formed among system/technology providers, such as the co-development agreement between MONDEX and Cybercash (*Business Wire*, September 1996) or the acquisition of MONDEX by Master Card International (*American Banker*, September 1996).

#### **Box 8. Co-operation between technology providers and financial institutions**

The two types of player in the development of electronic payment systems are e-money technology providers and e-money issuers. In general, software companies license e-money technologies and financial institutions issue e-money as licensees. For example, DigiCash (Netherlands) licenses the e-cash technology to the issuers. Currently, Mark Twain Bank (United States), EU Net (as an extension to Internet payment of Merita Bank), and Advance Bank (Australia) issue e-cash. Deutsche Bank is to issue e-cash in 1997, and e-cash can now be converted into "real" US dollars, Finnish marks, Australian dollars and deutschemarks.

#### *Policy concerns*

Electronic payment systems, like electronic commerce in general, are beneficial in terms of government interest in a competitive marketplace, with better prices and quality for consumers. However, government concerns over electronic payment systems have three main aspects: the impact on monetary policy and policies on financial markets, technology development, and consumer protection.

#### Monetary policy

There is concern that electronic payment systems may create new types of "currency" that may affect monetary policy. At the same time, the financial industry and some government bodies (e.g. the US Deputy Secretary of the Treasury, Reuters, 20 September 1996; the Nikkei financial study group in Japan, *Nikkei Techno Frontier*, 26 August 1996) seems to feel that electronic money is unlikely to have significant macroeconomic effects in the near or medium term. It is safe to say that the quantitative impact of electronic money on monetary policies is still uncertain.

Some experts and governments express concern that electronic money may facilitate "money laundering" operations. The Financial Action Trade Force (FATF), which combats money laundering, mentions in its 1995-96 annual report that electronic payment technologies can generate tremendous benefits for legitimate commerce but that the capacity to conduct significant transactions anonymously and entirely outside the banking system potentially represents a serious money laundering threat.<sup>23</sup>

## Technology/system development

It is important to clarify whether governments should take initiatives regarding methods of cryptography, protocols, or other system standards, and, if so, to what extent they should be involved. As almost all the technologies and systems are still experimental and undergoing improvements, government policy on standards setting or technology at this stage may have significant impact on the industry.

Although it would be difficult for governments to define the technology standard<sup>24</sup>, it may be important to clarify basic policies for certain features of the payment systems. For example, governments may view traceability of transactions as important for preventing financial crimes, and policy discussions on this topic would influence private sector activities in developing such systems.

## Consumer protection

Consumer protection in the financial area is an area where government can play a more concrete role. The issues are the qualification of electronic money issuers, operating conditions for payment systems, or evaluation systems from the perspective of consumer protection. A number of specific points should be considered:

- liability of issuers in case of loss or theft of electronic money;
- reimbursement of issuers if electronic money is damaged or value data is lost;
- consumer liability for unwittingly receiving forged electronic money;
- rules involving errors in downloading electronic money (by merchants);
- treatment of chargeback when transactions are cancelled;
- rules for converting electronic money into currency;
- government regulation of issuers, deposits, etc.

## *Positions of government and international organisations on the need to regulate electronic payment systems*

The views of government and the financial industry on e-money policies differ in different countries. In the United States, both the government and the financial industry feel that government should avoid any premature regulation of e-money issuers, deposits, systems, etc. (Reuters America, 18 September 1996). In Europe, Germany, for example, is taking initiatives to limit issuers of e-money to banks. In Japan, there is a law on issuing prepaid cards which may, to some extent, provide a legal framework for developing payment systems. The G10 has started discussions of issues at the international level.

In the United States, Congress has held public hearings since the autumn of 1995. In September 1996, the US Treasury Department held a conference, "Toward Electronic Money and Banking: The Role of Government" and the Comptroller of the Currency announced that the government would avoid premature regulation. At the same time, the US Treasury Department has formed a task force to examine

the impact of the move towards electronic money transfer and storage technologies on consumers (*American Banker*, September 1996). A draft report on electronic commerce by the US Information Infrastructure Task Force (IITF) argues against premature regulation (“A Framework for Global Electronic Commerce”, [http://www.iitf.nist.gov/electronic\\_commerce.htm](http://www.iitf.nist.gov/electronic_commerce.htm)).

In Europe, the EMI (European Monetary Institute) submitted a report on the multipurpose prepaid card in 1994 which concluded that only banks should issue e-money.

The German government plans to give banks alone the right to issue prepaid cards or so-called electronic purses, as part of a new German banking law. The law is still under preparation but is expected to be enacted in 1997 (Reuters, September 1996).

In October 1996, the Bank of England (BOE) warned the British nation against unreliable on-line banks. It named the European Union Bank (EUB), pointing out that EUB is not supervised by a major country and that depositors or investors might encounter problems. EUB does not issue e-money but has a sort of virtual bank in Antigua (a tax haven), which accepts Internet accounts and settlements.

In the early 1990s, when various Japanese companies (telecommunications, public transportation, gas stations, department stores, or food stores), began to issue prepaid cards, issuing more than 250 million a year, the Prepaid Law was enacted to protect consumers. It covers multipurpose prepaid cards and regulates conditions for issuing cards, deposits, etc. In 1995, the Ministry of Finance organised a council on e-money and e-money transactions.

In November 1996, the G10 formed a working party on electronic money, which was to submit a report on the following issues by April 1997:

- the current status of electronic money and a summary of work on electronic money undertaken by international organisations;
- a survey of recent legislative and regulatory developments in G10 countries;
- consumer protection issues (including cross-border implications);
- criminal law enforcement issues (including the incidence of money laundering);

In November 1995, the Bank of International Settlements (BIS) submitted a report on the influence of electronic money on monetary policies. The report points out that electronic money may affect the money supply or facilitate money laundering. It concludes that limiting issuers and setting regulations, such as limits on amounts, should be considered.

At the OECD, a workshop on the economics of the information society was held on 23-24 October 1996. The need to impose reserves or other requirements on entities issuing electronic cash was pointed out, as was the need for careful monitoring of the effects on the monetary policies. It was also strongly emphasised that, although government intervention is necessary, hurriedly drawn measures to regulate the cyber economy could be detrimental to the development of a potentially lucrative commercial activity with potential benefits for consumers.

Because electronic money commonly uses cryptography technologies, cryptography policies also closely affect the development and diffusion of electronic money. Export control on cryptography technology may also affect the use of electronic money for cross-border transactions.

### *Consumer protection issues*

The Internet can create a global marketplace, where consumers are able to purchase goods and services from sellers located anywhere in the world. While Internet sales of all kinds of goods and services are expected to grow, consumer issues such as conditions of cancellation or cooling off, warranties, or chargeback mechanisms are becoming important. This section examines specific cases of commercial activities, then reviews the activities of regulatory bodies and examines policy implications.

Consumer protection has many facets. The following five issues can be regarded as key consumer protection issues: *i*) fairness and truthfulness in advertising; *ii*) labelling and other disclosure requirements such as warranties, guarantees, product standards and specifications; *iii*) conditions for cancellation or cooling off; *iv*) refund mechanism in the case of cancelled orders, defective products, returned purchases and lost deliveries, etc.; and *v*) the mechanism for qualifying merchants in terms of the above. The cases described are discussed with respect to these issues (with the exception of advertising, discussed above).

### *Case studies*

This section gives examples of actions or measures taken by the major Internet shopping malls, Internet access service providers, on-line service providers (such as America Online, CompuServe, Prodigy, or NiftyServe), industry associations and government.

Competition provides consumers with important protections in these areas. For example, in order to encourage consumer confidence, many on-line service providers or shopping malls set certain qualification standards for merchants to be allowed to open a “shop” on their servers. They tend to apply the programmes or rules used by credit-card companies for liability in case of fraud. However, warranties for defective products, damaged products, or acceptance of returned merchandise generally remain at each merchant’s discretion. The schemes tend to be limited to transactions between domestic merchants and users.

#### AOL Certified Merchants Program and Guarantee

In October 1996, America Online (AOL), one of the largest US on-line service providers, announced its AOL Certified Merchants Program and Guarantee. Under this programme, merchants must comply with certain conditions, protect against credit-card fraud, and make interactive shopping quick, easy and secure. Merchants are expected to use e-mail effectively for order processing, customer service, order confirmation and for guarantees. These are the standards usually expected in the physical retail world, and in some respects AOL intends to surpass real-world standards, as all certified merchants are required to maintain world-class customer service policies. The AOL Guarantee protects transactions with AOL certified merchants from credit-card fraud and ensures complete customer satisfaction or money back (*Netwire*, 9 October 1996).

#### AT&T WorldNet Service

At the beginning of 1996, AT&T announced a liability programme for its Internet access service, AT&T WorldNet Service. When members use the AT&T universal card to make purchases on the Internet they will be protected by the service. The protection applies to fraudulent transactions by

unauthorised users. AT&T also started to compensate for electronic mail failure. AT&T WorldNet Service customers experiencing electronic mail failure will receive, for example, a 30-minute phone card or credit for a half-month of standard service on AT&T WorldNet.

## NiftyServe

In Japan, on-line service providers are also introducing programmes to protect consumers involved in electronic commerce. NiftyServe, the largest Japanese on-line service company, with 1.8 million subscribers and 110 merchants, has strict rules for merchants who open “shops”. For example, to qualify, merchants must have significant experience and skills in direct marketing.

## Current status and prospects

### *Market size and growth trends*

Currently, Internet commerce is quite small, representing at most about US\$ 500 million worldwide.<sup>25</sup> However, every source of market research forecasts significant growth in market size over the next three years. The most conservative forecasts expect growth of at least ten-fold for three to four years, and the most optimistic foresee about US\$ 780 billion in 2000 (Killen and Associates). The latter figure would represent about 10 per cent of the overall retail and wholesale market.

As mentioned in the section on authentication, direct marketing associations are accustomed to setting rules for quality of products or services, price, and cancellation procedures. These associations certify that member companies respect such rules, and they have begun discussion on expanding their rules and activities to Internet trade.

### *Issues for discussion*

If consumers are to have confidence in electronic commerce, new consumer protection mechanisms may be needed. Some of these mechanisms can come about through the competitive process, but others will require co-operation among industry and government on an international basis as well as consumer education. OECD discussions on the global marketplace from the viewpoint of consumer protection have taken place since 1994. Issues covered include the handling of credit-card fraud or misuse, simplifying customs procedures, establishing refund systems, ensuring fairness and truthfulness of advertising and standardising of labelling, and other disclosure requirements. While discussion originally centred on issues arising from international mail order or telephone order activities, it now covers electronic commerce as well. The following are issues which may require international co-operation mechanisms and regimes:

- Pay back mechanisms: These involve “refunds” for cancelled orders, defective products, returned purchases, and lost deliveries. Today, even if merchants accept returns or cancellations, refunds are difficult, especially for cross-border transactions. Cheques are normally limited to domestic use. International money transfer is expensive and the

procedure complicated. Credit-card refunds on international transactions encounter similar problems. Discussions of international chargeback on credit card transactions have been conducted at the OECD, with the aim of establishing industry guidelines.

- International harmonisation of rules of trade: Regulations to protect consumers differ among countries and regions. For example, there are differences in labelling or other disclosure requirements, warranties, guarantees, product standards and specifications, product liability, and rules for offering or accepting orders. For instance, Germany does not allow selling contracts solely over the telephone. It is important to the development of electronic commerce to minimise the difficulties caused by these differences, while avoiding uniformity of the sort that would harm consumer welfare by preventing firms from responding to consumer demand. It is also important to avoid rules that would stifle innovation. One possibility in this direction would be to agree on standards of consumer protection for cross-border trade or to create model contracts that include procedures for consumer protection.
- Consumer education by the industry or governments: International business-to-consumer commerce is just emerging, and consumers are not yet very aware of how to avoid potential problems, particularly for shopping on the Internet. It is important to enhance consumer awareness of potential problems, appropriate procedures, and measures to avoid problems.

### *Impacts on taxation rules*

The Internet has made it easier for both SMEs and individuals to enter the marketplace, as they need neither physical shops nor sales offices. The network revolution has also changed the concept of firms. Today, it is no longer necessary to have stocks, means of transportation, warehouses, or money collection systems. This means that cross-border transactions are likely to increase and that overseas or off-shore operations will benefit from electronic commerce over the global network.

This raises questions about how existing rules of taxation are to be applied or whether new rules are needed. For example, the nature of electronic commerce may make it difficult to define “taxable income” or “taxable transactions”. Nor is it easy to identify “taxpayers”. Moreover, it may be difficult for regional authorities to define business profits or royalties.

There is also the question of which government has jurisdiction in taxation matters in the traditional sense. It may be difficult to define where the substantive facility or assets are located or where transactions are taking place if servers are scattered throughout the network and transactions are processed across many countries. The risks are duplication of taxation and loss of opportunities to collect legitimate taxes and thus problems for governments’ fiscal policies. This section reviews recent discussions on taxation issues.

### *Tax issues under discussion*

A key question for governments is how the development of electronic commerce relates to the current tax system, including substantive principles of direct and indirect taxation, as well as increased opportunities for tax avoidance and evasion, and issues of tax administration.

## Issues relating to the OECD Model Tax Convention on Income and Capital

A major problem seems to involve the mismatch between the nature of cyberspace and a basic concept of taxation, i.e. permanent establishment (PE) of the OECD Model Tax Convention on Income and Capital.<sup>26</sup> The concept of permanent establishment is designed to determine when a non-resident of a country becomes subject to taxation in that country by virtue of business activities conducted there. It generally requires a “fixed place of business” or the physical presence of a dependent agent with the ability to conclude contracts in the name of the enterprise. This standard was developed in an era where the conduct of significant business could be carried out only through physical presence. The absence of a geographic “location” in cyberspace challenges also the jurisdictional rules for “source” and “residents”, and the nature of sites on servers challenges the PE concept under tax conventions while digitalisation and transmission technologies may change the character of income.

*Is the WWW site a permanent establishment for tax purposes?* The concept of PE is particularly unclear in cyberspace. There is debate over whether or not an Internet site on a computer server is a PE in the country where the computer is physically located. Given that mirror servers of the same sites are scattered all over the world, the issue remains quite unclear. Even if a permanent establishment is determined, attribution of income to the PE becomes difficult.

*Identifying residents and sources.* Another issue is the difficulty of identifying residents and sources. In order to tax effectively, a revenue authority must be able to identify taxpayers adequately, so that taxpayers are only taxed on their own income and, in case of non-payment, they can be identified and legal notices can be served on them or other action taken. An Internet business site does not necessarily identify a taxpayer, particularly when the business uses a trade name.

In the physical world, trade names are regulated and registered to taxable entities, the identity trail can be followed, and proof of identity arrangements reduce the risk of false identities. No such mechanisms exist for cyberspace entities, with the result that identification presents a problem.

Further, it has become easier to separate the source of service from the location where it is provided. For example, professional service providers, such as financial advisers, can provide their services to clients in other countries via the Internet. Therefore, it would appear very difficult for local authorities to identify residents and sources.

*Characterisation of income* is important for taxation as taxes differ according to the nature of the income, and electronic commerce may change the characteristics of various types of income. One of the distinctions used is to define income broadly as being derived from either goods or services. Today, however, technology is making goods and services interchangeable to some extent, and it is affecting the treatment of taxation. For example, digitalisation and transmission technologies are going to make it possible to download music, games, and computer or other software across borders through the network. The taxable income generated by a digital product may be of a different character from the taxable income generated by the physical equivalent of the product. This represents a challenge to the extent that there is an arbitrage opportunity in the tax rates applied to a digitised and a non-digitised product which are identical in the hands of the consumer.

*Issues relating to transfer pricing.* Electronic commerce has the potential to raise serious transfer pricing issues because of difficulties in applying the traditional rules to transactions carried out electronically, rules which are used to allocate, between countries, the taxable profits in highly integrated groups of companies. Computer networks allow for increased speed and integration of transactions,



thereby making it difficult to apply the transactional analysis prescribed in the OECD Transfer Pricing Guidelines. One example of this difficulty is the case of global trading carried out electronically, where many offsetting transactions are undertaken in locations around the world on a 24-hour basis.

*Issues relating to value added tax (VAT) and general sales tax (GST).* The VAT and GST issues for electronic commerce concern the rules governing when a country has the right to impose VAT or GST on a transaction for services, e.g. telecommunications services or information services. In general, services are subject to VAT based upon the “place of supply”, which for some types of services is the place where the customer resides or has a “fixed establishment”. In other cases, it is where the vendor resides or has a “fixed establishment”. The concept of “fixed establishment” for VAT or GST purposes may not be sufficiently comprehensive to deal with electronic commerce.

#### Tax administration issues

*Increased opportunities for tax avoidance and evasion.* Traditional concerns about cash economy will apply to electronic cash money but with new challenges, such as the reduction in bulk and the ability to evade existing reporting mechanisms. Governments are concerned by this potential loss of revenues.

*Record keeping and access.* Another problem is technical blockage of access to records, including by encryption. The tax law of most countries includes a requirement that taxpayers, or other parties to a transaction, keep records of the transaction, so that taxable income can be calculated. Generally, this requirement stipulates that the records should have certain characteristics, such as being kept in or convertible to a particular language, location, or form.

It is easy to convert digital transaction into books of accounts, and this can reduce the burden of merchants or authorities. However, commercial transactions in cyberspace may be encrypted or secured in some fashion, so that there is a possibility that the authorities could not access records unless they are given the right to access plain text or cryptographic keys.

*Enforceability of withholding taxes.* Electronic commerce leads to the elimination of middlemen between producers and consumers. These middlemen were traditionally leverage points for withholding taxes, and the loss of these compliance leverage points is a major concern as it may lead to lower levels of compliance and higher costs for tax administrations to collect revenues from a larger number of sources.

#### *Government initiatives*

While there are no obvious remedies, it is clear that consistent approaches at international level are urgently required to ensure the effectiveness of taxation laws. Some multinational initiatives have been taken. Given the possibility of either shared or conflicting interests between taxation and other issues involving the characteristics of the Internet, such as trademarks and encryption technologies, it is important to examine these issues in a co-ordinated manner.

In response to these challenges, the authorities of some countries are examining the issues and have begun to discuss solutions. In November 1996, the US Department of the Treasury Office of Tax Policy submitted a report, “Selected Tax Policy Implications of Global Electronic Commerce”.

In June 1996, the United States, Canada and Australia jointly submitted a paper for the OECD Committee on Fiscal Affairs, which decided to carry out in-depth work on the potential of the communications revolution for all significant aspects of taxation for which it is responsible.<sup>27</sup> The Committee on Fiscal Affairs continued its discussion in January 1997, on the basis of reports from various sub-groups.

### *Security*

This section describes issues involving network security, in particular with respect to electronic commerce. These include reliability of the network and protection of information systems against intrusion, fraud and other crimes.

### *Risks on the Internet*

In terms of security, the Internet is still immature<sup>28</sup>. The risk of hacking or tapping is much greater than for proprietary networks. Moreover, the Internet itself may not be dependable, as the growth in infrastructure capacity may not be able to keep up with the rapid growth in demand. Some experts claim that the network could break down entirely in the near future (*Nikkei Shimbun*, 12 November 1996).

Various technologies are designed to address these problems. Cryptography and firewall technologies are meant to ensure confidentiality of information and defend against intrusion. Investment in and improvement of the infrastructure is continuing, with expansion of transmission capacities and the introduction of ATM relay systems or other high-capacity infrastructure equipment. However, the situation is not fully under control. Some accidents have occurred which indicate the network's vulnerability. In August 1996, AOL's network operations ceased for about 18 hours owing to accidents. Microsoft Network has also stopped operating several times.

### *Liability sharing and security regulations*

#### Current status of liability issues for business-to-consumer electronic commerce

When the network is damaged or information transmission is interrupted, how should the liability be shared among network providers, IAPs, software providers and users (i.e. consumers and merchants)? From the perspective of more secure Internet electronic commerce, liability-sharing issues are important.

In the case of EDI transactions, which are more oriented to business-to-business trade, precise rules for liability sharing exist and these can be applied to cross-border trade as well. Among the various relevant initiatives, mention may be made of the EDI Agreement developed by the American Legal Profession Association in 1990, the Data Interchange Agreement (of the Japan Information Processing Development Center), and UNCITRAL (the United Nations Commission on International Trade Law) Model Law on EDI trade (still in draft form).

For business-to-consumer cross-border trade, discussions on standardisation of liability-sharing rules for mail order shopping have already started, for example in the OECD Committee on Consumer Policy, although on-line shopping has not yet been specifically discussed.

To gain the confidence of users who engage in electronic commerce, a standard international model for liability sharing among parties involved may be worth considering, following what was done for EDI in the early 1990s.

#### Rules and regulations on security

In countries such as Japan, there are guidelines for network security which some industries, such as banking, have to meet. So far, these guidelines are based on proprietary networks, but the same kinds of guidelines should be set so that the industry and consumers can see the level of network security.

In 1992, the OECD issued Guidelines for the Security of Information Systems. These guidelines provide an international framework for developing and implementing coherent security measures, practices and procedures in the public and private sectors.

In January 1996, European countries adopted common criteria, which can be a basis for an international security standard. The International Organisation for Standardisation (ISO) is also going to set an international standard in 1998. To enhance electronic commerce and avoid inappropriate activities, it may be necessary to hasten international standard-setting activities, considering the nature of the various industry activities.

## CONCLUSION

Business-to-consumer electronic commerce may bring significant benefits to consumers and industry. Risks for conducting transactions on the network remain. Technologies are being developed and tested to improve the environment for transactions over the Internet. Technological development is not sufficient, however. Existing regimes and rules may not be appropriate to electronic commerce across national borders. Electronic commerce has the possibility of creating a true global market regime, and governments, industries and consumers face a real challenge for establishing new market mechanisms.

Three major actions are needed. There should be more research on the economic implications of electronic commerce. Specific industry issues should also be reviewed. And most urgently, a horizontal approach should be taken to resolve various issues concerning electronic transactions, so that countries can come to agreement about relevant basic principles.

In establishing such basic principles, the following framework issues should be considered. First, it should be examined whether existing laws or regulations contain elements that obstruct the development of electronic commerce, and if so, they should be eliminated as soon as possible. Second, activities of individual firms and market mechanisms should be respected when solving some of the issues concerning the electronic commerce transactions. Third, attention should be paid to industry self-regulation, as firms may respond more swiftly to the dynamic development of the market. Fourth, in view of the rapid development of the technologies, premature introduction of new regulations should be avoided as much as possible.

### **A closer look at the economic impact**

The development of business-to-consumer electronic commerce can significantly influence existing market activities. It can be expected to create more dynamism, owing to more entrants into the market or more competition among the players. Consumers can expect to have more choice and convenience, as well as better prices.

Emerging intermediary businesses or functions, such as payment systems or shopping malls, may also affect market dynamics. They may provide market functions necessary for consumers and merchants in facilitating the growth of the market and realising competition between electronic commerce and traditional markets.

Further research needs to be conducted to identify further potential benefits and risks of business-to-consumer electronic commerce. Such research should be the foundation of policy decisions that address both general and industry-specific issues.

## **Industry-specific issues**

In some industry sectors, the penetration of electronic commerce is raising specific issues. It may bring in its wake new business conduct and actions that do not conform to existing industry practices or regulations. Discussions have already arisen in certain industries, concerning, for example, the retailing of pharmaceuticals or alcoholic beverages, resale price maintenance systems for books or music CDs, or practices in certain services industries such as travel or financial services. It is important to clarify the rules, and to identify regulations which require modification.

On-line transactions are likely to stimulate the growth of new industry sectors, such as digital publishing and on-line advertising. The development of such industries may also raise issues that governments should examine.

## **General issues**

The development of electronic commerce is creating “new” regimes for the global market. Various rules and systems developed for traditional economic activities now require careful review. They cover almost all aspects of transactions. While such a list is not exhaustive, horizontal issues such as authentication, contracting, content handling, privacy, payment, consumer protection, taxation, and security are among those that must be dealt with as a condition of carrying out commercial transactions on the network.

It is important to address these issues concurrently in order to achieve healthy development of electronic commerce. They need to be faced by both merchants and consumers in many sectors in all countries. If any one of them is not satisfactorily resolved, it may constitute a bottleneck in on-line business transactions. Concurrent discussion is the key factor in moving towards solutions. It is important to identify which issues should be dealt with by industries, and which should be dealt with by industry self-regulation and which by government regulations. Government action may be required to eliminate some obstacles to conducting electronic commerce, such as taxation. With respect to other issues, such as authentication, privacy and consumer protection, individual firms may have an incentive to find and implement solutions for their own use that would influence the behaviour of the firms with which they compete. However, competition may not be sufficient to resolve all aspects of these issues. In such cases, industry self-regulation may be part of the solution. It should be noted that industry self-regulation can, in general, be implemented more quickly in reaction to the dynamic development of the market and technologies than government regulations. Moreover, the introduction of regulations at a premature stage may hinder market development.

An internationally co-ordinated approach is urgently needed. Given the speed at which electronic commerce is developing, countries may apply or introduce various rules to address those issues. Also, industry-self regulation may also develop locally or regionally. However, if there is a lack of co-ordination, in basic principles on those rules, the healthy development of the electronic commerce market would be impeded. Moreover, once established, such rules or practices would not be easy to change. Basic principles and guidelines for addressing institutional issues related to electronic commerce should be established in a co-ordinated manner before countries establish rules independently.

Table 1. **Electronic commerce overview**

	Proprietary network <sup>1</sup>	Open network <sup>2</sup>
Business to business	Bank POS ACH (automatic clearing house e.g. SWIFT) EDI (electronic data interchange) CALS (continuous acquisition and lifecycle support)	Procurement or marketing on Internet using Web sites Commercial transactions using e-mail communication
Business to consumer	On-line shopping through proprietary networks, e.g. America Online, CompuServe or Minitel	Internet shopping on Web sites On-line banking via the Internet Commercial transaction using e-mail communication

1. Proprietary network: Owned and managed by the specific service providers or network management organisation. Use of the network is limited to the parties or participants who have rights or membership to use by agreeing upon the terms and rules for the use of network.
2. Open network: Network which has no specific manager or controller to govern the entire system. Anyone who wishes to connect to the network can do so if certain technical requirements are fulfilled. In case of the Internet, it is a network of various networks which are connected by fulfilling the technical communication protocols. There is, in general, no specific qualification for joining the network other than technical and commercial requirements, such as having the necessary equipment and subscribing to the services of certain service providers.

Table 2. **Electronic commerce market forecasts** <sup>1</sup>

		Billion US\$					
	Institutions	1994	1995	1996	1998	1999	2000
Electronic commerce market	Killen & Associates	small					775
	Activ Media		0.436			46	
	Forrester Research			0.518	1.849		6.6
	<i>Veronis, Suher &amp; Associates</i>	<i>0.048</i>				<i>3.5</i>	<i>(6.1)</i>
Distance trade	Killen & Associates	600					2 150
Total retail market	Killen & Associates	4 600					8 000

1. Numbers without brackets are market estimates for the Internet alone; numbers in brackets include all networks (America Online, CompuServe, CATV, etc.); figures are world-wide, except figures in italics, which are for North America only.

Source: Nomura Research Institute, Fuji Keizai America, and institutions represented in the table.

Table 3. **Emerging industry sectors**

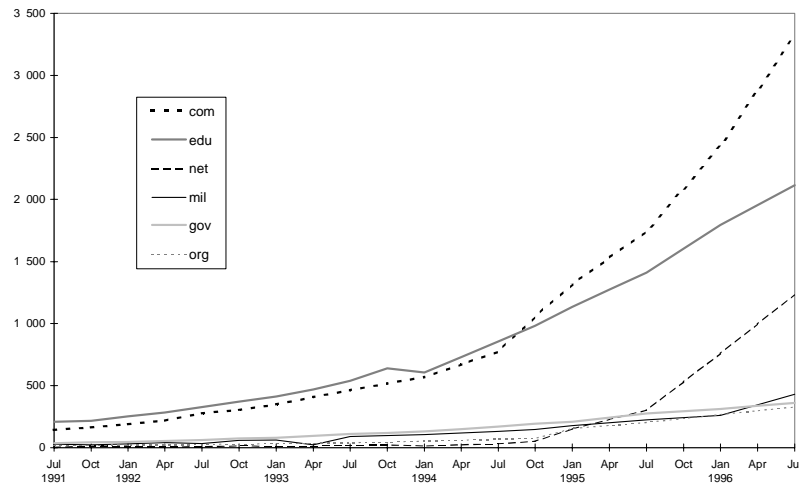
Percentage of users having used the applications

	Current situation on the Internet		Comparable sectors on the Minitel	
Agent services	Tickets & travelling	4	Travel services	47
Trade in goods	Music, CDs	22	Shopping	38
	Computer equipment	40		
Information services			Information services e.g. news services	29
			Yellow pages	95
Public services			Public services	52
Financial services			Home banking	53
Advertising			Advertising	23

Source: Forrester Research (June 1995); France Telecom (April 1995).

Figure 1. **Growth in commercial Web sites**

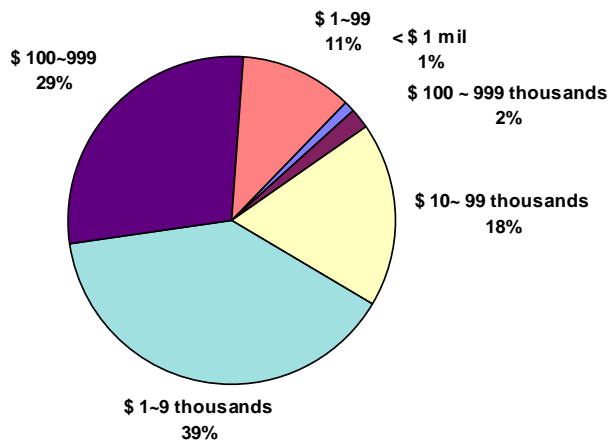
Thousands



Source: OECD, *Information Technology Outlook 1997*, from Merit, September 1996, <http://nic.merit.edu/nsfnet/statistics/>.

Figure 2. **Distribution of monthly sales generated by Web sites**

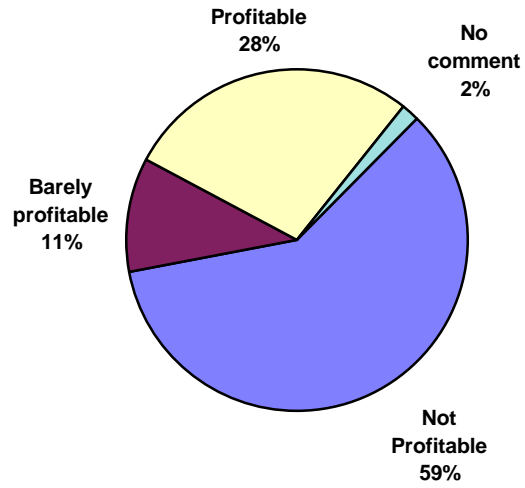
Percentage of respondents with some sales



1. Covers 150 US companies whose sales during the previous month were at least US\$ 7 100.  
Source: Fuji Keizai USA Inc., 1995.



Figure 3. **Profitability of Internet commerce activities**



1. Results of an e-mail survey covering 64 respondents from 150 Internet shops in Japan chosen at random by *Weekly Diamond Magazine* survey was conducted by e-mail.

**Source:** *Weekly Diamond Magazine*, October 1996.

**Table 4. Reasons for using Web sites**

Percentage<sup>1</sup>

	Aug.1995	Aug. 1996
Gathering product information	75	77
Researching competitors	49	49
Collaborating	45	53
Vendor support	43	52
Internal communications	39	42
Customer service	36	38
Publishing product information	31	33
Purchasing products	30	24
Selling products	16	11

1. Percentage of respondents indicating each reason; many gave multiple reasons.

Source: Commerce Net/ Nilesen Internet Demographics Survey.

**Table 5. Future use of Internet**

Percentage

	Nov.-Dec. 1995
Information access	70
Communications	68
Education	57
Advertising and marketing	39
Entertainment	35
Buying and selling	30
Community service	27

1. Based on a telephone survey conducted in November and December 1995 to 1 000 randomly selected Internet users.

Source: FindSVP, "The American Internet User Survey", <http://etrg.findsvp.com/internet/highlights.html>.

Table 6. Internet user profile

	Europe			United States		
		1995	Apr-May 1996		1995	Mar-Jun. 1996
Gender	Male	92%	85%		90%	66%
	Female	8%	15%		10%	34%
Marital status	Married	40%	n.a.		47%	
	Single	57%			53%	
Household income		\$100,000 (10%) \$50 000-100 000 (33%)	n.a.		Avg. \$59 600	\$80 000+ (22%) \$60 000+ (21%) \$40 000-60 000 (12%)
Avg. age		n.a.	28.8		29	27-28
Education	College degree	50%	n.a.	College degree	n.a.	47%
	Masters or higher	40%	n.a.	Post graduate	n.a.	29%
Occupation	Computer field	33%	n.a.	Computer	n.a.	16%
	Management & Professional	30%		Technical		17%
				Managerial, professional		37%
PC use	30 hours +/-week	50%	n.a.	Use once a day	n.a.	13%
				Frequent access to WWW		48%
				Purchase product or service		14%
				Business use of WWW		41%
Own PCs	10 hrs/week playing with PCs	78%		5 years+		64%
	At least one	90%		Home computer		79%
	Two or more	40%				
Internet experience	Less than a year	43%	n.a.	Had not used before April 1995	n.a.	55%
	More than 4 years	41%		Used more than 1 year earlier		45%

Source: EU: Graphs Visualization and Usability Centre, 5th User Survey; US: Simba Information, Inc., Univ. of Michigan Business School Study, Commerce Net/Nielsen Internet Demographic Survey, *Wired* Magazine.

Table 7. **Households with PC/modem and growth of the WWW**

Percentage

	United States		Canada		Japan		United Kingdom		France		Germany	
	1990	1995	1990	1995	1990	1995	1990	1995	1990	1995	1990	1995
Personal computers	15%	25.5%	16.28%	28.88%	15.5%	15.6%		20.1%	11.2%	14.3%		25%
Modem equipped PCs		15%	8.45%	12.1%				4.4%		1%		3%
No. of Internet hosts	427 817	8 224 279	18 582	424 356	6 657	496 427	6 990	579 492	9 290	189 786	21 109	548 168

Source: OECD, Information Technology Outlook 1997.

Table 8. Issues involving electronic commerce

Issues on the transaction steps								Horizontal Issues	
Steps	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7		
Activities	Establishment	Marketing	Production	Negotiation Contract	Payment	Nullification Cancellation	Payment of tax, custom duties	Privacy	Security
Consumer		<b>Privacy</b> - Excess individual marketing		<b>Authentication</b> - finding legitimate merchants/individuals - preventing forgeries	<b>Payment and Electronic money</b> - availability to everyone - economics - security - financial	<b>Consumer Protection</b> - nullification - cancellation - cooling off		<b>Privacy</b> - Intrusion of unwanted information into one's private space - confidentiality in disclosure of the information - autonomy over the individual information	<b>Security</b> - impacts on the Law Enforcement, national security - reliability of the system - durability of the system - liability sharing
Companies	Trademark rights	<b>Making rules</b>	IPR protection		Confidence	<i>Liability sharing</i>			
Governments		<b>Handling contents</b>		Effectiveness of electronic contracts			<b>Impacts on taxation rules</b> - Income tax - VAT		

Table 9. Various payment methods <sup>1</sup>

Pay before	Pay now	Pay after	Method	By
Prepaid payment systems			<b>VISA Cash</b> <b>Master Card Cash</b> <b>Cyber Cash 'Coin'</b> CAFE (conditional access for Europe) Avant Chip Knip DANMONT Proton Postcard, postmat BTSC Port Moedus Multi Banco <i>S Card</i> <i>FISCARD</i> <i>NETS</i> <i>Intelligent IC Card</i>	VISA International Master Card International Cyber Cash EU, Industry Consortium Finland, (Merita Bank, DKD Bank, Post Bank) Interpay (Netherlands) Jiro Bank, KTAS (Denmark) Banksis (Belgium), Interpay, Mitel (Brazil), etc. Swiss MPT Sociedad Española de Medios de Pago (Spain) Sociedate Interbancaria de Servicio (Portugal) Creative Star (Hong Kong) Financial Information System Center, Bank of China Consortium of banks in Singapore Fuji Bank (Japan)
	Cash-like payment systems		MONDEX e-cash <b>Net Cash</b> NTT e-money	MONDEX UK (Nat. West, Midlands, Master Int.) Digidash, Canada Royal Bank, Deutsche Bank, etc. Information Science Institute (UCLA) NTT
		Debit, money transfer-like payment systems	<b>FSTC (Financial Service Technology Consortium)</b> <b>SFNB (Security First Network Bank)</b> <b>Net chex</b> <b>Net cheque</b> <b>Net Bill</b> <b>Solo-payment</b> <b>Check Free Wallet</b> <b>Quicken</b> <b>Microsoft Money</b> Le port monnaie électronique	Citibank, Chemical Bank, Bank of America Security First Network Bank, FSB Net 1 Information Science Institute (UCLA) Information Networking Institutes (Carnegie Univ.) Merita Bank Check Free Intuites, 19 banks Microsoft, 10 banks France Telecom, France MPT
		Credit card-like payment systems	<b>First Virtual</b> <b>CyberCash</b> <b>Netscape Commerce Server</b> <b>SET (Secure Electronic Transaction)</b>	- First Virtual Holdings - Cyber Cash - Netscape Communications - VISA Int, Master Int.

1. Bold: US; plain: Europe; italic: Asia (Japan, Chinese Taipei, Singapore).

Source: Ito, Nakamura, "Digital Cash", Diamond Publishing, July 1996.

Table 10. Characteristics of the various payment systems

Category			Names	Nature of systems		Characteristics of the systems or technologies						Devel. phase		
Pay before:	Pay now	Pay after		Supplements existing payment methods	New payment scheme	Focus on off-line use	Focus on on-line use	Transferable (open loop)	Non-transferable (closed loop)	Available to small merchants	Available to all consumers	Anonymity	In commercial operation	Experimental
Pre-payment system			VISA Cash		x	x		x	y	2	y/n		x	
			Master Card Cash		x	x		x	y	2	y/n		x	
			Cybercash 'Coin'		x	(x) <sup>*21</sup>	x							
			CAFE <sup>*6</sup>		?	?		x	y	?			?	
			Avant <sup>*7</sup>		x	x			x	x		y	x	
			Chip Knip <sup>*8</sup>			?		x	?	?				?
			DANMONT <sup>*9</sup>		x	x		x	y	2				x
			Proton <sup>*10</sup>		?	?		x	?	2				?
			Postcard / Postmat <sup>*11</sup>		?	?		x	?	2				?
			BTSC <sup>*12</sup>		?	?		x	?	2				?
			Porta Moedus Multi		?	?		x	?	2				?
			Banco <sup>*13</sup>											?
			S Card <sup>*14</sup>		?	?			x	?	2			?
		FISCARD <sup>*15</sup>		x	?			x	?	2			?	
		NETS <sup>*16</sup>		?	?			x	?	2			?	
		Intelligent IC Card <sup>*17</sup>		(x)	x			x	y	2	y/n	x		
	Cash-like payment systems		MONDEX		x	x	(x) <sup>*21</sup>	x	y	2	y	x	x	
			e-cash		x		x		y	2	y	x		
			NetCash		x		x		y	2			?	
			NTT e-Money System		x		x		y	2			x	
		Debit, money transfer-like payment systems	FSTC <sup>*1</sup>	?		?			x	?			?	
			SFNB <sup>*2</sup>	x		?			x	?			?	
			NetChex	x			x		y	2			?	
			NetCheque	x			x		y	2			?	
			Net Bill	x			x		y	2	y/n <sup>*19</sup>		?	
			CheckFree Wallet	x			x		y	2	y/n		?	
			Quicken <sup>*3</sup>	?			x		?	?			?	
			Microsoft Money <sup>*4</sup>		?		?		x	?			?	
			Le port-monnaie électronique <sup>*5</sup>		x		?		x	?			?	

**Table 10. Characteristics of the various payment systems (cont'd)**

	Credit	Solo-payment	x		x	x	y	y	n	x	
	Card-like	First Virtual	x		x	x	y	1~2 <sup>18</sup>	n	x	
	payment	CyberCash	x		x	x	n	1	n	x	
	system	Netscape Commerce Server (RSA)	x		x	x	n	1	n	x	
		SET	x		x	x	n	1	n		x

Source : Ito, Nakamura, "Digital Cash", Diamond Publishing, July 1996.

1. Financial Service Technology Consortium (Citibank, Chemical Bank, Bank of America, etc.)
2. Security First Network Bank (Security First Network Bank, FSB)
3. Operated by Intuit and 19 banks
4. Operated by Microsoft and 10 banks
5. France MPT, French Telecom
6. Conditional Access for Europe
7. Finland, Consortium of leading three banks
8. Operated by Interpay (same as Proton)
9. Jairo Bank (Denmark), KTAS (Denmark)
10. Banksys (BE), Interpay (NL), Mitel (BR), Quicklink (AU) and Telecure (SW)
11. Swiss MPT
12. Operated by Sociedad Española de Medios de Pago (SEMP, Spain)
13. Operated by Sociedade Interbancaria de Servicio (SIBS Portugal)
14. Operated by Creative Star (Hong Kong)
15. FISC (Financial Information System Center) (Chinese Taipei)
16. A syndicate of banks in Singapore
17. Fuji Bank
18. First Virtual is now limited to credit-card users, but it is applicable for bank account transfer
19. Issuers cannot know " what the user purchased" but " when and where purchased"
20. ASIA ( Hong Kong, Japan, Singapore, Chinese Taipei)
21. Cybercash and MONDEX announced co-development plan



## NOTES

1. The Internet provides free search functions, such as Yahoo, Infoseek, Altavista and Lycos. Users can relatively easily search for Web sites containing user-specified key words. These engines can search through the registered sites, which number around 30 million pages world-wide.
2. For example, Active Media estimates electronic commerce on the Internet at US\$ 436 million for 1995 and Forrester estimates it at US\$ 518 million for 1996.
3. According to a survey by the Network Wizard Inc. (USA), there are 734 000 host computers connected to the Internet in Japan as of January 1997. And the estimate is that there are ten times as many users as host computers.
4. Corporate users are also high in Japan. According to the 1996 survey by Japan Electronic Mail Association, more than 50 per cent of Japanese companies have already introduced e-mail systems.
5. According to the WWW User Survey, based on European data from the Graphics, Visualization, & Usability Center (GVU) and Simba Information, Inc., for 1995 US data, and Commerce Net/Nielsen Internet Demographic Survey for 1996 US data.
6. For example, Amazon Books ([www.amazon.com](http://www.amazon.com)) handles over a million titles and manages inventory at lower cost. CD Now ([www.cdnow.com](http://www.cdnow.com)) also handles 165 000 CD titles.
7. For example, Andersen Consulting has a prototype agent software, BargainFinder (<http://bf.cstar.ac.com/bf/>), for comparing music CD prices at Web stores. It does not, however, guarantee finding the best offer, and, as of December 1996, some on-line CD shops are blocking the survey launched for this software.
8. See Jiro Kokuryo, "The role of 'Platform Business' in electronic commerce", *OECD Workshop on the Economics of Information Societies: Report on the Istanbul Workshop* Istanbul, 14-15 December 1995.
9. SET (secure electronic transactions) is a standardised protocol for safely transmitting sensitive bankcard information over public networks, which was jointly developed by MasterCard and Visa International. It uses public key encryption and authentication technologies.
10. Technology developments for the purpose of realizing secure data transmission are also going on. For example, in August 1996, the Cyber Business Association developed a system between credit card companies and merchants based on the HTTP and MOSS. The FEAL and ESIGN are being used as the encryption and authentication technology.
11. The term "key escrow" refers to the safeguarding of data recovery keys. Also used are "key archive", "key backup", and "data recovery system", as well as "trusted third parties", which is used particularly in Europe.

12. Dorothy E. Denning and Dennis K. Branstad, "Trusted Information Systems: A Taxonomy for Key Escrow Encryption Systems", March 1996, <http://www.cosc.georgetown.edu/~denning/crypto/Taxonomy.html>.
13. Cavazos and Morin, see note 9.
14. These proposed guidelines comprise a general explanation and definition of terms concerning CA, general management requirements for the operation of CA, requirements for specific business conducted by CA, and facility and system requirements. These guidelines were published in April 1997.
15. The ECOM of Japan has been drafting a model contract in electronic commerce for both consumers and shops. Its first version is based on the credit card type commercial transaction as exists within the current law and was published in April 1997. As the next step, the ECOM will draft a model contract in electronic commerce, including non-card type transactions and a proposal for the revision of the current related law.
16. The working group's most important function is the development and selection of standards within the Internet protocol suite. The IETF began in January 1986 as a forum for technical co-ordination by contractors for the then US Defense Advanced Research Projects Agency (DARPA). It worked on the ARPANET, the US Defense Data Network (DDN), and the Internet core gateway system. Since then, it has grown into a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
17. The bill was introduced by Representative Bob Francs (New Jersey) and Senator Dianne Feinstein (California).
18. Anne Wells Branscomb, "Privacy: At What Price?" National Privacy and Public Policy Symposium, November 1995.
19. Electronic money is value expressed in digital form. The US Department of the Treasury defines electronic money as follows: i) it purports to permit users, in some environments, to move funds electronically; ii) it relies upon advanced information technology to store, transmit, and receive representations of value; iii) it depends on modern developments in the science of encryption to provide security and upon public communications networks; iv) it is possible only because of the reduced costs and economies of scale that technological advances create; v) at some point, at least, it requires "loading" from funds held within the financial system ("Selected Tax Policy Implication of Global Electronic Commerce", November 1996).
20. In general, there are two categories. One is based on money flow, and payment systems are categorised as closed loop or open loop. So far, only MONDEX belongs to the second of these. The other is based on the timing of payment: pay before, pay now, or pay after.
21. Debit systems are often regarded as "pay now" systems, but there is always a time lag. Hence, they are here considered as "pay after".
22. Strictly speaking, cheques would fall into the "pay after" category. However the cheque system is based on demand deposit and, in this sense, it can be regarded as the same as the debit system.
23. Based at the OECD, the FATF was established in 1989 and has 28 members: 26 countries and jurisdictions (Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States) and two international organisations (the European Commission and the Gulf Co-operation Council).

24. But government initiatives do exist. For instance, MPT in Japan is developing technologies which enable more secure and reliable transmission of electronic money data on the Internet.
25. For example, Active Media estimates electronic commerce on the Internet at US\$ 436 million for 1995 and Forrester estimates it at US\$ 518 million for 1996.
26. Originally adopted in 1963, and revised in 1977, 1992, 1994 and most recently in 1995.
27. It also decided to create a group to oversee this work and to prepare a policy statement for the OECD Symposium on Electronic Commerce, held in November 1997.
28. There are initiatives for developing the next generation of Internet to overcome the risks on the current Internet. Internet Society has been working on the next generation protocol for Internet (Internet Protocol Version 6) and it has begun to be implemented. This version will improve the capability of handling the data transmission and enable service providers to provide better quality of service. In terms of a research agenda, the Japanese government (MPT) regards Ultra-high-speed transmissions of data, digital watermark technology for protecting IPR, security enhancement technology for data transmissions and reliability improvement technologies as the key features for the next generation of the Internet.