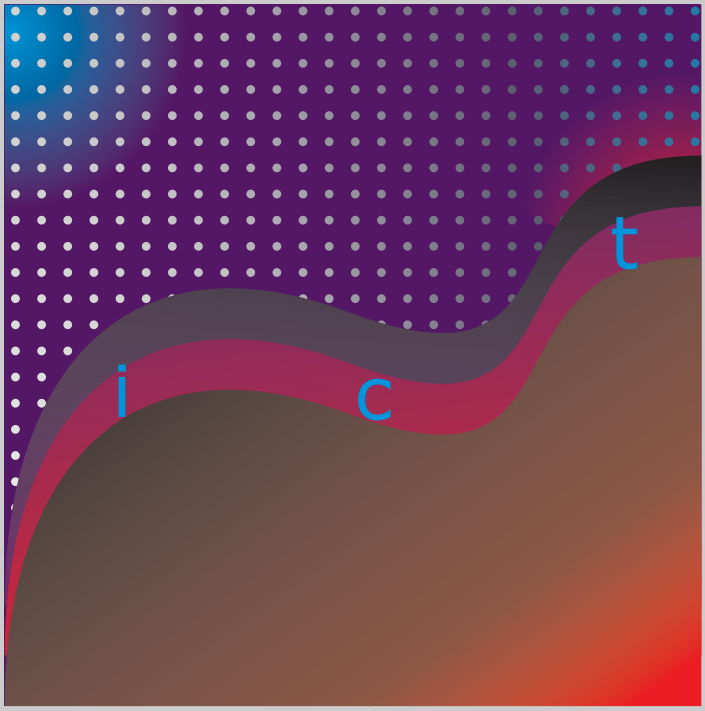
UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

E-COMMERCE AND DEVELOPMENT REPORT 2001

PART THREE

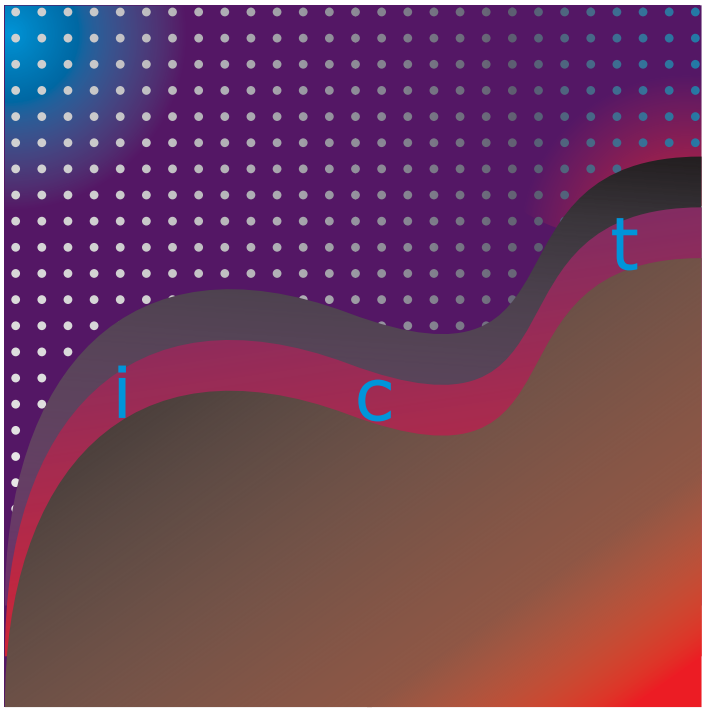
Prepared by the UNCTAD secretariat



UNITED NATIONS
New York and Geneva, 2001

Part Three

Electronic Commerce Environment and Practices



Chapter 6

OVERVIEW OF SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN ELECTRONIC COMMERCE

A. Introduction

The present chapter reviews some of the most pressing e-commerce issues, such as dispute resolution, applicable law, privacy and data protection, and provides an overview of other relevant legal and regulatory developments in the field of e-commerce, including e-commerce taxation. By e-commerce we mean not only contracts or transactions (both business-to-business and business-to-consumer),[1] but also torts. In addition, issues pertaining to applicable law, as well as to dispute resolution through courts and through alternative techniques, are analysed here. An attempt is made to explain both the status of the solutions currently available, as they may be applied by courts in some countries,[2] and the evolution of international negotiations on these matters.

However, first of all, the current discussion on whether the Internet constitutes only a space by and of itself which could be called "cyberspace" needs to be explained. This discussion is important because if the conclusion is positive, a number of consequences will follow. If the Internet is a space, it is a space without borders in which private international law does not have any meaning since the rules of private international law are made in order to deal with different legal systems and borders. As a result, the Internet should have its own uniform legal system specifically applying to it. Finally, there is no reason why private operators cannot be accepted as the source of norm together with, or in lieu of, States. Indeed, claims that the Internet is a specific and separate space leads to the assertion that States should not be trying to legislate on Internet issues.[3] However, most agree nowadays that States do have an important role to play even though an increased role is to be given to the private sector. Let us consider for a moment the most evident feature of the Internet — the one which gives cyberspace its very original nature — the domain name system.[4] It is true that the way in which Internet operators are allowed to access and operate on the Internet, i.e. through the domain name system, transforms the nationality question which is traditionally important for private international law. The generic top-level domain names (the .com, .net, .org, etc.) do not give any indication about the nationality or location of the "site" or the person who owns or operates it. Therefore, expressions such as "a foreign site" or "a domestic site" are without any meaning in the present context. Even national top-level domain names (e.g. the .fr for France, .us for the United States, .ch for Switzerland and .cm for Cameroon) are no longer meaningful. Indeed, most registrars in charge of the registration of national domain names do not block registration by domain name owners that are not domiciled in the country in question.[5] For example, a national or resident of the United States can register a domain name in France and vice-versa. In other words, the domain names are of no help for private international law issues. But, in our view, this is not enough to conclude that cyberspace is a space.

It is also said that the Internet is a space because it is an entirely decentralized system with absolutely no inherent control since it is a network of networks, linking two techniques — computers and telecommunication means. However, this description is purely a technical one and does not automatically mean that the Internet is a space. In fact, this technical description shows one thing: the Internet is a means of communication between human beings, or entities composed of human beings. Whether this communication is partially or entirely automated and software-driven does not alter the fact that the use of a software is possible only through the will of a human being or an entity.

The fact that the Internet is a means of communication does not mean that it does not have its own specific characteristics which will have an impact on private international law. Those characteristics will be rapidly reviewed here, first in order to determine

whether the Internet is international or transnational. Whoever sends data via the Internet, even to a local correspondent, may well be dealing with operators located in different countries, sometimes without knowing it. Therefore, the use of the Internet may mean that a transaction will be international even though both parties to the transaction are located in the same country. Thus, it may mean that a new concept of internationality is born, that of "electronic transaction". As soon as the electronic communication system is used, the transaction is an electronic transaction and may necessitate the application of specific rules.[6]

Cyberspace is also characterized by its ubiquity and multiplicity since the Internet allows a person to reach out to a multitude of persons at the same time. This has an immediate consequence. At first sight, because the Internet covers the whole world, each of the 200 or so countries around the globe may have a claim to apply its own legal system to an Internet transaction. Instead of there being the vacuum of which some may have warned a little too quickly,[7] there are in fact too many potentially applicable legal rules. Because this result is impossible to accept, there must be a shift in the analysis. We need to recognize that there are only two relevant contact points: the places where the parties to the transaction are located.[8] With the Internet, it is necessary to accept that the place of conclusion or the place of enforcement of a transaction, traditionally used in private international law analysis, is no longer pertinent.

A third characteristic of great importance is the extreme rapidity of Internet communications. This is particularly crucial for torts. Indeed, harmful actions in cyberspace may have more damaging effects than in real life, just because of this factor. One immediate consequence for dispute resolution follows from this: courts must act more quickly and international judicial cooperation is absolutely essential.

A fourth characteristic is the very low cost of market entry. It is therefore very easy for a one-person shop to start a multinational activity as long as that person organizes his or her logistics carefully with independent partners. Nowadays, the expression "transnational enterprise" or "multinational enterprise" has another, completely different meaning. As well as referring to the traditional giants with a bricks and mortar presence in many States, it can refer to very small entities dealing via the Internet. This will necessitate a new analysis of the concept of "consumer". This aspect of the problem will be discussed in Section B, paragraph (c) (i).

Finally, a new phenomenon is starting to spread through Internet activities which is of a major concern particularly for torts. Although the Internet was initially created as a transparent network in which each and every participant was identified and identifiable, many claim nowadays that they enter cyberspace and deal on the net with full anonymity.[9] Again, this is contrary to the original philosophy behind the Internet but does not yet seem to cause much concern in international forums. This will be discussed mainly in Section B, paragraphs (d), (e) and (f).

In the preparation of this chapter the work done by a number of organizations (either intergovernmental or non-governmental) was taken into consideration: the preliminary draft Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters[10] and other work done by the Hague Conference;[11] discussions and proposed texts adopted under the auspices of UNCITRAL; discussions and recommendations adopted under the auspices of the OECD; work done by the European Union and studies prepared by the American Bar Association (ABA), discussing a range of legal issues associated with jurisdiction in relation to the needs of electronic commerce.[12] In addition, we have studied declarations released by professional interest groups such as the Global Business Dialogue in Electronic Commerce (GBDe)[13] and the Internet Law and Policy Forum (ILPF).[14]

B. Dispute resolution

When legal relations are essentially based on contracts, the role of dispute resolution mechanisms is absolutely crucial. Traditional means of dispute resolution include recourse to national courts, but arbitration and mediation have always had their role to play in different cultures and at different times. Arbitration has had a renewed preponderant role in international trade, at least for the past half-century. Since e-commerce is based on party autonomy (at least in business-to-business (B2B) transactions), arbitration may be the preferred means for dispute resolution[15] in this area as well. However, there are cases in which arbitration or other alternative dispute resolution (ADR) mechanisms are not suitable[16] or may not be working. Thus, it is important that courts of law be available and clear rules of jurisdiction be

offered to private operators. This is usually known as the "last resort rule".

1. Court jurisdiction

In the last few years, attention was focused on a major project undertaken by the Hague Conference on Private International Law to propose a worldwide convention on jurisdiction and foreign judgements in civil and commercial matters.[17] This project tried to use the very successful experience of a number of European countries with the Brussels[18] and Lugano[19] Conventions on the same issues. Although the Hague draft[20] did not fully take into consideration potentially specific e-commerce needs, several subsequent meetings discussed them. The following discussion will draw both on the work done at The Hague and on the work subsequently done in a number of other forums.[21]

(a) Choice of court

Since e-commerce has increased the need to rely on party autonomy, choice-of-court clauses become central to any discussion of court jurisdiction. It is essential that national legal systems clearly provide for rules on which parties can rely in order to ensure that their choice-of court-clauses will be deemed valid. Uncertainty in this respect is detrimental to the trust which private operators will have in the judicial and legal systems of a particular country. This is why it is so important that countries develop rules. The best way would be to develop them collectively, in an international forum. But if this is not possible, countries should at least develop a set of rules of their own.

An example of a possible rule to be adopted by States is the proposed Article 4 of the preliminary draft Hague Convention, which reads as follows:

> "1. If the parties have agreed that a court or courts of a Contracting State shall have jurisdiction to settle any dispute which has arisen or may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction, and that jurisdiction shall be exclusive unless the parties have agreed otherwise. Where an agreement having exclusive effect designates a court or courts of a non-Contracting State, courts in Contracting States shall decline jurisdiction or suspend proceedings unless the court or courts chosen have themselves declined jurisdiction.
>
> 2. An agreement within the meaning of paragraph 1 shall be valid as to form, if it was entered into or confirmed -
>
> a) in writing;
>
> b) by any other means of communication which renders information accessible so as to be usable for subsequent reference;
>
> c) in accordance with a usage which is regularly observed by the parties;
>
> d) in accordance with a usage of which the parties were or ought to have been aware and which is regularly observed by the parties to contracts of the same nature in the particular trade or commerce concerned.
>
> ...."

The important features of this rule are as follows:

1. The jurisdiction conferred on the court chosen by the parties to the agreement is exclusive unless the parties have expressly provided otherwise. This rule, which is not yet accepted all over the world,[22] seems to be preferred by practitioners since it provides more predictability and certainty.
2. The effect of a court selection clause on non-contracting States is relevant only when the rule is inserted in an international treaty. Obviously, if the rule is adopted by a national legislative body, this part of the rule will have to be deleted. It may be replaced by a direction given to national courts that in the event that it is seized of a dispute when a choice-of-court clause grants jurisdiction to a court of a foreign country, the court seized suspends the proceedings unless the court of the foreign country has declined jurisdiction.
3. As far as the formal validity of the clause is concerned, subparagraph (b) is the most relevant for e-commerce purposes since it accepts the validity of electronically formed agreements. This provision is in conformity with the most advanced state of the art in this respect. This was the conclusion of the Geneva Round Table,[23] and it did not give rise to any criticism in the forums where jurisdictional rules were discussed. The language

is that adopted by the UNCITRAL Model Law on Electronic Commerce, of 1996.

4. Finally, it should be noted that the provision does not include a rule on the substantial validity of the choice-of-court clause.[24] This is due to the fact that in B2B transactions there is an assumption that the contract is executed by equal partners. Thus, the protection of one partner against the other may not be necessary. This is different in relations between a professional and a consumer, as will be discussed below. However, in electronic commerce there may be a need to reassess the notions of "equal partners" and "consumers". This will also be dealt with below.

(b) Business-to-business contracts

This is one of the most difficult issues in international jurisdiction. Before we look at potential provisions relating to it, it is important to stress why a specific business contract jurisdiction has been considered necessary in the past (in addition to the defendant's domicile or habitual residence).[25] When deciding on court jurisdiction rules, legislators try to find the most suitable court with regard to the parties and to the claim, taking into consideration in particular the location of the evidence. In the real world, the most frequently used contract, that of sale of goods, may lead to disputes involving most of the time defective or non-conforming products. Thus, very often, it is easier to grant jurisdiction to the court in the location where these products are located, which is usually the court where the contract was performed or was to be performed.

The preliminary draft Hague convention reflects this kind of thinking, since it provides as follows in Article 6:

"Article 6. *Contracts*:

A plaintiff may bring an action in contract in the courts of a State in which:

(a) in matters relating to the supply of goods, the goods were supplied in whole or in part;

(b) in matters relating to the provision of services, the services were provided in whole or in part;

(c) in matters relating both to the supply of goods and the provision of services, performance of the principal obligation took place in whole or in part."

This rule is slightly different from the rule in the Brussels and Lugano Conventions and in the European Regulation of December 2000. But it stems from the same reasoning as that explained above. It is important to reassess this rationale in view of the specificity of electronic commerce. But before doing so, it should be understood that any contract jurisdiction is a jurisdiction by default, i.e. a jurisdiction for all contracts in which the parties have not taken the precaution of including a valid choice-of-court clause.

Recent discussions show that three fundamental issues arise in e-commerce. The first is need to distinguish between contracts which are concluded electronically but performed offline (see (i) below), and contracts which are both concluded and performed electronically (see (ii) below). The second issue is the identification and location of the parties to the contract ((iii) below). The third issue is the distinction traditionally made between products and services. As this will be raised during the discussion about contracts which are to be concluded and performed online, it will be discussed here in that context.

(i) Contracts concluded online and performed offline

Although it is customary in many e-commerce discussions to stress that, as far as possible, rules for online dealings must not be different from those applied to real-life dealings, there is one exception which seems to be accepted: special rules are needed when the contract is performed entirely online. Indeed, in the latter case, the link of the contract (and the potential dispute arising out of it) to a specific territory does not exist separately from the location of the parties to the contract. This will be discussed below, together with the identification of parties.

For the time being, the present discussion is limited to one very important consensus: any analysis of a potential jurisdictional rule for contracts must separate contracts performed offline from those performed online. A rule such as the one in Article 6 of the draft Hague Convention may be satisfactory when the contracts in question are concluded electronically, although performed offline.[26] In that case, it seems to be agreed that no special provision is necessary because the traditional approach defining jurisdiction, with a focus on the place of performance, is still pertinent. However, for contracts which are concluded and performed online, the question of a potential supplementary clause arises. It may be con-

sidered, at the end of the analysis, that the defendant's forum coupled with the forum chosen by the parties may be sufficient for the needs of e-commerce. However, before this conclusion is reached, a thorough analysis of the needs must be conducted.

(ii) Contracts concluded and performed online

The question that arises with regard to these contracts is whether the traditional distinction between products and services is a realistic one for electronic transactions. This is a subject that is still debated in the World Trade Organization. In the European Directive on Electronic Commerce,[27] however, it has received an answer. For the European Community, the subject matter of an electronic exchange is primarily information, and this information has to be treated as equivalent to services. However, it is not entirely clear whether the description of an online contract is absolutely necessary for the definition of a jurisdictional rule. In any case, whether one accepts that an online contract is one for "services" or that no description is necessary, it may be said that the distinction proposed by Article 6 of the draft Hague Convention is not pertinent for contracts performed online.

One should focus on finding the most appropriate court, taking into consideration all the specific factors mentioned above which make the Internet a specific means for conducting business. With this in mind, it is clear that the place where the contract is performed is not relevant in the online world. Many "places" have been proposed, for example where the server's computers are located or where the Internet service provider (ISP) is located. But none of them are relevant when the contract in question does not involve the server or the ISP. In fact, the analysis leads us back to a fiction: the contract is deemed to be performed where either of the parties is located. This is why the identification and the location of the parties are of such importance in an Internet transaction.

(iii) Identification and location of the parties

All documents published in the past two years or so emphasize the crucial importance of the identification and location of the parties when one is dealing over the Internet.[28] As far as the identification of the parties is concerned, it is assumed that no request for anonymity can seriously be made when the transaction in question is a commercial one. Whoever takes the risk of dealing anonymously over the net runs the risk of not having access to the courts on a favourable basis. Dealing under cover of anonymity may be a preferred way of protection for some operators. However, it cannot be used afterwards to claim court jurisdiction detrimental to the other party.

The location of the parties must be defined as the place where the party has its bricks and mortar location. All agree nowadays that a site is not a location per se.[29] The discussions under the auspices of the Hague Conference seem to show that a preferred approach could focus on the concept of presumption. This could be summarized as follows:

(a) Maximum use should be made of freedom of contract (party autonomy);

(b) Statements by the parties to the contract concerning their identification and location, during the negotiation and in the contract itself, should be used for jurisdictional purposes;

(c) If a provider of services[30] wants to know in advance which court may have jurisdiction to settle any disputes he may have with his co-contractor, he will have to ask him for details of his location;

(d) The co-contractor will then be bound by the information he supplies concerning his location, and the jurisdictional rule will apply in respect of this information;

(e) In the event of difficulties due to false information, error or lack of information, the specific jurisdictional rule will no longer apply. In such a case, the traditional defendant's forum or the branch forum will be the only jurisdiction available.

A system which is based mainly on statements made by the parties may present some disadvantages, particularly the abuses which may arise from it. It is quite conceivable that one of the parties to the contract may declare that he or she is situated on the territory of a given State, solely in order to confer jurisdiction on the courts of that State for reasons entirely unconnected with the contract itself, such as the way in which those courts operate, the rules of procedure they follow or the rules of evidence or conflict of laws used in them. Of course, this danger is not entirely absent from the system proposed. However, it is the role of any co-contractor to be vigilant and to check, if necessary, that the information supplied by the other party matches the true situation.

In the unlikely event that the prudence of the co-contractor has not been sufficient, the court seized of the dispute may still have the possibility to use its discretion to refuse jurisdiction if it finds that it is not the most appropriate forum. It is true that not all systems in the world provide for a *forum non conveniens* theory to be applied by their courts. But it seems that there is a consensus nowadays for some kind of *forum non conveniens* to be applied in international cases.

(c) Consumer contracts

(i) A new concept of "Consumer"?

One of the most difficult issues in e-commerce discussions is the definition of a consumer. In most legal systems, a consumer is defined as an individual acting for personal or family purposes, and thus any enterprise, undertaking or company and any person having a business purpose[31] is excluded from the definition.

The characteristic feature of the Internet is that it greatly lowers the cost of entry into the market. Thus the size of an undertaking which may start an Internet activity has been reduced to an unprecedented level. An individual is now able to conduct a multinational business from a one-man shop as long as it has secured the proper contracts for goods and delivery. Thus, two questions must be asked. First, does this very small undertaking deserve protection in the online world? Secondly, when dealing with its own consumers, is this small undertaking at arms length or do those consumers still deserve protection?

Another factor also is adding some complexity to the discussion. Consumers now have at their disposal software products by which they can search the web and find the best offer for a service or a product they are looking for. These are known as BOTs (short for robots). Some argue that using a BOT gives the consumer a sophistication transforming him or her into a much more powerful contractor. Thus, the cyber-consumer, using a BOT, would not need any more protection.[32]

It is impossible to give an answer to these questions for the time being, as the debate is still raging. Consumer protection groups around the world claim the same protection in the online environment as in the real world,[33] whatever the size of the business.

At an early stage, many Governments declared that consumers must be protected in the same manner whether dealing over the Internet or in the real world. However, interest groups representing corporations have argued that if consumers are protected by the possibility of their suing from home and by the application of the relevant rules of their domicile, Internet operators on the other hand are not at all likely to be knowledgeable about all the laws in the world and to be able to defend themselves in all the courts in the world. Their conclusion therefore is that we should do away with the rules protecting consumers.

Although it is not claimed that it is easy to give an answer, a few guidelines may be kept in mind for further reflection. First, it may be possible to agree on a new definition of a sophisticated consumer who may need less or no protection in the online world. In Europe, in the financial service sector, a concept of "sophisticated investor" has been used for a number of years[34] which may be used as a starting point for a definition of the cyber-consumer. Second, Internet operators make considerable savings when they start their business over the net and could be asked to use part of those savings to buy some special insurance coverage for their Internet dealings.[35] Third, operators may define their price policy in order to offer different prices to consumers and to professional buyers. Knowing that it is more costly to sell to a consumer (if current rules still apply), the buyer would be able to buy at the price he prefers: either he saves money immediately knowing that he will not have much protection if something goes wrong, or he pays a higher price in order to be better protected.[36]Fourth, operators should make use of jurisdiction avoidance. This means that if they feel unable to sell in one jurisdiction, when a consumer declares that he/she is located in that jurisdiction, a notice should appear on the site to the effect that no sale may be concluded in that jurisdiction. If the consumer decides to make a statement that he/she is located in a different jurisdiction, he/she will not be able to claim, later on, protection of his/her real jurisdiction.

(ii) Any place for party autonomy?

Referring to the Hague project is not the best way to discuss the potential place for party autonomy in business-to-consumer transactions. As it stands now, the rule in Article 7[37] does not leave room for party autonomy except under very strict conditions which are not pertinent to online dealings. In fact, the whole rule was prepared without taking into account the issues relating to electronic commerce.

The same applies to the new European Regulation which will replace the Brussels Convention.[38] That was why, before the text could be finally adopted and published in the *Official Journal of the European Communities*, an agreement was reached between the Council and the Commission so that work would continue to develop ADR systems within the European Union. This shows the importance currently given to ADR in business-to-consumer relations even in a system traditionally unfavourable to ADR such as the European legal system.[39]

Almost all international meetings held over the past two years or so have shown that ADR or online dispute resolution (ODR) could solve many disputes at an early stage without use of the court system. Once this has been said, all the rest needs to be defined. How will the ADR/ODR system be linked with the court system? What procedural rules will be applied by the ADR/ODR service providers? Will the consumer be able to choose an ADR/ODR system? If not, how will the system ensure that the ADR/ODR system chosen by the company, co-contractant to the consumer, is independent and fair? These are only a few of the numerous questions to be asked.[40]

As regards the validity of the choice-of-court clauses in business-to-consumer contracts, it is as controversial as the use of ADR. The traditional European attitude towards such clauses in consumer contracts has always been very restrictive.[41] Similarly, a number of courts in the United States have recently refused to uphold choice-of-court clauses in Internet contracts.[42] However, it is still too early to say that a trend has already been established in that country. During the Hague discussions, several proposals led to a solution whereby choice- of- court clauses would be valid if the State of the consumer's habitual residence accepted them as valid. There would be an express statement by the relevant country in its legislation. This solution might be a means of achieving consensus by maintaining the status quo but does not solve the actual issue.

(iii) The present solutions

Whatever the place of ADR/ODR, there will always be some role for courts. Whether it is a last-resort role if the ADR system does not work, or whether it is the "juge d'appui" role in aid of the ADR system, there must be a definition of a jurisdictional rule for courts in business-to-consumer contracts. At present the systems applied in various countries differ.

In the United States, the definition of jurisdictional rules specifically for consumers is rendered unnecessary by two factors. Indeed, rules on jurisdiction are very flexible in that country. They assume, as a starting point, that the plaintiff's choice of a forum must be respected unless it is unfair to the defendant. From that point, courts have developed an ever-increasing body of case law defining what set of circumstances is fair or unfair to the defendant. In that context, they do not need a specific starting point for consumers, and it is only the set of circumstances acceptable from the defendant's point of view that is different. But the reasoning is the same in B2B and B2C contracts.

In Europe, because the starting point is just the opposite, i.e. the plaintiff's forum is used only in exceptional circumstances as a derogation from the "normal" forum — that of the defendant — special rules have developed for consumers. This was true in the Brussels and Lugano Conventions. It is also true in the new Regulation, although the content of the rule has been slightly amended to include some kind of "targeting".

The present wording of Article 7 of the Hague draft requires all the conditions in its subparagraphs (a) and (b) to be fulfilled in order for the consumer to initiate proceedings in the courts of his or her habitual residence. Those conditions are:

(a) The conclusion of the contract must be linked to the activities of the business in the State of the consumer's residence, or directed at that State in particular by soliciting business through means of publicity;

(b) The consumer must have taken the necessary steps to conclude the contract in his or her State of residence.

The main question is whether placing material on an Internet site is regarded as advertising by the business. If so, the first condition will always be met. Thus, it does not seem to have any further relevance for the purposes of electronic commerce. As for the second condition, present-day means of telecommunication enable a consumer to conclude the contract in a place other than his/her habitual residence, but this does not have any particular implications for the purpose of deciding which courts have jurisdiction.

In order to solve these difficulties there must be a clear assessment of the interests at stake. States want to encourage electronic commerce, especially in the area of consumer contracts. Enterprises which offer

goods and services via the Internet may be very small businesses, which need to be encouraged. From another point of view, it is clear that in the context of trade with consumers, the Internet will take off only if consumers themselves have confidence in it. And one of the essential points for consumers is to make sure that if a problem arises in their relationship with a business, they can obtain redress both rapidly and cost-effectively.

Would the inclusion of targeting be of some help? If the enterprise has specifically targeted consumers in a particular country, it would be logical to decide that the courts of that country have jurisdiction for consumers residing on its territory. On the other hand, if the business uses an unsophisticated site, i.e. one which does not make it possible to target certain consumers, the result will be that no particular conclusion can be drawn as regards jurisdiction. This development is not unanimously endorsed as yet.[43] In fact, we find the concept of targeting somewhat inconsistent with the fact that the Internet allows any service provider or seller to propose services and goods all over the world with no restriction except possible filtering of accessibility by local authorities. Therefore, it seems not "natural" in the cyber context to require some targeting. In addition, the circumstances usually considered in order to assess whether there is targeting or not may not be very determinative.[44]

In any event, even if the rule of default jurisdiction is kept for the consumer's habitual residence, the same principle as the one discussed for relationships among businesses would apply to the identification and location of the parties to the contract. The consumer would be required to identify his or her habitual residence in order to bring the jurisdictional rule into play.

(d) Torts

The major difficulty with tort[45] committed via the Internet is twofold: (i) it is very difficult to discover who committed the tort; and (ii) it may have had an immense impact on the victim before the latter was able to stop it. Thus, tort jurisdiction, even if needed, may have little impact unless ISPs[46] provide cooperation.

The difficulty is also that the tort impact or effect may be all over the world as some recent cases have demonstrated. Although they concern criminal matters, the recent Italian Supreme Court decision[47] and the French Yahoo case are interesting for our analysis.[48] The latter is particularly important since after defending fully in the French case and deciding to discontinue the harmful acts which were the very core of the French action, Yahoo! Inc. nonetheless decided to continue the action filed in a San Jose (California) court. The core of the United States action was to ask the United States court to rule that France did not have jurisdiction in that particular dispute. This cross-Atlantic battle over jurisdiction shows how urgent it is to have an international agreement on jurisdictional rules.

Italy and France have asserted jurisdiction against a foreign corporation on the basis of the harmful effect felt in each of those countries through websites owned by that foreign corporation. In each case, the remedy sought was an injunction to stop the harmful acts. Although the remedy was one that could have also been sought equally in a civil or commercial action, it is important to note that the harmful acts did violate criminal law in both countries. It is not certain whether the French and Italian courts would have asserted jurisdiction for a similar injunction if the dispute had been purely civil or commercial, unless some other links than the pure accessibility of the site was demonstrated between the circumstances and the forum.[49] At any rate, these two cases do pose the very questions which need to be answered when dealing with Internet tort jurisdiction.

Although it has been the subject of some criticism, Article 10 of the Hague draft could be taken as a starting point for discussion of what could be an internationally agreed rule.[50] The major feature of the rule is that it grants jurisdiction to the court of the place where the act takes effect (the place where the injury occurs), unless it can be shown that the perpetrator could not reasonably foresee that or a similar consequence. The courts of the place where the injury occurs will also be competent to rule on all the injury suffered anywhere in the world by an injured party, provided that party is a habitual resident of the State in which the court seized is situated. In all other cases, the jurisdiction of the courts of the place where the injury occurs is limited to injury suffered on their territory.

It may be pointed out that in the cyberworld the proof required in Article 10.1(b) can never be adduced. Internet sites, it is true, operate somewhat like newspapers which are distributed worldwide. A person

who uploads defamatory information onto a site can reasonably foresee that it may be read anywhere in the world. The only unknown factor is the number of "copies" distributed (to pursue the analogy of the printed press).

Another criticism has been voiced about the use of the place of the wrongful action since that place specified in Article 10.1 a) is very difficult, if not impossible, to identify with the Internet. Thus, we may need to equate that place with the place where the perpetrator is located. However, in a tort action this would lead automatically to the defendant's forum which is otherwise made available in the Hague draft. Thus, it is questionable whether, in this context, we need a separate rule also pointing to the defendant's forum but through a different route. The second inconvenience resides is that it is very easy for a defendant to locate in a friendly jurisdiction with a judicial system which is not functioning well. This may be of concern in the drafting of such a rule.

In consequence, it appears that offences committed through the Internet make it necessary to have an alternative forum to the defendant's forum, but one which also has general jurisdiction (i.e. a court which can deal with injury suffered everywhere). The rule in Article 10, paragraph 4, of the preliminary draft was therefore welcomed by some as a particularly important one in the electronic context.

Since discussions on the Hague draft are still continuing, it is difficult to predict at this stage whether a common understanding and agreement will emerge.

(e) Branch offices

Jurisdiction based on a branch or business office is present in many legal systems. It is assumed that a corporation that uses a branch office in a country other than the one in which it conducts its main business or in which it is incorporated must be answerable in the courts of the country where the branch is located for disputes arising out of the activity of the branch. The same idea underlies some of the jurisdictional rules applied in the United States on the principle that a corporation which avails itself of the economic environment and the rules of a State has implicitly agreed to be accountable in the courts of that State.

There are two main questions regarding branch office jurisdiction in the context of electronic commerce:

1. Can an Internet site be regarded as a branch office?
2. Does the reply to the previous question depend on the level of interactivity of the site?[51]

It can be said that on the first question a clear consensus has already been reached which seems to cover a broad range of stakeholders. At a regional level, the European Union has clearly stated that a website is not a branch or establishment for any legal purpose.[52] This conclusion was also reached by experts, meeting under the auspices of the Hague Conference.[53] More recently, the OECD stated that a website is not a permanent establishment within the context of the model tax convention.[54]

The answer to the second question is also clear: whatever level of interactivity of the website, it will not change the conclusion reached above. However, if a site is an interactive one, it may lead countries which apply a doing-business concept for court jurisdiction to assert jurisdiction as long as the interactivity could be seen as a clear link with the State whose court asserts jurisdiction. On this issue there is a long line of cases in the United States showing how jurisdiction is asserted on the basis of an interactive site. This line of reasoning is difficult to apply in practice. It necessitates a very sophisticated reasoning both for the judge and the parties. Because of its casuistic nature it may not be predictable for parties. It involves an appreciation of the targeting concept. But it is difficult to agree on what targeting is and how much targeting is necessary in order to justify a court's assertion of jurisdiction.

(f) Is a domain name a real property?

This question is posed directly because of the Anticybersquatting Consumer Protection Act adopted in the United States on 29 November 1999.[55] It is not our aim to analyse all the provisions of the Act[56] but only to show how its jurisdictional provisions were recently interpreted and the difficulties in applying it in international cases.

The Act is mainly aimed at providing a forum and an action to a plaintiff whose intellectual property rights are violated by a domain name. Although the Internet Corporation for Assigned Names and Numbers (ICANN) has established a quasi-arbitration system to resolve such disputes[57] and many cases have already been decided under it by one of the three accredited dispute resolution service providers, the

United States thought it was not sufficient and adopted the above-mentioned Act.

The Act provides that in a case where the defendant cannot be found, the plaintiff may file a request for an injunctive relief before the court of the place where the domain name is registered. The court jurisdiction is purely *in rem*. In order to provide for this jurisdictional ground, the Act proceeds with two legal fictions: (i) a domain name is a property; and (ii) the location of that piece of property is deemed to be at the place of registration.[58]

This legislation is well intended in principle since it specifies that the *in rem* jurisdictional ground can be used only if the defendant cannot be found, i.e. if no personal jurisdiction (*in personam*) can be asserted. The American legislators wanted to combat trademark infringement by anonymous cybersquatters who, in bad faith, register a domain name that violates a valid trademark but then prove to be beyond the reach of an action. However, one of the first decisions rendered under this Act in an international context is worrying, and it may be of interest in the context of this chapter to discuss it in a little more detail.

The case involved two Internet domain names "Technodome.com" and "Destinationatechnodome.com" which the plaintiff, Heathmount A.E. Corp, claimed infringed its trademarks.[59] Both the plaintiff and the defendant (the owner of the domain names) were Canadians having places of business in Canada. There was no doubt that, under Canadian jurisdictional rules, there was *in personam* jurisdiction in Canada. However, the court in Virginia asserted *in rem* jurisdiction under the Act for two main reasons: (i) there was no *in personam* jurisdiction in the United States; and (ii) Canadian law did not provide a body of law similar to the United States Act.

It appears that the Virginia court interpreted the Act without taking into consideration the fact that *in personam* jurisdiction was available in Canada for a dispute between two Canadian citizens or legal persons. In addition, the second reason offered by the court for asserting jurisdiction was based on the lack of equivalent legislation in Canada. The court never considered the possibility that a Canadian court would apply the United States law. This lack of international perspective when dealing with Internet issues might lead to confusion and more forum shopping.

As a general and practical principle, *in personam* jurisdiction must always be preferred to an *in rem* jurisdiction since it allows the court to solve the entire dispute between the parties. Usually, it also facilitates enforcement of the decision.

2. Alternative dispute resolution

Because the judicial systems around the world face new challenges at a time when they have not entirely resolved old ones, private sector operators call for an increased role for alternative dispute resolution offered by private enterprises. We have already mentioned the discussion about the potential role of ADR/ODR in a business-to-consumer relationship. We will now explain briefly the type of services which are already offered and the ongoing discussions on a potential international legal framework for these services.

(a) Developments in different organizations

Numerous meetings have already taken place in various forums to develop alternative dispute resolution mechanisms with an emphasis on online techniques.[60]

(i) Meeting on alternative methods of dispute resolution, Brussels, March 2000

At the initiative of the European Commission, a meeting was held in Brussels on 21 March 2000 to deal with the alternative methods of resolving online disputes between consumers and businesses. The documents made available to the participants, and the report of the meeting, are available on the site dedicated to this Working Group.[61]

The main conclusions of the meeting can be summarized as follows:

1. Confidence in e-commerce will be achieved only if clear sets of rules are approved by all stakeholders at a European level, if not at an international level;
2. Any ADR/ODR system must be regarded as visible and transparent, accessible, affordable and efficient for users;
3. The decision taken or the transaction concluded after an ADR process must be fair;
4. The finality of the decision or transaction remains to be discussed, particularly with regard to the consumer;

5. ADR systems must be independent and impartial; and

6. Any work in this area must promote cooperation and coordination between consumers, companies and public institutions.

After the meeting, the European Commission launched the ECODIR project, which is an attempt to define a complete framework for a European ADR system. The project, which includes technical, legal and policy aspects, should be completed in the spring of 2001.[62]

(ii) Meeting organized by the United States Federal Trade Commission and the Department of Commerce, Washington DC, June 2000

The aim of this meeting was to identify the interests involved in electronic commerce when the transaction is concluded between a business and a consumer. Many ADR service providers attended the meeting. The participants discussed which avenues should be explored in the future to give confidence to consumers, and the incorporation of alternative methods into a complete dispute resolution system, specifically in relation to court proceedings.[63]

The meeting was a unique opportunity to gather first-hand information on the services which are already available and the principles on which they act. The conclusions of the meeting may be summarized as follows: (i) the ongoing process of trying to find global solutions must be favoured and emphasized with all stakeholders present (private and public sector alike); (ii) the technological innovations which were presented during the meeting must be developed further since they will help a more user-friendly set of systems to be offered; (iii) "one size won't fit all", i.e. ADR/ODR systems to be developed must be tailored to deal with certain types of disputes so that they are best adjusted to their specific needs; and (iv) fairness and effectiveness are the two main features which any ADR system must aim at.

(iii) Joint meeting between the OECD, the Hague Conference and the ICC

In December 2000, a meeting was held at The Hague under the joint auspices of the OECD, the Hague Conference on Private International Law and the International Chamber of Commerce (ICC).[64] It allowed stakeholders to present progress made in the course of the year regarding ADR/ODR services from different angles: cultural, political, economic, legal and policy. Issues were discussed from the point of view of consumer contracts and privacy protection. The role of ADR/ODR was again emphasized, but no firm conclusion could be drawn from the discussion about the actual place of ADR/ODR as a sole recourse or as part of a more complete system including recourse to courts.

(b) The potential place of ADR in the global system

In our view, there is quite a pressing need to develop ADR/ODR systems adapted to Internet dealings both for business-to-business contracts and for consumer contracts. Several important statements have been released by some countries on this issue. The United States–European Union joint statement is an important one and represents the strong influence of private sector interests.[65] It focuses essentially on consumer confidence and will therefore be dealt with in paragraph (ii) below, after a few words have been said about ADR/ODR in B2B relations (paragraph (i)).

(i) Business-to-business contracts

In business-to-business contracts, it is not difficult to see how ADR/ODR will continue to have a major role to play. Mediation and arbitration had already become preferred means of dispute resolution in the B2B context long before the Internet was used. The Internet will only increase the need to use ADR.

The legal norms applicable to ADR all over the world have developed and are firmly established thanks to the considerable work done by the United Nations Commission on International Trade Law (UNCITRAL).[66] In addition, arbitration is well established around the globe. What is needed is some adaptation work to use increasingly electronic means for the arbitration process. This will be done in the course of time. It is already clear that the writing requirement of Article 2 of the New York Convention can be met by an electronic functional equivalent. Also, there is a consensus that the place of arbitration may be used as a legal fiction and does not need to be purely a geographical place.[67]

However, there is one aspect which has not been developed so far in the area of mediation. The result of successful mediation is a settlement. In most legal systems, a settlement is considered to be a contract. Therefore, if the settlement needs to be enforced

outside the country in which it was reached, the rules applicable to arbitral awards or court decisions are not applicable. In addition, since the settlement is a contract, no automatic enforcement can be obtained. A court procedure may be necessary. This seriously impairs the value of a settlement. Thus, we think that work is needed on unified rules for transborder enforcement of settlements obtained through an out-of-court mediation system.

(ii) Consumer contracts

As explained above, the most controversial aspects of ADR/ODR concern consumer contracts. The joint statement by the United States and the European Union may set an important framework for further discussion at an international level. Part of the statement reads as follows:

"We now reaffirm these important goals and objectives, including the agreement to provide "active support for the development, preferably on a global basis, of self-regulatory codes of conduct and technologies to gain consumer confidence in electronic commerce". We also reaffirm our commitment to the OECD Guidelines on Consumer Protection in the Context of Electronic Commerce issued in December 1999.

Our common aim is to help generate consumer confidence, which is necessary for open, competitive, and cross-border electronic commerce. Ensuring consumer protection and generating consumer confidence requires a combination of private sector initiatives and a clear, consistent and predictable legal framework.

The means of building consumer confidence and consumer protection in shopping online is good business practice and enforceable self-regulatory programmes such as codes of conduct and trust marks. Key elements to building consumer confidence and consumer protection also include security and confidentiality, respect for privacy, high standards of customer service, timely delivery, full and fair disclosure of information, and responsiveness to complaints.

We recognize that consumers should have meaningful access to redress, consistent with the applicable legal framework and should be protected from fraudulent, deceptive, and unfair practices.

The Internet, which can support the growth of cross-border consumer transactions at unprecedented levels, poses challenges to the existing legal framework. The issues of applicable law and jurisdiction will be difficult to resolve in the near term, but solutions at the international level would help to achieve our shared goals of global electronic commerce growth, consumer confidence and predictability."

Most agree that any ADR/ODR system proposed for consumer disputes must be independent and impartial, transparent, efficient, legal, fair, and embody a procedure which fully respects the principle of contradiction.[68]

Some propose that the systems should be taking as a model the system embodied in the Uniform Domain Name Dispute Resolution Policy (UDRP)[69] of ICANN.[70] We do not deny that the UDRP rules may be of interest when reflecting on ODR. However, we think that these rules can only be a starting point and cannot be considered to be a model. The main reasons for that assertion are as follows: (i) the UDRP system covers a very limited area of substantive law, namely cybersquatting, i.e. the violation of trademark rights by domain names, whereas consumer disputes are much more diverse and may relate to different kinds of damages and different kinds of actions; (ii) the UDRP contains specific rules of evidence, whereas it is not possible to set in advance rules of evidence in a context where actions are diverse; (iii) the UDRP includes a limited sanction if the violation has been recognized, whereas sanctions in consumer disputes may be monetary and hence present specific difficulties of enforcement; and (iv) the UDRP contains its own enforcement rules, whereas such rules will need to be different depending on the type of sanction.

Disagreement is still strong on the following aspects: (i) How costly should the process be for consumers? (ii) Who will choose the ADR/ODR system? (iii) Would the consumer be obliged to go first to an ADR/ODR system before having recourse to court? (iv) If so, would the ADR/ODR process be limited in time? (v) How binding would the result of the ADR/ODR process be? Would it be binding only on the business? Or on both parties?

Most of the systems available in Europe, do not preclude the consumer from having recourse to the court system if the consumer disagrees with the decision rendered or the solution proposed by the ADR system. However, it should be noted that two systems propose an arbitration mechanism which is

binding on the consumer. At an international level, the discussion is still going on in order to answer the questions posed in the preceding paragraph.

C. Applicable law

In comparison with dispute resolution, not much has been done at the international level to address the issues of applicable law. However, because in some countries, particularly common-law countries, the issues of court jurisdiction and applicable law are dealt with together, it can be said that a large part of the same controversies triggered by the proposed court jurisdiction rules also relates to applicable law rules. For example, work was started in the European Union, to revise the Rome Convention of 1980[71] in order to transform it into a new Regulation and to prepare another Regulation (called Rome II) on extra-contractual obligations. Both projects, however, have been halted for the past year or so because Internet operators claimed that these texts were unfair to them, obliging them to know all the laws in the world.[72] The present status of the conflict of law rules will therefore be described briefly, in the knowledge that much more work is needed at an international level on this issue.[73]

1. Business-to-business contracts

The main feature of the debate is the renewed interest in codes of conduct. It is not necessary to recall the details of the controversy, which are well known and have agitated international lawyers for the past half century at least. The Internet has simply put the role of codes of conduct once again in the forefront of international negotiations. That is why this aspect of the subject matter will be discussed briefly before mentioning a few words about party autonomy and default conflict rules.

(a) The place of codes of conduct

It would seem indisputable that, in a business-to-business context, parties to a contract may decide either to adhere to a pre-existing code of conduct or to create one of their own. After all, most States have been keen on giving as much freedom to businesses as possible and codes of conduct are considered to be a large part of the *neo lex mercatoria* which developed all over the world in the 1960s. It is thus understandable and acceptable that operators over the Internet develop their own codes of conduct.[74]

That said, however, States must not think that their role ends there. On the contrary, because the effect of codes of conduct stops where States' public policy starts, States are confronted with an ever more pressing duty to define carefully the limits of their public policy. It is arguable that a special effort should be made to set the scene at an early stage, perhaps as early as at the domestic legislation stage. It has always been said in international law that, except in extraordinary circumstances, national legislators legislate only for their own domestic needs without regard for the international aspects of a question. This may not be possible any more, at least to some extent.

Another consequence of the Internet may be the need for States to agree internationally on a minimum standard of public policy. This idea is contrary to the tradition whereby States are recognized to be the masters of their public policy and to have the sovereign right to decide unilaterally on these matters. It is not at all our intention to suggest that States will not be able to continue to define their public policy for themselves (particularly for reasons of cultural specificity). It would, however, facilitate access to and use of the Internet if some common international ground was to be found.

(b) Party autonomy

In the conflict of laws, the expression "party autonomy" reflects the freedom for operators to choose the law which will be applicable to their transactions. Party autonomy is clearly the rationale behind the codes of conduct studied above, but it does not stop at that. In all international contracts, parties may include a choice-of-law clause which is normally upheld by all countries around the world. The limit of that freedom is again, as for codes of conduct, the public policy of each State. The discussion above is pertinent here and we will not repeat it.

Party autonomy is limited in two ways in respect of regulated professions such as doctors, security brokers and lawyers. If the professional uses the Internet to render services in the jurisdiction in which he is located, professional regulations will continue to apply to him as before and the extent of his freedom will not be different from that in the period before the Internet. If the professional uses the Internet to provide services in a different jurisdiction he may still be obliged to respect the regulations of his own jurisdiction and will also be obliged to respect professional regulations in the jurisdiction in which its

clients are located. Therefore, a lawyer would not be free to offer legal services via the Internet to clients located in a different jurisdiction, unless he or she respected the rules of the profession in that jurisdiction.[75] This result is not different from the one in real life.

As far as the validity of the choice-of-law clauses included in electronic contracts, i.e. contracts negotiated and drawn up over the Internet, is concerned, the rules to be developed will be very similar to those already developed for choice-of-court clauses. This aspect of the question has been discussed above,[76] and what we said then can apply *mutatis mutandis* to choice-of-law clauses.

(c) Default conflict-of-laws rules

If the parties have not included a choice-of-law clause in their contract or if the choice was held to be invalid, the contract will be considered to be subject to the law defined by the conflict of laws rules of the country in which the court seized of the dispute is located.

A preliminary remark is necessary at this stage. The way in which conflict-of-laws rules work obliges parties to a contract, who have not used the freedom granted to them to choose the law to be applied, to first assume which court will hear the dispute in order to be able to discover what conflict rules are to be applied. In the European Union the inconvenience is not so great since several member States apply the same conflict rules.[77] Outside Europe, however, the problem remains.

Many countries have codified their conflict rules.[78] In consequence, these rules are more readily accessible to operators. It is not possible, in the context of this chapter, to analyse in detail all rules available around the world even in codified legislation. Briefly stated, to the best of our knowledge, most rules take into consideration the main obligation which characterizes the contract in question and look at the location of the party which must provide this main obligation. The law of that country is deemed applicable. This is also the basic principle used in international conventions adopted under the auspices of the Hague Conference on Private International Law.[79] In electronic commerce, the link with the location of the party which must provide the contractual obligation does not seem to trigger difficulties in the B2B context.

2. Consumer contracts

Because of the specific nature of consumer contracts, in countries where consumers are protected, the law applicable to those contracts — among the laws which may apply to such a contract — is almost always that which is more favourable to the consumer. Therefore, if the law of the location of the consumer is the most favourable, it will apply; but if, on the contrary, it is not, the law of the professional who supplied the service or the goods will apply.

This is the main reason why Internet operators have been so keen on blocking adoption of rules of the same sort for the Internet. The controversy mentioned above with regard to dispute resolution is also relevant here.[80] Discussions are going on in the international sphere. The joint United States-European Union statement mentioned above calls for the use of codes of conduct including for consumer relations. The use of such codes in a field where partners are not equal may pose difficulties. If this course of action was to be favoured, public authorities would have a clear role to play in ensuring that the process of elaboration is a fair one and the result takes into consideration the specific needs of consumers.

This discussion shows that there is a clear need for an international agreement on common rules of protection for consumers. Before the Internet, it was commonly said that a consumer contract was rarely international. Indeed, a consumer contract was usually formed and performed locally (the proximity principle). This is why the Internet has changed the nature of the consumer contract dramatically.

3. Torts

Anyone studying legal systems around the world will discover that basically two conflict rules for tort cases coexist: that of the country where the tort was committed and that of the country where the effect is felt. Some countries apply both rules, allowing the victim to choose the law that is more favourable to its interests.

The rationale behind the first conflict rule takes into consideration the fact that in order for a tort to be committed, there must be a violation of a norm. Thus, it is only fair to impose on the offender respect for the norms in force in the place where the act occurred. This clear policy, however, has been

undermined by the evolution of liability rules around the world and the increase in insurance coverage. Increasingly strict liability systems have been put in place which require a person whose acts have adverse effects to repair the damage.

The rationale behind the second conflict rule stems from the observation that a victim of a tort must be protected at least up to the point allowed by the law where that victim feels the effects. In the application of this rule, one difficulty stems from the fact that a victim may be injured in one place but returns to the place where it has its habitual residence, where it continues to suffer damage. It is usually considered that the law to be applied is the law of the country where the first damage was experienced.

The terms are slightly different with the Internet. Indeed, as mentioned above for the place of conclusion and performance of a contract, the place where the wrongful act was performed over the Internet is not easy to locate. In fact, the only sensible answer is to say that this place coincides with the place where the offender is located. However, an immediate objection comes to mind: if this rule were to become the international standard it would be an incentive for potential violators to locate in digital havens. Thus, the conflict rule cannot lead to that law since it would be all too easy to commit torts without ever having to face their consequences.

This is why most decisions which have been taken by national courts around the globe apply the law of the place where the effect was felt.[81] The limitation in most of these cases was that plaintiffs asked only for compensation of the damages suffered in that particular country. Again, this is the usual limitation applied in international tort cases. This rule has to be reassessed against Internet specificity. Recent discussions, notably on torts dealing with intellectual property, show that the plaintiff must have one forum where it can consolidate all the claims for all the damages suffered in as many jurisdictions as exist.[82] Indeed, the court would have to apply several different laws. But this is not an absolute obstacle in practice. Courts in many countries around the world are accustomed to applying foreign law. In addition, Internet-based information may ease the findings of the content of foreign law.

The other difficulty stems from an injunctive relief. Some Internet operators claim that it is technically not feasible to filter the web so that certain sites or pages cannot be accessed in a specific country, while others claim the contrary.[83] If the first group is right, an injunction decided by one court would have effects all over the world. If the second group is right, it would be possible for a court in one State to decide on an injunction with limited effects.

D. Privacy and data protection

The Internet has rendered the question of privacy and personal data protection acute. This is due not only to the very nature of the Internet itself, with its special technical features which allow data banks to be set up with a large amount of information to be retrieved in many different ways, but also to the fact that the value of many Internet corporations depends on the amount of data they have been able to gather. Thus, personal data about consumer habits, tastes and the like are of great value to any corporation wishing to operate over the net.[84] The problem is not new; what is new is its scale.[85] This is why an attempt to unify substantive law has been made, with the European Union in the forefront (para. (1)). However, the difficulty in completely unifying substantive law leaves some role for the conflict of laws rules (para. (2)).

1. Attempts to unify substantive law

The explanations given below are essentially on the work done in Europe, since it seems to be the most advanced on these questions. The European system of data protection is based on the European Convention on Protection of Personal Data of 1981 (Convention No.108).[86] In 1995, the European Community adopted a Directive on the protection of personal data and their freedom of circulation within the Community.[87] However, the Directive is considered not sufficient in view of the specific features of Internet communications and this is why a new Directive is being proposed for this field.[88] The new Directive will not replace that of 1995, which remain in force, but will complement it.

The main features of the protection proposed by these two Directives may be summarized as follows: (i) the confidentiality of communications must be guaranteed; (ii) legal persons must be protected, as well as individuals, in the context of electronic communications; (iii) this protection is necessary in order to increase confidence in electronic communications, which is crucial to the effective development of this

economic sector; (iv) ISPs must take appropriate measures to provide security for their services and inform their clients of the limits of that security; (v) data banks containing personal data must be collected and maintained only to the extent necessary for the services provided and for a limited period of time; (vi) any other use of those data may be made only with the express consent of the person whose data are collected; (vii) persons must be able, without difficulty, to require deletion of personal data and to have access to courts for their protection; (viii) member States may limit the use of anonymity or other filtering processes in order to combat criminal activity.

Before entering into an agreement with a foreign country to allow free circulation of personal data outside Europe, the European Community must evaluate the adequacy of data and privacy protection in that country. This has been done with regard to a number of countries, for example Switzerland,[89] Hungary,[90] the United States[91] and Canada.[92] Other countries may follow when their data protection system has evolved.[93] It took a long time to reach the decision concerning the United States since it related to the specific system applied in that country, known as the "safe harbour" principle. This system is based on a proactive attitude by operators themselves (self-regulation), as there is no preventive legislation in the United States. The system was criticized by the European Parliament and by some privacy groups (including American privacy groups) during the hearings held by that body before the final approval of the Commission's decision. Experience will show whether the system is viable or not.[94]

Another organization that has been very active in the field of privacy protection is the OECD. As early as 1980, it drew up "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data".[95] These lay down principles for the collection and processing of personal data, to apply at both the national and international levels. Member countries are called upon to implement these principles internally, by introducing legal, administrative or other provisions, or setting up institutions to protect privacy and personal data.

Similarly, in 1985 the Governments of the OECD member countries adopted a declaration on transboundary data flows, emphasizing their intention of seeking to achieve transparency in the rules and policies affecting international trade, and developing common approaches or harmonized solutions for dealing with the problems associated with this trade.

The OECD continued its work in an expert group on security of information and privacy, which in 1997 issued a report on "Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet".[96] This report discusses the growing importance of data protection, especially in an electronic online environment. As several surveys have shown, the fears of Internet users concerning the collection and use, even for commercial purposes, of their personal data, are tending to hold back the development of electronic commerce. The report also describes the complaints recorded in certain OECD member countries about problems such as the use of electronic addresses and the right of employers to inspect the electronic mail of their employees; inaccurate information and fraudulent activities on the Internet; and the ease with which personal information, especially electronic addresses, can be derived from activities conducted on the Internet and then used in the compilation of commercial marketing lists without the knowledge of those concerned. The report describes certain methods of data collection on the Internet, and mentions some initiatives taken by the private sector to protect privacy on websites. According to the group of experts, solutions have to be found through dialogue between Governments and the private sector. The report highlights the role of Governments, and reaffirms that the guideline principles must be implemented through law or through self-regulation, and that remedies must be available for individuals if they are breached. The report also encourages Governments to support private sector initiatives to find technical solutions for implementing the Guidelines. In conclusion, it recommends collaboration among all players on the Internet, emphasizing the important role of the OECD.

In February 1998 the OECD organized in Paris, with the support of the Economic and Industrial Consultative Committee of OECD (BIAC), an international conference on "Privacy Protection in a Global Networked Society".[97] This conference was an opportunity to bring together representatives of Governments, the private sector, consumer organizations and the authorities responsible for data protection. At the end of the conference, its Chairman noted that there was a broad consensus on the need to strike a proper balance between the free

circulation of information and the protection of privacy. In order to evaluate the current situation on the web, an "Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of Privacy Guidelines on Global Networks"[98] was drawn up in September 1998. This inventory comprises the laws and mechanisms of self-regulation which have been adopted at the regional, national and international levels.

At the OECD Ministerial Conference held in Ottawa from 7 to 9 October 1998, the OECD Ministers adopted a Declaration on the Protection of Privacy on Global Networks, reaffirming their commitment to achieving effective protection of privacy on these networks and their determination to take the necessary steps for this purpose, and recognizing the need to cooperate with industry and businesses. They also agreed that the OECD should provide practical guidance for implementing the guidelines on the protection of privacy, based on national experience and examples.[99]

In the light of the undertaking by Ministers at the Ottawa Conference, the OECD decided to devise, in collaboration with industry, specialists in the protection of privacy and consumer associations, an experimental "html" tool, a generator of OECD policy declarations on the protection of privacy. This tool is addressed to public organizations and private sector enterprises, to encourage them to draw up policies and declarations on protecting privacy. It is presented in the form of a detailed questionnaire which will enable the organizations concerned, after an internal review of their privacy protection practices, to draw up a policy declaration on the protection of privacy which will appear on their site. The generator is currently available in English, French, German and Japanese, and is accessible on the OECD Internet site. The questions posed in the generator are very similar to those included in the "safe harbour" analysis annexed to the European Commission decision concerning the protection of personal data in the United States.

2. What role for conflict-of-law rules?

The unification of substantive law is certainly the best solution for international protection of privacy and personal data. However, it is not always possible to unify all aspects of the law; and, therefore, the question of applicable law is still pertinent in that context.

In preparing the guidelines mentioned above, the group of experts paid great attention to the problems of conflicts of law and of jurisdiction raised by transboundary flows and the protection of privacy, but did not offer any specific detailed solutions. However, the guidelines do contain one general recommendation, that "Member States should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data".[100]

Although paragraph 22 of the guidelines was never repeated in the subsequent work of the OECD, identification of the applicable law, in the context of establishing modes of dispute resolution which will be readily accessible and efficient, is still one of the possible techniques for bringing about the effective protection of privacy in a transnational framework.[101] This was the aim of the Joint Conference organized in The Hague in December 2000 which explored online dispute resolution mechanisms as potentially applicable to privacy protection.[102]

What could be the conflict rule? If we look at the aim of personal data protection, it is clear that it leads us to favour the law of the location of the person whose data have been collected. It is the law which that person would be deemed to know. He or she is probably going to act in accordance with the level of protection which that law provides. However, this conflict rule clashes with the economic needs of Internet operators. This is why if it is the rule that may be adopted, it must remain a default rule to be applied only if substantive unification is not possible.

E. Other legal and regulatory issues

1. Electronic signatures

The enforceability of e-commerce transactions is the most basic and fundamental issue to be addressed by e-commerce legislation. Moreover, it is the subject that has seen the most activity during the past year, generally in the form of electronic signature legislation.[103] Thus, it has been recognized in many instances that electronic signature legislation can provide the predictability which businesses require in order to engage in e-commerce transactions.[104] Governments wishing to promote e-commerce are urged to identify and remove legal barriers that hinder the recognition of electronic authentication.[105] In this

regard, electronic signature legislation might accomplish two important goals: to remove barriers to e-commerce, and to enable and promote the desirable public policy goal of e-commerce by helping to establish the trust and the predictability needed by parties doing business online.[106]

There are at present three main functions attached to electronic signatures:

(1) **Data origin authentication**: This can provide assurance that a message came from its purported sender;

(2) **Message integrity**: This enables the recipient of a message to verify that a message has not been intentionally or accidentally altered during transmission;

(3) **Non-repudiation**: The sender cannot deny that the message was sent.

At the moment, several methods are available for carrying out the above functions.[107] However, one type of electronic signature, the so-called digital signature technology based on public key cryptography, is today regarded as the most common and reliable technique. For digital signatures to achieve authenticity functions it is necessary to use a trusted third party called a certification authority (CA), which, given satisfactory evidence, is prepared to certify the identity and attributes of the parties.

A review of legislative and regulatory activities reveals three basic approaches to electronic signature legislation.[108]

(1) **Minimalist approach**: The primary motivation is to remove existing legal obstacles to the recognition and enforceability of electronic signatures and records. Legislation is limited to defining the circumstances under which an electronic signature will fulfil existing legal requirements for tangible signatures. This kind of legislation does not address specific techniques and is, therefore intended to be technology-neutral. The minimalist approach focuses on verifying the intent of the signing party rather than on developing particularized forms and guidelines. The UNCITRAL Model Law on Electronic Commerce (see Article 7)[109] and a number of common-law countries (e.g. Canada, the United States,[110] the United Kingdom, Australia and New Zealand) have adopted such an approach.

(2) **Digital signature approach** (prescriptive approach): This establishes a legal framework for the operation of digital signatures (PKIs), whether or not other forms of secure authentication are included or permitted. Legislation and regulations enacted under this approach share the following characteristics: adoption of asymmetric cryptography as the approved means of creating a digital signature; imposition of certain operational and financial requirements on certification authorities (CAs); prescription of the duties of key holders; and definition of the circumstances under which reliance on an electronic signature is justified. The prescriptive approach has been adopted by a number of civil-law countries (e.g. Italy, Germany and Argentina).

(3) **A two-tier approach**: This represents a synthesis of the two previous approaches. The laws enacted prescribe standards for the operation of PKIs and take a broad view of what constitutes a valid electronic signature for legal purposes. This approach achieves legal neutrality by granting minimum recognition to most authentication technologies, while at the same time it incorporates provisions for an authentication technology of choice. The two-tier approach has been followed, by, among others the European Union (1999 Directive on Electronic Signatures), the UNCITRAL Model Law on Electronic Signatures, 2001 and the 1998 Singapore Electronic Transactions Act.

Some recent samples of regional legislation and international model law legislation on electronic signatures that might guide States wishing to enact legislation in this field are as follows:[111]

- **EU Directive of December 1999 on a Community Framework for Electronic Signatures:**[112] The aim of the Directive is to establish a harmonized Community-wide legal framework for electronic signatures and electronic certification services. This means in particular that electronic signatures cannot be denied legal effect just because they are in electronic format, but are recognized in the same way as handwritten signatures relating to paper-based data. The Directive does not apply to closed systems, such as a corporate Intranet or banking network, although electronic signatures used within closed systems benefit from legal recognition. In an effort to ensure that the Directive will not soon become obsolete a technology-neutral approach is

adopted, one which is based on an open electronic signature concept that includes digital signatures based on public-key cryptography as well as other means of authenticating data.[113] In addition to providing a definition of electronic signature (article 2 (1)), the Directive refers to the "advanced electronic signature" that is designed to provide a higher level of security.[114] Although member States are prohibited from making the provision of Certification Services subject to prior authorization, they are entitled to set up voluntary accreditation schemes to provide consumers with a higher degree of legal security as regards certification service providers (CSPs).[115] Furthermore, they are required to ensure the establishment of an appropriate system that allows for supervision of CSPs which are established on their territory and issue qualified certificates to the public.[116] The Directive does not preclude the establishment of a private-sector-based supervision system or oblige CSPs to apply to be supervised under an accreditation scheme. It establishes common requirements for qualified certificates (annex 1), CSPs (annex 2) and secure signature-creation devices (annex 3). As regards liability, the CSP is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate unless the CSP proves that he has not acted negligently. Under certain conditions, the CSP is entitled to set limits regarding the use of a certificate and the value of transactions for which the certificate is valid.[117] Article 7 of the Directive addresses the international dimension of electronic commerce by ensuring that certificates issued in a third country are recognized as legally equivalent to certificates issued by a CSP established within the Community under certain precise conditions. Article 8 of the Directive, which refers to data protection, provides for the application to CSPs and national bodies responsible for accreditation/supervision of Directive 95/46EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Furthermore, it is specifically provided that CSPs may collect personal data directly from the data subject only, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

- **UNCITRAL Model Law on Electronic Signatures, 2001**: Following the adoption in 1996 of the Model Law on Electronic Commerce and in particular of Article 7 concerning "signatures",[118] UNCITRAL requested the Working Group on Electronic Commerce to develop further rules on electronic signatures (the original mandate read "digital signatures and certification authorities"), so as to help provide more certainty through implementation of the said provision. The Working Group began its work in February 1997 and finished it at its thirty-seventh session in September 2000. The Model Law on Electronic Signatures (MLES),[119] together with the Guide to Enactment,[120] was adopted by UNCITRAL on 5 July 2001. The MLES three main parts: on criteria for reliable electronic signatures; on the duties of the three potential functions involved in an electronic signature (signatory, certification service provider and relying party); and on the recognition of foreign certificates and electronic signatures.[121] In addition, the Guide to Enactment, much of which is drawn from the preparatory work on the Model Law, is intended to assist States in considering which, if any, of the MLES provisions should be varied in order to be adapted to any particular national circumstances. Furthermore, a number of issues not included in the MLES are referred to in the Guide so as to provide guidance to States enacting the Model Law.[122] The MLES applies only to commercial activities (Article 1) in a wide sense that includes the supply or exchange of goods or services, distribution agreements, agency, factoring, leasing, investment, financing, banking, insurance and carriage of goods. Article 6 constitutes one of the main provisions of the MLES, since it provides guidance in paragraph 3 as to the test for reliability of electronic signatures. The criteria are as follows:[123]

"(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to

> the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable."

Article 6 (4) emphasizes that there is no need to meet all the above-mentioned criteria for a signature to be reliable but that reliability could be established in any other way. Furthermore, and in accordance with article 7, any person, organ or authority, whether public or private, specified by the enacting State as competent, may determine which electronic signatures satisfy the provisions of article 6. Any such accreditation must be consistent with recognized international standards. Article 8 sets out what the signatory must do and article 9 describes the conduct of the CSP. Concerning the recognition of foreign certificates and electronic signatures article 12 establishes the general principle of legal equivalence between foreign and domestic signatures and certificates if the system in the State of origin offers a level of reliability "substantially equivalent" to that in the receiving State. Although the MLES does not constitute a comprehensive set of rules on the subject, its rules are consistent with international practices and it provides an important international model for countries wishing to enact legislation on electronic signatures.

2. Electronic contracting

Following the adoption in 1996 of the UNCITRAL Model Law on Electronic Commerce,[124] which is intended to remove legal barriers to the use of electronic communications and provides "functional equivalents" to the use of paper-based documents, a number of countries, including developing countries, have enacted legislation based on the Model Law.[125] Although the Model Law offers national legislators a set of internationally acceptable rules that could be used to overcome some of the main obstacles when conducting legal transactions in cyberspace, it seems that, at least in some jurisdictions, a problem might arise in order to overcome references to "writing", "signature" and "document"[126] in conventions and agreements relating to international trade.[127] It is precisely for this reason that the Centre for the Facilitation of Procedures and Practices for Administration, Commerce and Transport (CEFACT) of the United Nations Economic Commission for Europe (ECE) recommended[128] to UNCITRAL that it "consider the actions necessary to ensure that references to writing, signature and document in conventions and agreements relating to international trade allow for electronic equivalents". In a note[129] of 20 December 2000 entitled "Legal barriers to the development of electronic commerce in international instruments relating to international trade: ways of overcoming them", the UNCITRAL secretariat included the advisory opinion of a law professor as to the "adaptation of the evidentiary provisions of international legal instruments relating to international trade to the specific requirements of electronic commerce". The note was submitted to the thirty-eighth session of the UNCITRAL Working Group on Electronic Commerce in March 2001. The Working Group agreed to recommend to the UNCITRAL Commission that it undertake work towards the preparation of an international convention to remove legal barriers that might result from international trade law instruments.[130]

At the regional level, the European Union adopted a "Directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market" (Directive on electronic commerce),[131] which lays down a general framework to ensure the free movement of information society services in the EU. The Directive covers all information society services, B2B and B2C, as well as services provided free of charge to the recipient. It establishes rules in various areas, including the following: definition of where operators are established; transparency obligations for ISPs; transparency requirements for commercial communications; conclusion and validity of electronic contracts; liability of Internet intermediaries; and online dispute settlement. Although the Directive does not apply to services supplied by service providers established in a third country (outside the EU), the solutions provided for some of these issues may serve as a model for countries wishing to regulate this area.

Other recent work of a related nature that focuses on contractual matters is the Electronic Commerce Agreement (the E-Agreement), developed by the UN/CEFACT.[132] The E-Agreement is intended to serve the commercial needs of B2B electronic commerce partners. It contains a basic set of provisions which can ensure that one or more electronic commercial transactions may be concluded by commercial partners within a sound legal framework. Although the E-Agreement could also be used in the B2C relationship, it does not include provisions relating to consumer protection. Thus, businesses wishing to use the E-Agreement in the B2C sector must be aware of the need to comply with mandatory

consumer protection laws. Furthermore, parties must ensure compliance with other mandatory national and local laws, such as tax regulations and data protection legislation.

In addition to the above-mentioned contractual solutions, the UN/CEFACT has recommended a Model Code of Conduct for Electronic Commerce as a means of facilitating e-commerce transactions. The Code of Conduct, which is a self-regulatory instrument, can work in parallel with other measures to facilitate electronic commerce, such as trustmark schemes. The Recommendation that requests States, for the promotion and development of self-regulation instruments for electronic business, includes as an example the "Model Code of Conduct for Electronic Commerce developed by the Electronic Commerce Platform of the Netherlands", which is annexed to the Recommendation.[133]

F. Fiscal and customs regulations

1. E-commerce taxation

The question of taxing e-commerce has increasingly been of concern to Governments and tax authorities in both developed and developing countries. Fears about revenue losses resulting from uncollected taxes on Internet transactions, coupled with the substantial growth of Internet commerce in the past years and predictions for the next few years, have prompted Governments and international organizations to set up committees to evaluate the implications of e-commerce for national and international tax systems and provide recommendations on how to change existing legislation to take account of e-commerce.

The main players in the debate on e-commerce taxation have been the United States, the European Union (EU) and the Organisation for Economic Co-operation and Development (OECD). The United States and the EU member States are primarily concerned with how their respective tax systems will be affected by e-commerce (see below). The OECD secretariat, whose Model Tax Convention serves as a basis for most bilateral tax treaties (including between non-OECD member countries), has been asked by its member States to take the international leadership role in e-commerce and taxation, a mandate that was confirmed at the 1998 OECD Ministerial Meeting in Ottawa. It has prepared a number of taxation principles that should govern e-commerce and has worked closely with the EU on consumption tax issues.

Developing countries have participated little in these debates and the proposals and papers so far produced by the OECD countries have given scant consideration to developing countries' concerns.[134] While it is true that developing countries' shares in e-commerce are still modest, the international rules and regulations that are adopted now will impact on e-commerce in many countries in the future, including in the developing countries. In addition, the increasing number of small and medium-sized enterprises (SMEs) that will be drawn in by e-commerce from the developing countries have little experience in international taxation issues. It is therefore crucial to include their concerns as early as possible. This section will briefly introduce two key issues currently debated as regards Internet taxation: consumption taxes and income taxes. It will present proposals put forward on how to change existing tax regulations in the light of e-commerce and discuss possible implications for developing countries.

(a) Consumption taxes: Which jurisdiction applies?

Consumption taxes usually include value added taxes, sales taxes and turnover taxes. Traditionally, they are borne by the consumer and collected by the seller; different rules apply depending on the product or service sold, the location of consumer and seller, and the type of consumer (business or individual). With e-commerce, the number of foreign online suppliers, who are often subject to different taxation rules, has increased considerably. Research carried out in the United States on the impact of taxation on Internet commerce and consumer online purchasing patterns found that consumers living in high sales tax areas are significantly more likely to buy online than those living in low sales tax areas (Goolsbee, 1999). Hence, differentiated Internet taxation rules among countries could have a significant impact on the purchasing behaviour of consumers, with the latter shifting from domestic to foreign suppliers.[135]

This raises several problems for tax authorities. First, it leads to the gradual elimination of traditional intermediaries (so-called disintermediation) such as wholesalers or local retailers, who in the past have been critical for identifying taxpayers, especially private consumers. Second, foreign suppliers may be tax-exempted, whereas local suppliers are normally

required to charge value added tax (VAT) or sales taxes. Third, direct orders from foreign suppliers could substantially increase the number of low-value shipments of physical goods to individual customers. These low-value packages now fall under so-called *de minimis* relief from customs duties and taxes in many countries, basically to balance the cost of collection and the amount of tax due. A substantial increase in these shipments as a result of e-commerce (where foreign suppliers replace domestic ones) could pose an additional challenge to tax as well as customs authorities.

(i) European Union vs. United States proposal

Major differences exist between the EU and the United States in the way taxes are redeemed and hence in their approaches to international taxation rules on e-commerce. The EU countries derive about 30 per cent of government tax revenue from taxes on domestic goods and services (mainly VAT). In addition, VAT extra charges contribute 45 per cent to the EU Community budget (in addition to customs duties and GNP contributions) (European Commission, 1998). Their main concern is the increasing import of digital content and services from outside the EU, which would be exempted from VAT payments in the EU. The United States Government, on the other hand, derives most of its tax revenues from personal and corporate income tax and social security contributions; revenues from taxes on domestic goods and services are extremely low (3.6 per cent) (although individual States depend significantly on local sales taxes, see below). The United States is currently both a net exporter and the main exporter of e-commerce worldwide. Hence, it has a great interest in encouraging business (including e-commerce business) to locate in the United States and pay direct taxes to the United States tax authorities.

Therefore, the issue of consumption taxes on international e-commerce has received most attention in the OECD and the EU. In particular, the EU feels very strongly about maintaining VAT duties and is likely to modify tax rules in a way that will ensure a continuation of VAT contributions, rather than lowering or eliminating them. A closer look at current VAT regulations in the EU will explain the growing concern among EU tax authorities and Governments.[136]

Goods. Imported goods from non-EU members are subject to (import duties and) VAT of the importing country. Sales within the EU are subject to the VAT of the receiving country in the case of business-to-consumer trade. Businesses selling to businesses in another member State are tax-exempted; the receiving or importing business is required to pay VAT locally (i.e. in the country of final consumption).[137] Exports to non-EU countries are zero-rated.

Services. Services differ according to the type of services traded. In the case of information (currently the majority of e-services), imports from non-EU businesses to EU consumers are not subject to customs duties and are VAT-exempted (except in Denmark, France and Italy). Sales from non-EU businesses to EU businesses are subject to self-accounted VAT at the local rate (a so-called reverse charge). Intra-EU service suppliers are required to charge VAT in the country in which they are established (location of the seller), if selling to private consumers. EU business-to-business services trade is subject to VAT in the country of the final consumer. Sales to customers outside the EU are subject to VAT in the location of the seller (European Commission, 1999; Kerrigan, 1999).

The challenges to EU tax authorities that arise from e-commerce therefore lie in non-EU supplies of e-services to EU customers (and in an increase in non-EU customers not subject to EU VAT). Under current tax law, these are exempted from VAT, while at the same time their share is increasing, in direct competition with EU suppliers who are subject to VAT payments. Furthermore, the VAT exemption provides incentives for suppliers to locate outside the EU, a fairly easy undertaking in e-commerce, which no longer requires the presence of human and technical resources.

Even though the United States Government has been less concerned about VAT regulation, the potential loss in sales taxes as a result of e-commerce has caused major concern among local Governments. Within the United States, individual states have autonomy with regard to determining and collecting State tax and local sales tax, which are often their largest source of revenue. Sales taxes differ substantially among States, ranging from 0 to 7 per cent. United States-based online suppliers selling to out-of-State (including foreign) customers do not currently have to charge local sales tax. States are therefore becoming increasingly worried about how to secure their sales tax revenues

in the light of Internet commerce, and estimates of revenues lost due to Internet sales range from $ 1.2 billion (1999) to 10.8 billion (2003) (University of Tennessee, 2000).

In 1998, the United States Congress created the Advisory Commission on Electronic Commerce, under the Internet Tax Freedom Act, to study a variety of issues involving e-commerce taxation, including international issues. The Commission collected proposals from the public and private sectors for consideration, which contributed to the final report and recommendations submitted to Congress in April 2000. At its final meeting in March 2000 (Dallas, Texas), the Commission voted *inter alia* to extend a three-year moratorium on domestic "new" Internet taxation imposed by the Internet Tax Freedom Act and due to expire in October 2001, until 2006. The moratorium essentially bans taxes on Internet access fees. However, owing to a disagreement among the Commission's members, no solutions have been provided on the question of State and local tax collection.

The National Governors' Association has therefore initiated the Streamlined Sales Tax Project (SSTP), an ad hoc group composed of 30 States whose aim is to simplify and harmonize State sales tax systems in the light of e-commerce. Model legislation was approved in December 2000, providing for a Uniform Sales and Use Tax Administration Act and Streamlined Sales and Use Tax Agreement, which are expected to simplify the collection of sales taxes on online transactions. The group hopes that other states so far not participating will follow suit.

(ii) A multilateral framework?

At the Ottawa Ministerial Conference, the OECD proposed a number of "framework conditions", including on consumption taxes, which since then have been adopted by a large number of countries, including OECD non-member countries (OECD, 1998a). These conditions include:

- Cross-border trade should be taxed in the jurisdiction where consumption takes place;
- The supply of digitized products should not be treated as a supply of goods for consumption tax purposes (differences in the definition among countries may lead to uncertainties about the tax treatment of products from outside suppliers);
- Where services and intangible property (i.e. goods) from suppliers outside the country are acquired, countries should examine the use of reverse charge, self-assessment or other equivalent mechanisms;
- Appropriate systems should be developed to collect tax on the importation of physical goods.

On the basis of these conditions, the EU has proposed changes to its current VAT legislation taking into consideration e-commerce (European Commission, 2000a). Under this proposal, non-EU suppliers with annual sales to the EU exceeding •100,000 would be required to apply taxes on the same basis as an EU operator when transacting business in the EU. This would follow the Ottawa framework condition whereby taxation is applied in the jurisdiction where the consumption takes place.[138] In order to facilitate compliance, the European Commission proposes that non-EU e-commerce operators be required to register in one EU member State only and have the possibility of discharging all their obligations by dealing with a single tax administration. This has been a controversial point among members States who are concerned that Luxembourg, the State currently with the lowest VAT rate (15 per cent), would be the preferred country of registration and collect taxes without having to compensate other member States. EU suppliers, on the other hand, would not be obliged to levy VAT on products sold to customers outside the EU. Business-to-business transactions would not be affected by the proposed new Directive: as in the past, the tax would be accounted for in the EU under the reverse charge system whereby traders assess their own VAT liability.

The proposal has prompted a strong reaction from non-EU suppliers (notably businesses in the United States), who have little interest in collecting VAT for EU tax authorities, arguing that this would impose an unnecessary burden on their overseas transactions and, in general, restrict e-commerce. The VAT Directive is to be implemented on 1 January 2001, but it is unlikely that it will become law for another few years.

A key problem for tax authorities will be to identify the customer and the location of the jurisdiction responsible for collecting the tax. Because of the process of disintermediation, apart from the seller and the customer there are no other parties involved in the transactions (which could collect the tax). Credit

card companies, ISPs, banking and payment systems providers and telecommunications companies have all been mentioned as potential new intermediaries in verifying the location of a customer and the respective tax jurisdiction ("trusted third parties" – TTPs). This, of course, raises privacy issues and could lead to abuses of information. It could also lead to an increasing use of foreign credit cards or digital cash; needless to say, the customer's location may differ from the billing address. In addition, how can an Internet seller determine whether the customer is a business or an individual consumer, each of which is subject to different VAT rules? An increasing number of e-commerce businesses are small entrepreneurs operating from home who may receive services for business or personal purposes.

Following the OECD framework conditions, the EU also proposed that for VAT purposes trade in digitized goods be treated as a supply of services and that VAT rates on all e-services be harmonized into a single rate. This could result in tax losses since consumption taxes are lower on services than on goods. It could also lead to losses on tariffs and import duties on digitized goods that were shipped physically in the past and which would now be subject to much lower duties. This would impact in particular on the developing countries, whose reliance on import duties as a government revenue source is much higher than that of the developed countries.

At the Ottawa Conference, the United States took a different position on this issue: digital products should be characterized on the basis of the "rights transferred" in each particular case. It argued that some goods which are now zero-rated (such as books and newspapers) would be subject to VAT if treated as a service. Customers may therefore prefer to buy local zero-rated books rather than digitally imported (and taxed) services, many of which could be supplied by United States online providers. As an alternative, the United States has proposed an origin-based consumption tax for intangibles (e-services), which would be collected from the supplier and not from the consumer. It argues that it is easier to identify the supplier than the customer on the basis of the permanent establishment rule (see below), and since businesses are subject to audit. The United States as a net exporter of e-commerce would benefit from an origin-based tax, although such as tax may further erode the tax base in e-commerce-importing countries. On the other hand, it disadvantages domestic producers in their export sales since they would have to pay the tax on the exports, instead of the final consumer. This may encourage business to set up shop in countries with no origin-based taxation. Finally, it needs to borne in mind that most e-commerce will be business-to-business (currently 80 per cent of e-commerce), which is often tax-exempted or subject to voluntary compliance.

(iii) Implications for developing countries

How does consumption tax legislation affect developing countries? Most of them rely heavily on consumption taxes for their government budgets (Teltscher, 2000). Given that many developing countries will be net importers of e-commerce in the medium term, they would have a strong interest in not eroding their tax bases by switching to an origin-based tax system. They need to be aware, however, that tax collection on e-commerce activities will require access to the latest technologies by tax authorities. Thus, developing countries need to catch up on modernizing their tax administration systems in order not to lose important tax revenues on the collection of consumption taxes. In this context, the OECD, in cooperation with four regional tax organizations, is organizing a conference on "Tax administrations in an electronic world", to be held in Canada in June 2001. The OECD expects the conference to be attended by participants from 106 countries (including many developing countries) and eight international organizations.

To avoid double taxation, some multi- or bilateral agreements have to be adopted on where consumption taxes are to be collected: in the country where the supplier is established, the country where the customer is established or the country of consumption. The proposal by the EU to require non-EU suppliers to register for and charge VAT in a EU country would not favour providers from developing countries, thus placing an additional burden on their e-commerce exports.

(b) Income taxes: "Permanent establishment" in cyberspace?

The taxation of income, profits and capital gains is another major source of government revenue, especially in the developed countries. There are two basic concepts of how countries tax income. First, source-based taxation is applied in the jurisdiction where the economic activity takes place, for example the sale of the service or digital good traded. Foreigners who do not reside in the jurisdiction where their economic

activity takes place are still taxed on their profits earned in that jurisdiction. Second, residence-based taxation takes place in the jurisdiction of the place of residence of the person/business earning the income. In other words, taxpayers are taxed on their worldwide income by the country in which they live. Among the OECD countries, it is agreed that if a "permanent establishment" has been determined, source-based taxation applies; if not, residence-based tax principles apply (Lukas, 1999). The usual practice among OECD countries is to tax residents on their worldwide income and non-residents on the income they earn in the relevant country.[139] To avoid double taxation, countries enter into bilateral treaties, for example to reduce or eliminate source tax. Treaties are normally based on the OECD Model Tax Convention, which defines residence-based taxation according to where the management takes place. If no treaty exists, domestic tax legislation governs the taxation of non-resident businesses carrying on business in the country. In this case, the source principles generally apply.

Traditionally, direct taxation of income has employed the "permanent establishment principle" used in the OECD Model Tax Convention (Article 5) to determine in which country income has been generated and is therefore taxed. Accordingly, business profits of non-resident enterprises may only be taxed in a country to the extent that they are attributable to a permanent establishment that the enterprise has in that country, which must also be a "fixed place of business". However, the principle was drafted in 1963 and is not fully compatible with e-commerce as it relies on physical presence. For example, the source-based concept of income taxation could lead to a substantial erosion of the tax base since the link between income-generating activity and a specific location becomes blurred in e-commerce. In particular, the question of whether a website or web server can constitute a permanent establishment or fixed place of business has been at the centre of the debate. In December 2000, the OECD reached consensus on the following important changes to the Commentary on Article 5, which would be applied to e-commerce (OECD, 2000):

- An Internet website does not constitute a "place of business", as there is "no facility such as premises or, in certain circumstances, machinery or equipment". Hence, a website in itself cannot constitute a permanent establishment. On the other hand, the server operating the website is a piece of equipment which needs a physical location and may thus constitute a "fixed place of business" of the enterprise that operates it.
- A distinction between the enterprise that operates the server and the enterprise that carries on business through the website is necessary. If the website is hosted by an Internet service provider (ISP) and a different enterprise carries on business through the website, the server cannot be considered a fixed place of business. The server and its location are not at the disposal of the enterprise and the enterprise does not have a physical presence in that place since the website does not involve tangible assets. However, if the web server is owned or leased by the business which carries on business through a website located on that server, the place where that server is located could constitute a permanent establishment.
- A server constitutes a "fixed" place of business if it is located in a certain place for a sufficient period of time.
- In the case of ISPs, even though they own and operate the servers (i.e. a fixed place of business), they cannot be considered to constitute permanent establishments of the businesses whose websites they host, because they will not have the authority to conclude contracts in the name of the enterprises they host and thus are not agents of those enterprises.
- Whether computer equipment used for e-commerce operations may be considered to be a permanent establishment needs to be examined on a case-by-case basis, depending on whether the equipment is used for activities that form an essential part of the commercial activity of an enterprise (as opposed to being used for merely preparatory or auxiliary activities). In this case, and if the equipment constitutes a fixed place of business, it would be a permanent establishment of the enterprise.[140]

What would be the possible implications for tax revenues of these amendments to Article 5? For example, if a web server constitutes a permanent establishment of a business, and since few resources are needed to set up and maintain a server, it could encourage the migration of servers and computer equipment to low-tax countries, including some of the developing countries. Currently, the United States has the highest concentration of web servers in the

world;[141] should these be considered permanent establishments and thus be subject to direct taxation, the United States may take a minimalist position on income tax to prevent servers from migrating across the border. One problem that needs to be addressed is tracing the legal entity operating a business through a website and identifying the business and its physical location.[142]

Because of the difficulties in defining permanent establishment (and because of its large tax base), the United States has favoured residence-based taxation over source-based taxation. However, residence-based taxation may not favour developing countries, given their small number of residents with e-businesses. In the short run, they are primarily net e-commerce-importing countries; hence, they would have an interest in source-based rather than residence-based taxation. Also, a move to residence-based taxation may shift tax revenues from developing to developed countries once developing countries' share as consumers of e-commerce increases. On the other hand, residence-based taxation favours tax havens, which are often developing countries. Here, developing countries could be attractive to foreign investors looking for certain, low-skilled activities in the production of digital content.

If Article 5 were not amended, countries that are net importers of technology would face significant revenue losses because businesses would close down branches and replace them with Internet communications and e-commerce, which would not be regarded as permanent establishments and would thus be tax-free. Hence, the main business activity would not take place in the country any more, and the country's source-based tax would decrease.

The amendments to Article 5 refer to the definition of permanent establishment as it currently appears. Another OECD group is examining the more important issue of whether any changes should be made to that definition or whether to abandon the concept of permanent establishment altogether. Given that today's technology allows a company to base itself in one or more places and outsource all activities which require physicality, the concept of permanent establishment may become obsolete.

On a related issue, the OECD has discussed whether income from the sale of digital products or services should be characterized as business profits or royalties (OECD, 2001b). While business profits are taxed in the country where the business has permanent establishment, royalty income is taxed by the country from which the royalties arise. A minority of countries argued in favour of classifying digital sales as royalties, arguing that the payment is only for the right to copy.[143] This would allow e-commerce-importing countries to capture tax on sales to their residents, if permitted under their treaties. Developing countries, however, often do not have tax treaties and are net importers of e-commerce. They could, therefore, still tax digital sales to their residents, whether these were classified as royalties or business profits.

(c) A need for global coordination

No matter what changes to the existing tax legislation are adopted, without a certain degree of international cooperation and harmonization of existing tax rules, the expansion of e-commerce will be hampered. Traditionally, tax collection has been based on the belief that individual countries have the right to set their own tax rules; thus, there has been little international cooperation and few multilateral agreements have been concluded. Unless this approach changes and countries agree to enter into multilateral tax agreements, tax competition will intensify with e-commerce. This is a likely scenario since, even within the OECD, individual countries implement domestic tax rules that give them a competitive edge.[144] This is also why it is unlikely that countries will collect taxes for other countries, for example in the case of VAT, where the EU has suggested that VAT be collected from the supplier of the non-member country. On the other hand, if rules are not harmonized internationally, the risk of double taxation may keep foreign suppliers/competition out; and non-taxation may distort competition against local suppliers.

With a few exceptions, developing countries will not be part of an OECD agreement on Internet taxation. Nevertheless, they can use the principles and rules agreed upon as a basis for adjusting their own legislation. One of the first developing countries to develop national legislation on e-commerce, including on taxation, has been India. In December 1999, the Ministry of Finance set up a technical committee on e-commerce taxation, which was expected to submit its report, including recommendations on e-commerce taxation in India, by the end of 2000.

Developing countries have used tax legislation in the past to attract private foreign direct investment (FDI). Multinationals increasingly operate in countries that

have low taxes or are willing to negotiate favourable tax regimes to attract foreign business. In fact, fiscal incentives are the most widely used type of FDI incentives (UNCTAD, 1996). Depending on the agreements adopted in the OECD, developing countries could negotiate specific bilateral treaties for e-commerce taxation, which would give them a competitive edge.[145] For example, the transaction costs of setting up or moving a web server are low; hence, e-commerce allows companies to respond quickly to tax incentives offered by Governments and move their web servers to a developing country.

However, any decision that developing countries may take on modifying their tax legislation to accommodate e-commerce, will have to take into account the significant role of tax revenues in their national budgets. Until new international agreements on e-commerce taxation have been defined, an increasing number of goods and services will be traded online, largely tax-free. In the short to medium term, developing countries will be net importers of e-commerce and will therefore run a greater risk of losing revenues if traditional imports are replaced by online delivery. Therefore, the development of efficient tax collection systems for e-commerce should be a priority for all developing countries.

2. Customs duties

Compared with the debate on e-commerce, where countries in principle agree that e-commerce should be taxed, the debate on whether to levy customs duties on electronic commerce has been more controversial. A number of countries have advocated a tariff-free environment for e-commerce, while others have expressed concern about possible revenue losses if products that have been subject to customs duties in the past are now imported duty-free.

The World Trade Organization (WTO) addressed this issue at its second Ministerial Meeting (Geneva, May 1998), when Ministers agreed to ban the imposition of customs duties on electronic transmissions until the 1999 WTO Ministerial Meeting in Seattle. The Seattle meeting, however, failed to address electronic commerce and a decision on whether to extend the customs moratorium was deferred; it may be considered at the next Ministerial Meeting, to be held in Doha in November 2001.

In the meantime, the discussions in the WTO in the area of e-commerce continue. One of the most controversial points in the debate has been the question of how to define or "classify" digitized products, i.e. products than can be shipped both physically and digitally. These include software, books, printed material, and sound and media products. Traditionally, they have been shipped physically, via carrier media such as CDs, tapes or cassettes. They were physically moved across borders, where they were subject to customs duties. Today, and increasingly so in the future, these products are being sent via data files through virtual networks, thereby crossing numerous (often-unknown) borders. How should these data or their content be classified? Are they equivalent to a hard copy of a book or catalogue, a CD or a videotape and therefore to be classified as a "good"? Is the transmission of the data itself a service, and thus should the "data" fall withing the "services" category? Or should there be a third category of electronic transmissions, some mixture of goods and services - but in that case, which would be the governing multilateral rules?

Within the WTO context, there are important political and regulatory implications associated with the electronic delivery of goods and services. Depending on the classification, the trade is subject to different multilateral rules: goods are subject to the General Agreement on Tariffs and Trade (GATT), the Agreement on Technical Barriers to Trade, the Agreement on Customs Valuations, or rules of origin; while services would be subject to the General Agreement on Trade in Services (GATS).

In general, the multilateral rules for services are still far less elaborate than the multilateral rules for trade in goods, providing countries with substantially more leeway for national policy discretion in the services trade. One important difference between the GATT and the GATS relates to general obligations. While the GATT's general obligations include most favoured nation (MFN), national treatment and a general prohibition on quantitative restrictions, the GATS includes the national treatment principle only in negotiated specific commitments and specific services. For example, WTO member countries have defined in their national schedules whether, for a certain services trade, foreign suppliers will be given national treatment, i.e. whether they are subject to the same rules as domestic suppliers of the equivalent service. In other words, if a country grants national treatment, and if the WTO members decide to include electronic transmissions in the GATS framework, no additional taxes can be imposed on foreign suppliers

by that country. If no national treatment is specified, on the other hand, imports could be subject to higher taxes than domestically supplied services.

A second important difference between the GATS and the GATT relates to the possibility of imposing quantitative restrictions or quotas. While the GATT (in general) prohibits the use of quotas, they are allowed under the GATS (depending on the market access commitment specified in a country's schedule). Thus, theoretically, this could mean that a country could impose (in principle) a limit on, say, the number of books transmitted electronically via the Internet. Although it is not clear how this could be enforced, it is a question that has to be solved in the discu-ssions on how to include e-commerce in the WTO agreements.

3. Fiscal implications of digitized goods trading

Until WTO member States have agreed on whether to (i) extend the customs moratorium, and (ii) classify digitized products as goods or services, discussions will continue on the question of potential tariff revenue losses resulting from the ban on customs duties. As a contribution to the debate, this section will briefly present UNCTAD calculations on tariff and tax revenues currently collected from the import of digitized goods. This will provide countries, in particular in the developing world, with concrete numbers for potential fiscal implications of digitized goods imports.

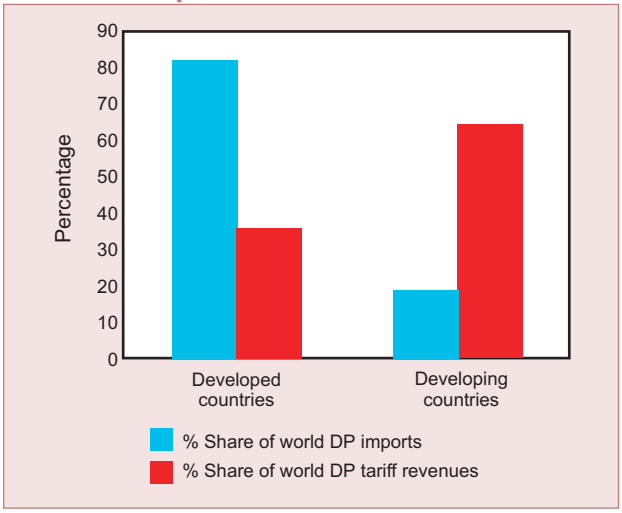
For this purpose, a number of commodities have been selected, which traditionally have been shipped physically and been subject to border tariffs, but which today can be transformed into a digitized format and sent through the Internet. More specifically, these "digitized products" are here defined as goods, identifiable by Harmonized System (HS) headings, that can be sent both physically via carrier media and electronically via networks. They comprise five product categories: (i) printed matter, (ii) software, (iii) music and other media products, (iv) film and (v) video games.[146]

The calculation of fiscal revenue is based on two types of customs duties: first, the MFN applied tariff; and second, additional duties such as customs surcharges and consumption taxes levied on imports.

Table 21 shows fiscal revenue resulting from the MFN tariff levied on digitized products, per country. The majority of countries that are most affected by tariff revenue losses come from the developing world. Given their higher levels of MFN rates applied to these products, this should not come as a surprise. What is remarkable, however, is the magnitude: despite the developing countries' import share in digitized products of only 18.5 per cent, their *absolute* tariff revenue (loss) is almost double that of the developed countries, amounting to 64.5 per cent of world tariff revenue losses for these products (chart 8). This clearly shows that, as far as potential fiscal losses are concerned, developing countries would be much more affected by the proposed ban. The top ten countries affected by fiscal loss are the EU, India, Mexico, Malaysia, Brazil, Canada, China, Morocco, Argentina and Israel.

These losses now need to be placed in the context of total government revenues. Table 22 compares tariff revenues from digitized products with total revenues and revenues from import duties. As has been shown elsewhere,[147] the percentages are relatively low: for all countries, tariff revenues from these products amount to only 0.14 per cent of total government revenues and 1.7 per cent of revenues from import duties. Nevertheless, there are some significant differences between countries, with shares ranging from 0 to 1.1 per cent of total revenue and from 0 to 20 per cent of revenues from import duties. Generally, customs duties as a source of government revenue play a more important role in many developing countries than in developed countries. Hence, a reduction in customs revenues as a result of e-commerce would be felt more strongly in the developing countries.

Chart 8
DP imports and tariff revenues



Apart from the MFN tariff, many countries collect a number of additional duties on their imports, such as customs surcharges and fees and consumption taxes. These additional duties would also be lost if products were "imported" electronically and duty-exempted. Therefore, it is important to consider the amount of those revenues (table 23). Calculations show that, compared with the tariff rates, the rates for additional duties are significantly higher. They account on average for 23.2 per cent (all countries), with a wide range between 0 and 120 per cent. The (on average) high rates are largely due to the relatively high consumption taxes levied on imports, in particular in the developed countries. Consumption taxes on imports of digitized products account for 15.2 per cent (all countries), 17.3 per cent (developed countries) and 14.4 per cent (developing countries).

Given these relatively high rates of additional duties collected on digitized products, revenues resulting from the collection of these duties ought to be high as well. As far as absolute numbers are concerned, table 23 shows that while total tariff revenue from digitized products was $977 million, total revenue from both tariffs and additional duties is now more than $8 billion. A large proportion of this is explained by consumption taxes levied on developed countries' imports ($6.2 billion). The shares of these duties in government revenue now account on average for 0.5 of total government revenue, up from 0.1 per cent (tariff only), an increase of 400 per cent. Shares in import revenues have also changed considerably. The combined tariff and customs surcharges (excluding consumption taxes) amount now to 3.6 per cent of total import revenue, up from 1.7 per cent (tariff only), an increase of more than 200 per cent.

To summarize, fiscal losses from customs duties are small compared with total government revenue, but significant in absolute terms and if additional duties are taken into account. Developing countries suffer higher losses from tariff revenues, while developed countries would mainly be affected by forgone consumption taxes on the import of digitized products. The significant amount of lost consumption taxes highlights the importance of addressing taxation in cyberspace and the need to find an agreement at the international level.

G. Policy recommendations

A legal and policy infrastructure that is supportive of and conducive to electronic commerce is an important prerequisite for the growth of the latter. Thus, the existence of a predictable and supportive legal framework has been singled out as an essential tool to increase the much-needed confidence of both business and consumers in international transactions.[148] As pointed out in a report[149] prepared by the UNCTAD secretariat, the key for developing countries may be to identify: (i) those areas in which an international consensus has emerged on how to treat electronic commerce issues; (ii) those areas where domestic action is absolutely necessary in order to foster an environment favourable to electronic commerce; and (iii) those areas where it is possible for developing countries to resolve the legal issues expeditiously. On that basis, it is suggested that developing countries wishing to accommodate e-commerce might wish to give consideration to the following:

- To ensure that e-transactions are given the same legal effect as traditional paper-based transactions, Governments are urged to examine their legal infrastructure to ascertain whether paper-based form requirements prevent laws from being applied in an e-environment.[150] They might consider using UNCITRAL's Model Law on Electronic Commerce as a basis for preparing new laws or adjusting current ones.
- As regards encryption and electronic signatures, there seems to be a consensus that a mechanism for secure authentication of electronic communication is critical to the development of e-commerce. Such a mechanism must provide for confidentiality, authentication (enabling each party to a transaction to ascertain the identity of the other party) and non-repudiation (ensuring that the parties to a transaction cannot subsequently deny their participation). The new UNCITRAL Model Law on Electronic Signatures and the Guide to Enactment, together with some recent examples of regional legislation on electronic signatures described in this chapter, might guide developing countries wishing to prepare legislation on electronic signatures.
- As pointed out in this chapter, a key element in building trust is to ensure that users and consumers have effective redress for disputes arising from transactions online. Since traditional dispute

settlement mechanisms do not provide effective redress in e-commerce transactions, there is a need to consider ADR/ODR mechanisms that would provide speedy, low-cost redress for a large number of the small claims and low-value transactions arising from consumers' online interactions. It is assumed that the adoption of rules and standards concerning consumer protection, resolution of disputes online and choice-of-court clauses will significantly increase consumer confidence in e-commerce.

- International cooperation is absolutely essential, because of the very nature of e-commerce. It is important in this regard that harmonized rules based on international standards be adopted in order to combat criminal activities, and that judicial cooperation be strengthened.
- In the area of e-commerce taxation, developing countries are encouraged to follow the international debates closely and adjust their own legislation using as a basis the rules and principles agreed upon. Furthermore, they could negotiate specific bilateral treaties for e-commerce taxation, which would give them a competitive edge. Any decision that developing countries may take on modifying their tax legislation to accommodate e-commerce will have to take into account the significant role of tax revenues in their national budgets. In the short to medium term, developing countries will be net importers of e-commerce and will therefore run a greater risk of losing revenues if traditional imports are replaced by online delivery. Therefore, the development of efficient tax collection systems for e-commerce should be a priority for all developing countries.
- Governments of developing countries are encouraged to participate in helping shape the emerging international consensus and to contribute to the preparation of various legal instruments being considered in international forums. To this end, cooperation and coordination among countries with similar problems and concerns are critical in order to ensure that, ultimately, all voices are heard in the various international forums.

Table 21
Applied MFN rates and tariff revenue on DP imports, 1999

Country/Economy	Ave.MFN %	W.MFN %	Tariff revenue ($ 000)	Country/Economy	Ave.MFN %	W.MFN %	Tariff revenue ($ 000)
European Union	1.8	1.5	165 277	Sri Lanka	4.6	8.5	1 462
India	23.1	27.1	110 503	Tanzania, United Rep. of	14.9	12.6	1 358
Mexico	15.6	12.2	104 037	Zambia	16.4	9.5	1 323
Malaysia	7.3	10.5	53 331	Iran, Islamic Rep. of	6.0	2.8	1 320
Brazil	13.3	9.7	43 386	Papua New Guinea	13.4	15.4	1 311
Canada	1.9	0.9	42 776	Bangladesh	16.9	5.4	1 297
China	8.8	7.5	40 138	Barbados	12.1	12.8	1 284
Morocco	30.7	30.7	24 159	Gabon	16.2	10.1	1 268
Argentina	13.6	6.8	22 677	Jordan	19.7	10.7	1 211
Israel	5.9	8.0	21 800	Malta	5.3	3.8	1 192
Thailand	11.3	11.8	21 311	Jamaica	9.7	5.1	1 173
Pakistan	38.7	30.2	20 533	Honduras	7.9	4.7	935
Australia	1.5	1.7	19 639	Costa Rica	5.9	2.0	867
Czech Republic	4.2	4.7	19 534	Belize	12.1	17.5	805
Korea, Republic of	4.0	3.7	18 529	Uganda	7.3	6.3	799
Russian Fed.	12.0	6.9	18 472	Cuba	8.0	6.3	779
Venezuela	9.8	7.9	15 726	Oman	5.0	5.0	725
Poland	5.9	3.1	14 412	Saint Vincent	11.2	18.4	675
Nigeria	11.5	20.6	14 123	Nepal	8.8	7.9	603
Hungary	5.2	5.0	13 886	Mozambique	19.6	13.4	564
Asia (other)	2.7	1.9	12 627	Malawi	13.0	4.9	488
United States	0.3	0.2	12 050	Mali	14.2	17.0	476
Colombia	8.6	8.7	12 023	Maldives	17.5	16.9	419
Philippines	7.1	5.1	11 109	Belarus	12.0	5.9	406
Chile	9.0	9.0	10 817	Bahrain	5.2	2.7	361
Paraguay	11.4	10.9	9 540	Norway	0.1	0.0	352
Egypt	16.7	10.3	8 856	Seychelles	20.4	14.3	349
Peru	12.0	12.0	8 811	Albania	14.7	12.5	326
Saudi Arabia	10.4	8.1	8 574	Georgia	9.9	11.6	318
Algeria	15.3	15.9	8 085	Ethiopia	21.2	8.2	312
Tunisia	23.8	16.3	6 864	Madagascar	3.8	5.3	298
Dominican Republic	14.7	15.3	6 695	Chad	16.2	12.0	293
Romania	12.2	6.9	5 537	Antigua, Barbuda	11.1	8.5	290
South Africa	2.6	1.5	5 414	Nicaragua	3.6	2.2	276
Ukraine	8.0	8.7	5 229	Cent. Afr. Rep	16.2	9.8	266
Uruguay	13.5	8.3	5 120	Saint Lucia	10.9	6.6	242
Latvia	7.4	8.1	5 077	Dominica	11.8	9.1	144
Cote d'Ivoire	16.3	13.6	4 370	Suriname	11.6	8.5	142
Indonesia	9.4	8.2	4 305	Moldova	3.2	2.5	129
Turkey	2.6	2.4	4 297	Saint Kitts and Nevis	11.1	10.6	112
Lebanon	14.7	8.4	4 137	Eq. Guinea	16.2	9.1	105
New Zealand	1.4	1.5	3 981	Grenada	11.2	4.7	102
Libya	23.7	14.3	3 173	Brunei Darussalam	1.3	0.6	84
Panama	6.8	5.1	3 152	Solomon Islands	27.0	5.4	57
Slovenia	5.5	2.8	2 698	Guyana	12.1	1.5	32
Rwanda	45.6	23.4	2 433	Montserrat	12.2	17.4	28
Viet Nam	16.7	17.0	2 371	Bhutan	16.5	16.0	27
Zimbabwe	22.5	18.3	2 349	Sudan	1.5	0.3	12
Ecuador	10.8	4.5	2 209	Bahamas	0.0	0.0	4
Kazakhstan	6.9	9.4	2 124	Hong Kong (China)	0.0	0.0	0
Guatemala	6.7	5.1	2 120	Estonia	0.0	0.0	0
Mauritius	9.7	10.2	2 014	Japan	0.0	0.0	0
Kenya	16.2	9.9	2 004	Kyrgyzstan	0.0	0.0	0
Ghana	12.8	7.8	1 995	Lithuania	0.0	0.0	0
Burkina Faso	29.6	31.5	1 990	Singapore	0.0	0.0	0
Bolivia	8.9	7.1	1 798	Switzerland	0.0	0.0	0
Iceland	3.9	4.4	1 717	Turkmenistan	0.0	0.0	0
Lao, People's Dem.Rep.	9.3	11.8	1 715				
Congo	16.0	15.7	1 512				
El Salvador	5.4	4.1	1 480	**World**	**10.7**	**8.5**	**1 036 973**
Trinidad and Tobago	12.0	9.1	1 480	**Developing countries**	**15.3**	**13.1**	**689 767**
Cameroon	16.2	9.6	1 476	**Developed countries***	**3.6**	**2.9**	**347 206**

Sources: Comtrade, TRAINS.

Note: Excludes intra-EU trade. Excludes imports which are subject to specific tariffs.

* Includes economies in transition.

Table 22
Tariff revenue losses from DP imports per country

Country	DP tariff revenue ($ 000)	DP tariff revenue as % of total rev.	DP tariff revenue as % of imp.rev.	DP tariff revenue as % of tax rev.	Country	DP tariff revenue ($ 000)	DP tariff revenue as % of total rev.	DP tariff revenue as % of imp.rev.	DP tariff revenue as % of tax rev.
European Union	165 277	0.01	1.06	0.01	Mauritius	2 014	0.22	0.85	0.26
India	110 503	0.19	0.96	0.27	Kenya	2 004	0.08	0.54	0.09
Mexico	104 037	0.18	4.30	0.21	Ghana	1 995	0.27	1.35	0.35
Malaysia	53 331	0.22	2.00	0.26	Bolivia	1 798	0.12	2.15	0.15
Brazil	43 386	0.02	0.91	0.03	Iceland	1 717	0.07	5.49	0.08
Canada	42 776	0.03	2.15	0.03	Congo	1 512	0.25	2.56	0.78
China	40 138	0.07	1.06	0.07	El Salvador	1 480	0.11	1.00	0.11
Morocco	24 159	0.24	1.69	0.30	Trinidad and Tobago	1 480	0.10	1.71	0.11
Argentina	22 677	0.06	0.87	0.06	Cameroon	1 476	0.11	0.42	0.13
Israel	21 800	0.05	7.20	0.06	Sri Lanka	1 462	0.05	0.38	0.06
Thailand	21 311	0.11	1.21	0.12	Zambia	1 323	0.26	1.56	0.27
Pakistan	20 533	0.21	1.74	0.28	Iran, Islamic Rep. of	1 320	0.00	0.03	0.00
Australia	19 639	0.02	0.79	0.02	Papua New Guinea	1 311	0.03	0.10	0.03
Czech Republic	19 534	0.11	5.74	0.11	Jordan	1 211	0.06	0.30	0.08
Korea, Republic of	18 529	0.02	0.29	0.02	Malta	1 192	0.11	2.64	0.13
Russian Federation	18 472	0.05	1.06	0.06	Costa Rica	867	0.03	0.62	0.03
Venezuela	15 726	0.09	0.97	0.13	Belize	805	0.57	1.93	0.64
Poland	14 412	0.03	1.06	0.03	Oman	725	0.02	0.35	0.07
Hungary	13 886	0.08	2.47	0.09	Saint Vincent & the Gre.	675	0.67	1.69	0.78
United States	12 050	0.00	0.07	0.00	Nepal	603	0.12	0.45	0.14
Colombia	12 023	0.10	1.39	0.12	Maldives	419	0.24	0.76	0.49
Philippines	11 109	0.09	0.52	0.10	Belarus	406	1.37	20.66	1.49
Chile	10 817	0.07	0.98	0.08	Bahrain	361	0.02	0.23	0.07
Paraguay	9 540	1.01	8.13	1.57	Norway	352	0.00	0.10	0.00
Egypt	8 856	0.04	0.36	0.07	Seychelles	349	0.13	0.33	0.20
Peru	8 811	0.11	1.10	0.13	Albania	326	0.05	0.34	0.07
Algeria	8 085	0.06	0.42	0.06	Georgia	318	0.08	2.20	0.10
Tunisia	6 864	0.12	1.00	0.13	Ethiopia	312	0.03	0.14	0.04
Dominican Republic	6 695	0.25	0.71	0.26	Madagascar	298	0.09	0.17	0.09
Romania	5 537	0.06	1.17	0.07	Nicaragua	276	0.06	0.29	0.06
South Africa	5 414	0.01	0.55	0.02	Moldova, Republic of	129	0.04	1.35	0.05
Uruguay	5 120	0.09	2.80	0.10	Saint Kitts and Nevis	112	0.17	0.48	0.21
Latvia	5 077	0.24	18.77	0.28	Guinea	105	0.01	0.03	0.01
Côte d'Ivoire	4 370	0.19	0.57	0.20	Grenada	102	0.13	0.80	0.16
Indonesia	4 305	0.01	0.72	0.02	Bhutan	27	0.03	2.65	0.09
Turkey	4 297	0.01	0.81	0.01	Bahamas	4	0.00	0.00	0.00
Lebanon	4 137	0.13	0.45	0.18	Estonia	0	0.00	0.00	0.00
New Zealand	3 981	0.01	0.40	0.01	Japan	0	0.00	0.00	0.00
Panama	3 152	0.14	1.40	0.20	Kyrgyzstan	0	0.00	0.00	0.00
Slovenia	2 698	0.04	1.15	0.04	Lithuania	0	0.00	0.00	0.00
Rwanda	2 433	1.19	3.73	1.30	Singapore	0	0.00	0.00	0.00
Viet Nam	2 371	0.05	0.21	0.06	Switzerland	0	0.00	0.00	0.00
Zimbabwe	2 349	0.14	0.86	0.16					
Ecuador	2 209	0.08	0.81	0.10	**Total**	**977 532**	**0.14**	**1.70**	**0.17**
Kazakhstan	2 124	0.14	4.05	0.18	**Developing countries**	**630 326**	**0.16**	**1.44**	**1.44**
Guatemala	2 120	0.12	0.89	0.12	**Developed countries**	**347 206**	**0.04**	**2.70**	**0.05**

Sources: As for table 21.

Table 23
DP revenues from tariffs, additional customs duties and taxes, 1999

Country	DP tariff revenue ($ 000)	DP cons. tax revenue ($ 000)	DP tariff and cust. surch. revenue ($ 000)	DP all imp. duties revenue ($ 000)	DP tariff and cust. surch. as % of imp. rev.	DP all imp. duties as % of imp. rev.	DP all imp. duties as % of tax rev.	DP all imp. duties as % of total rev.
Albania	326	326	326	653	0.3	0.7	0.1	0.1
Algeria	8 085	10 656	49 773	60 429	2.6	3.2	0.5	0.4
Antigua and Barbuda	290	410	376	785	..	..	..	..
Argentina	22 677	69 609	42 348	111 957	1.6	4.3	0.3	0.3
Australia	19 639	436 773	19 639	456 412	0.8	18.3	0.5	0.5
Austria	1 452	185 834	1 452	187 286	0.6	71.8	0.3	0.3
Bangladesh	1 297	3 598	3 216	6 814	..	..	..	..
Barbados	1 284	1 511	1 284	2 795	..	..	..	..
Belarus	406	1 032	467	1 499	23.8	76.3	5.5	5.1
Belgium (Belg./Lux.)	2 606	238 981	24 040	263 021	1.9	20.5	0.2	0.2
Belize	805	691	805	1 496	1.9	3.6	1.2	1.1
Bolivia	1 798	3 809	6 079	9 888	7.3	11.8	0.8	0.7
Brazil	43 386	36 772	87 057	123 829	1.8	2.6	0.1	0.1
Burkina Faso	1 990	946	2 621	3 567	..	..	..	..
Cameroon	1 476	2 872	1 476	4 348	0.4	1.2	0.4	0.3
Canada	42 776	710 261	504 405	1 214 665	25.3	60.9	1.0	0.9
Chad	293	0	523	523	..	..	..	..
Chile	10 817	16 281	10 817	27 098	1.0	2.5	0.2	0.2
China	40 138	80 731	44 968	125 699	1.2	3.3	0.2	0.2
Colombia	12 023	21 406	12 023	33 429	1.4	3.9	0.3	0.3
Congo	1 512	0	5 441	5 441	9.2	9.2	2.8	0.9
Costa Rica	867	5 871	1 368	7 239	1.0	5.2	0.3	0.2
Côte d'Ivoire	4 370	6 414	5 171	11 585	0.7	1.5	0.5	0.5
Cuba	779	0	779	779	..	..	..	..
Czech Republic	19 534	80 702	19 534	100 235	5.7	29.5	0.6	0.6
Denmark	1 336	160 268	1 336	161 604	0.4	51.1	0.3	0.2
Dominica	144	221	238	459	..	..	..	..
Dominican Republic	6 695	18 352	12 902	31 254	1.4	3.3	1.2	1.1
Ecuador	2 209	3 027	2 665	5 691	1.0	2.1	0.2	0.2
Egypt	8 856	12 945	11 445	24 390	0.5	1.0	0.2	0.1
El Salvador	1 480	2 889	1 480	4 369	1.0	2.9	0.3	0.3
Estonia	0	7 793	0	7 793	..	..	0.6	0.5
Ethiopia	312	182	4 679	4 861	2.0	2.1	0.6	0.4
Finland	1 038	51 541	1 038	52 578	0.7	33.5	0.1	0.1
France	8 265	390 312	8 265	398 577	0.5	22.7	0.1	0.1
Gabon	1 268	1 884	1 268	3 152	..	..	..	..
Germany	16 274	405 459	16 274	421 733	0.4	11.5	0.1	0.1
Ghana	1 995	4 147	1 995	6 142	1.4	4.2	1.1	0.8
Greece	685	27 957	685	28 642	0.3	14.2	0.1	0.1
Grenada	102	437	211	649	1.7	5.1	1.0	0.9
Guatemala	2 120	4 399	2 120	6 519	0.9	2.7	0.4	0.4
Guinea	105	0	187	187	0.1	0.1	0.0	0.0
Guyana	32	0	32	32	..	..	..	..
Honduras	935	1 389	1 034	2 423	..	..	..	..
Hong Kong (China)	0	0	332	332	..	..	..	..
Hungary	13 886	73 333	17 379	90 712	3.1	16.2	0.6	0.5
Iceland	1 717	9 515	1 717	11 232	5.5	35.9	0.5	0.4
India	110 503	0	216 547	216 547	1.9	1.9	0.5	0.4
Indonesia	4 305	5 649	4 305	9 954	0.7	1.7	0.0	0.0
Ireland	2 139	102 528	32 469	134 997	12.8	53.1	0.6	0.5
Israel	21 800	80 857	203 695	284 552	67.3	93.9	0.8	0.7
Italy	2 868	262 541	2 868	265 409	0.2	19.3	0.1	0.1
Jamaica	1 173	3 431	1 173	4 604	..	..	..	..
Japan	0	189 482	0	189 482	0.0	2.1	0.0	0.0
Kazakhstan	2 124	7 183	13 418	20 601	25.6	39.2	1.7	1.3
Kenya	2 004	3 244	2 004	5 247	0.5	1.4	0.2	0.2
Korea, Republic of	18 529	49 182	18 529	67 711	0.3	1.0	0.1	0.1
Kyrgyzstan	0	863	1 849	2 712	23.5	34.5	2.2	1.6
Latvia	5 077	11 226	45 615	56 841	..	..	3.1	2.7
Lithuania	0	6 805	0	6 805	0.0	14.1	0.3	0.2
Luxembourg	241				..	..	..	..

Table 23 (contd.)

Country	DP tariff revenue ($ 000)	DP cons. tax revenue ($ 000)	DP tariff and cust. surch. revenue ($ 000)	DP all imp. duties revenue ($ 000)	DP tariff and cust. surch. as % of imp. rev.	DP all imp. duties as % of imp. rev.	DP all imp. duties as % of tax rev.	DP all imp. duties as % of total rev.
Madagascar	298	3 937	1 985	5 922	1.1	3.3	1.8	1.7
Malawi	488	0	1 536	1 536	..	..	..	..
Malaysia	53 331	50 667	53 331	103 998	2.0	3.9	0.5	0.4
Mali	476	0	476	476	..	..	..	..
Malta	1 192	0	1 192	1 192	2.6	2.6	0.1	0.1
Mauritius	2 014	1 742	2 014	3 756	0.8	1.6	0.5	0.4
Mexico	104 037	143 359	111 873	255 232	4.8	10.9	0.5	0.5
Moldova	129	1 061	144	1 206	1.5	12.6	0.5	0.4
Montserrat	28	32	44	77	..	..	..	..
Morocco	24 159	15 742	36 162	51 904	2.5	3.6	0.6	0.5
Mozambique	564	1 755	878	2 633	..	..	..	..
Nepal	603	1 149	603	1 752	0.5	1.3	0.4	0.3
Netherlands	15 684	267 177	15 684	282 861	0.8	14.5	0.2	0.2
New Zealand	3 981	0	37 491	37 491	3.7	3.7	0.1	0.1
Nicaragua	276	3 759	276	4 035	0.3	4.2	0.9	0.9
Nigeria	14 123	2 084	19 608	21 692	..	..	..	..
Norway	352	180 595	0	180 595	0.0	53.3	0.4	0.3
Oman	725	0	725	725	0.3	0.3	0.1	0.0
Pakistan	20 533	8 508	20 533	29 041	1.7	2.5	0.4	0.3
Panama	3 152	3 226	6 877	10 103	3.1	4.5	0.6	0.4
Papua New Guinea	1 311	0	5 045	5 045	0.4	0.4	0.1	0.1
Paraguay	9 540	18 414	9 540	27 954	8.1	23.8	4.6	3.0
Peru	8 811	40 793	8 811	49 603	1.1	6.2	0.7	0.6
Philippines	11 109	19 653	11 109	30 762	0.5	1.4	0.3	0.3
Poland	14 412	99 579	85 998	185 577	6.4	13.7	0.4	0.4
Portugal	555	50 351	555	50 906	0.3	25.2	0.1	0.1
Romania	5 537	18 956	9 963	28 919	2.1	6.1	0.4	0.3
Russian Federation	18 472	67 200	63 524	130 723	3.6	7.5	0.4	0.3
Rwanda	2 433	1 561	3 047	4 608	4.7	7.1	2.5	2.2
Saudi Arabia	8 574	0	12 262	12 262	..	..	..	..
Singapore	0	20 355	0	20 355	0.0	7.5	0.2	0.1
Slovenia	2 698	17 988	5 005	22 993	2.1	9.8	0.3	0.3
Solomon Islands	57	215	57	272	..	..	..	..
South Africa	5 414	56 315	5 414	61 730	0.5	6.3	0.2	0.2
Spain	2 138	152 878	2 138	155 016	0.3	21.7	0.1	0.1
Sri Lanka	1 462	0	9 464	9 464	2.4	2.4	0.4	0.3
Saint Kitts and Nevis	112	157	143	301	0.6	1.3	0.6	0.4
Saint Lucia	242	1 448	443	1 892	..	..	..	..
Saint Vincent & the Grenadines	675	0	767	767	1.9	1.9	0.9	0.8
Sudan	12	0	12	12	..	..	..	..
Suriname	142	0	175	175	..	..	..	..
Sweden	2 690	159 782	2 690	162 471	0.6	38.9	0.2	0.2
Switzerland (Switz/Licht)	0	163 230	0	163 230	0.0	26.5	0.3	0.2
Tanzania, United Rep. of	1 358	3 039	1 358	4 398	..	..	..	..
Thailand	21 311	12 359	21 311	33 670	1.2	1.9	0.2	0.2
Trinidad and Tobago	1 480	2 667	1 480	4 147	1.7	4.8	0.3	0.3
Tunisia	6 864	30 316	6 864	37 180	1.0	5.4	0.7	0.7
Turkey	4 297	42 491	4 297	46 788	0.8	8.8	0.2	0.1
Uganda	799	2 155	799	2 954	..	..	..	..
Ukraine	5 229	13 050	5 229	18 279	..	..	..	..
United Kingdom	25 266	492 775	25 266	518 041	0.9	17.5	0.1	0.1
United States	12 050	0	12 050	12 050	0.1	0.1	0.0	0.0
Uruguay	5 120	14 159	10 969	25 128	6.0	13.8	0.5	0.4
Venezuela	15 726	32 655	17 705	50 360	1.1	3.1	0.4	0.3
Viet Nam	2 371	1 392	2 371	3 764	0.2	0.3	0.1	0.1
Zambia	1 323	2 444	1 323	3 767	1.6	4.4	0.8	0.7
Zimbabwe	2 349	0	6 198	6 198	2.3	2.3	0.4	0.4
Total	**928 922**	**6 037 696**	**2 140 561**	**8 178 257**	**3.6**	**13.3**	**0.6**	**0.5**
Developed countries	**265 167**	**5 102 676**	**1 144 248**	**6 246 924**	**4.9**	**26.9**	**0.4**	**0.4**
Developing countries	**663 755**	**935 020**	**979 784**	**1 914 803**	**2.9**	**6.5**	**0.7**	**0.6**

Sources: As for table 21.

Notes

1 We will not deal in this chapter with business-to-government transactions. See chapter 5 on digital government.

2 We are not in a position to give a full picture of all national case law, but we will try to explain the most important decisions rendered so far in Europe, the United States and a few other countries.

3 This refers to the famous "Declaration of independence of the Internet" , to be found at http://www.eff.org/~barlow/declaration-final.html. This clearly marks a new attack on State-made law in the erroneous belief that the "market" will regulate the Internet by itself.

4 A domain name is a commercial comprehensible alternative to an address Internet Protocol (IP),which web servers use to identify each other on the Internet. The domain name system is the hierarchical system by which easy-to-remember, human-friendly names are associated with Internet locations.

5 The notion of "domicile" in international law is defined as follows: (i) for individuals, it is mostly equated with habitual residence, i.e. a place where the individual presents most of the contact points for his/her personal, family and professional lives; (ii) for corporations or other legal entities, legal systems vary in their definitions. Thus, in some systems, a corporation is domiciled at the place of incorporation and in others the main centre of activity or principal establishment is the essential contact point. A third category would also accept the place where a branch or another establishment is situated. So far, all attempts to agree on a single definition worldwide have failed, and international agreements usually respect the different variations described above. For an example of this, see Article 3 of the Hague preliminary draft Convention on Jurisdiction and Foreign Judgements in Civil and Commercial Matters (accessible on www.hcch.net, work in progress).

6 This does not mean that specific rules are automatically needed. In fact, as demonstrated below, existing rules may very often be enough to deal with questions posed by the use of the Internet.

7 This is the conclusion reached in 1997 at the Utrecht Colloquium, reproduced in Boele-Woelki and Kessedjian (1985, p. 143).

8 That is to say, where they are domiciled (see note 5 above).

9 The issue of anonymity is a difficult one. It is linked with the responsibility which Internet service providers (ISPs) have to disclose the names of persons using their services. This is a major controversy, partially addressed in national laws adopted recently for Internet activities. In summary, it can be said that ISPs are not responsible for content when their role is only one of transport. However, no law directly addresses the potential obligation of ISPs to disclose information they possess. This is a question which will have to be addressed sooner or later at the international level.

10 Work was initiated by the United States in 1992. After a few years of preliminary studies, negotiations started in June 1996 and culminated in October 1999 with the adoption of the preliminary draft convention to be found on the Conference's website (www.hcch.net) under the heading "work in progress". On the site can also be found all preliminary documents drafted to help the negotiations and the explanatory report written by Mr. Peter Nygh and Mr. Fausto Pocar, co-rapporteurs for the draft.

11 The Hague Conference organized a colloquium in 1997 Boele-Woelki and Kessedjian, 1998. In September 1999, the Hague Conference organized a round table in cooperation with the University of Geneva, to review all aspects of the private international law of the Internet. The report of that round table is included in a more general report on the information society available on the Hague Conference site, under the heading "Special Commission on General Affairs and Policy", as Preliminary Document No.7, (ftp://hcch.net/doc/gen_pd7e.doc).

12 In the ABA project, the word "jurisdiction" stands for both adjudicatory jurisdiction and applicable law. The report on the study was released in public in New York and London in July 2000. It is the product of a Working Group on Cyberspace, set up by the ABA in 1998, entitled "Transnational issues in cyberspace: A project on the law relating to jurisdiction". The Working Group consisted of sub-groups, dealing respectively with (i) advertising and consumer protection, (ii) data protection, (iii) intellectual property, (iv) payment systems and banking, (v) public law gaming, (vi) sale of goods, (vii) sale of services, taking tele-medicine as an example, (viii) securities and (ix) taxation. The report may be accessed at www.kentlaw.edu/cyberlaw.

13 The GBDe has a website at www.gbde.com.

14 The ILPF has a website at www.ilpf.org.

15 We will not deal at length with arbitration in this report. The literature on arbitration, is considerable and the specific problems with arbitration and e-commerce are not so complicated that they need extensive discussion. The one question which was debated at length was the writing requirement in the New York Convention of 1958. But as in the case of all writing requirements in international conventions or national law, the solution is to be found in the authentication and electronic signature systems which are now admitted by an ever increasing number of legal systems. The second question

posed by online arbitration relates to the "place of arbitration". However, this is also being solved by the consensus achieved on the fact that the place of arbitration is a legal fiction which is useful for the law applicable to the arbitration process and, potentially, to the procedure. Thus, favouring online arbitration does not mean that a place of arbitration must not still be chosen by the parties. See the debate at the Geneva Round Table in September 1999 (Hague Conference on Private International Law, 1999).

16 In the present discussions, it is customary to attack the judicial systems for being inefficient, too slow and too expensive and, therefore, not suitable to e-commerce disputes. Even though it is true that judicial systems around the world need some reform, it is dangerous to give the impression that societies can do without them. The increasing privatization of justice has its limits, particularly because, as mentioned earlier, if society increasingly relies on contract, the justice system cannot also rely only on contract. A contractual relationship is first and foremost, a relation of force. The justice system must be able to restore the balance when necessary.

17 All preliminary documents for this project are available at http://hcch.net/, under the heading "work in progress.

18 The Brussels Convention of 27 September 1968 is in force between all members States of the European Union and will be replaced by a European Regulation owing to the entry into force of the Amsterdam Treaty amending the Treaty on the European Community. The new Regulation was adopted on 22 December 2000 (published in OJEC L12, 22 December 2000) and will enter into force on 1 March 2002.

19 The Lugano Convention of 16 September 1988 was negotiated between the EU member States and the States party to the EFTA Agreement. The Lugano Convention can also be adhered to by non-EFTA countries. This is the case of Poland, which became a party to it in 1999.

20 It was adopted by the Special Commission in October 1999. The draft can be accessed at the following address: http://www.hcch.net/e/conventions/draft36e.html.

21 These forums are too numerous to be cited *in extenso* here. However, mention must be made of the work done at informal meetings within the Hague framework; by the European Union both for the revision of the Brussels and Lugano Conventions and for the electronic commerce Directive; the numerous discussions in the United States with non-governmental organizations such as ILPF and the ABA and with government bodies (see particularly the Federal Trade Commission (FTC) and Department of Commerce workshops (http://www.ftc.gov/bcp/altdisresolution/index.htm).

22 For example, in some common-law countries the jurisdiction conferred on the chosen court is not exclusive unless the parties have so indicated.

23 See note 15 above.

24 For this notion, see, for example, C. Kessedjian (in Hague Conference on Private International Law, 1999).

25 In all jurisidictional discussions, it is assumed that the defendant's forum is always available even though, in some countries, flexible theories such as that of *forum non conveniens* may apply to the defendant's forum.

26 See the Report on the Ottawa Expert meeting at ftp://hcch.net/doc/jdgmpd12.doc. The Geneva Round Table reached the same conclusion (see Hague Conference on Private International Law, 1999).

27 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce' OJ L 178 17.07.2000 p.1.*)*.

28 They are too numerous to be cited. Suffice it to say that they emanate both from international governmental organizations such as the OECD and from NGOs such as the ICC.

29 See the discussion below in paragraphs 2.1.5 and 6.1 (A).

30 For the purposes of this chapter, the word "services" is a term of convenience; it has no legal implications.

31 For a thorough analysis of legal provisions applying to consumers or currently proposed by a number of countries and some international organizations, see Andrews (2000).

32 For further details on BOTs, see the ABA report cited in note 12.

33 See, for example, the discussions at the FTC/Department of Commerce Seminar in Washington, DC, in June 2000, http://www.ftc.gov/bcp/altdisresolution/index.htm.

34 This concept is found in Article 11 of the EU Investment Directive (93/22).

35 Insurance companies have started to offer special coverage for some judicial and legal protection when doing business over the net.

36 This is already what some sellers on the net do. The potential buyer is asked to state, before he/she starts shopping, whether he is buying for his/her personal use or for professional reasons. In the latter case, the price offered is lower.

37 The text of Article 7 reads as follows:

"Article 7 Contracts concluded by consumers

1. A plaintiff who concluded a contract for a purpose which is outside its trade or profession, hereafter designated as the consumer, may bring a claim in the courts of the State in which it is habitually resident, if

a) the conclusion of the contract on which the claim is based is related to trade or professional activities that the defendant has engaged in or directed to that State, in particular in soliciting business through means of publicity, and

b) the consumer has taken the steps necessary for the conclusion of the contract in that State.

2. A claim against the consumer may only be brought by a person who entered into the contract in the course of its trade or profession before the courts of the State of the habitual residence of the consumer.

3. The parties to a contract within the meaning of paragraph 1 may, by an agreement which conforms with the requirements of Article 4, make a choice of court

a) if such agreement is entered into after the dispute has arisen, or

b) to the extent only that it allows the consumer to bring proceedings in another court."

38 See note above 18.

39 This is attested by the fact that, at present, in Europe, not few than eight Directives apply to the protection of consumers which are said to be equally applicable to Internet dealings. See the answer given by Mr. Bolkestein on behalf of the European Commission to the European Parliament on 17 November 1999 (OJEC C303E of 24 October 2000, p.10).

40 See section 2 below.

41 See Articles 13 to 15 of the Brussels and Lugano Conventions and Articles 15 to 17 of the new Regulation replacing the Brussels Convention. This attitude was confirmed by the European Court of Justice on 27 June 2000 in the joint cases C-240/98 to C-244/98. The Court said in point 24: "It follows that where a jurisdiction clause is included, without being individually negotiated, in a contract between a consumer and a seller or supplier within the meaning of the Directive and where it confers exclusive jurisdiction on a court in the territorial jurisdiction of which the seller or supplier has his principal place of business, it must be regarded as unfair within the meaning of Article 3 of the Directive in so far as it causes, contrary to the requirement of good faith, a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer."

42 See, for example, *Mark Williams et al vs. America Online Inc*, a Superior Court decision rendered in February 2001. The court was seized of a class action against America Online for problems that appeared after AOL 5.0 was installed on clients' computers. The court refused to transfer the case to Virginia, which was the chosen forum in the contract.

43 The report published by the Working Group of the American Bar Association in July 2000 (cited above in footnote 12) discusses this development and its limitations. See also the discussion in Kessedjian (2000).

44 For example, some would use the language as a criterion for targeting, while others would use the currency. But would the use of English or the dollar be really meaningful?

45 We define "tort" as an "act which causes harm to a determinate person, whether intentionally or not, not being the breach of a duty arising out of a personal relation or contract, and which is either contrary to law, or an omission of a specific legal duty, or a violation of an absolute right". Burke, J., "Osborn's Concise Law Dictionary", Sweet & Maxwell, London, 1976, p. 327.

46 The questions posed by ISP's responsibility will not be developed here.

47 We had access only to the English translation prepared by the office of Steptoe and Johnston. The document is available at http://www.steptoe.com/webdoc.nsf/Files/ItalySupCt/$file/ItalySupCt.doc. The case involved defamation and insults on a site, owned by a foreign resident, against an Italian resident. The Italian Supreme Court decided that Italy had jurisdiction since end-users connect to the site from Italian territory.

48 After the French decision was rendered, German courts began to reconsider asserting jurisdiction in similar cases. See Reuters News, 19 February 2001.

49 In a civil case, a Canadian Appellate decision refused to enforce a Texas judgement rendered between two Canadian residents (*Braintech, Inc. V. Kostiuk (1999)* 171 D.L.R. (4th) 46). Texas asserted jurisdiction on the basis of the fact that the defamatory data were accessible in Texas. The Canadian court decided that the link was too tenuous and that Texas did not have jurisdiction. One must add, to fully understand this decision, that the Texas decision was rendered *ex parte* since the defendant did not appear in the proceedings in that State.

50 The text of Article 10 reads as follows :

"*Article 10 Torts or delicts*

1. A plaintiff may bring an action in tort or delict in the courts of the State :

a) in which the act or omission that caused injury occurred, or

b) in which the injury arose, unless the defendant establishes that the person claimed to be responsible could not reasonably have foreseen that the act or omission could result in an injury of the same nature in that State.

2. Paragraph 1 *b)* shall not apply to injury caused by anti-trust violations, in particular price-fixing or monopolization, or conspiracy to inflict economic loss.

3. A plaintiff may also bring an action in accordance with paragraph 1 when the act or omission, or the injury may occur.

4. If an action is brought in the courts of a State only on the basis that the injury arose or may occur there, those courts shall have jurisdiction only in respect of the injury that occurred or may occur in that State, unless the injured person has his or her habitual residence in that State."

51 A third question arises in the context of the draft Hague Convention: What level of interactivity must a site be shown to possess, or what level of targeting must it comprise, for it to be regarded as a "regular commercial activity" within the meaning of Article 9? This question will not be discussed in this report since the notion of "regular commercial activity" is a very controversial one and has not yet been defined with enough precision to be considered as reflecting a general consensus.

52 See the Electronic Commerce Directive, cited in footnote 27 above.

53 See the Report of the Ottawa meeting, cited in footnote 26 above.

54 See "Clarification on the application of the permanent establishment definition in e-commerce: Changes to the commentary on Article 5 of the model tax convention", OECD, January 2001. For further details, see paragraph 6.1 (B).

55 The Act amends Section 43 of the Trademark Act of 1946 (15 U.S.C. 1125) and is cited as 15 U.S.C. §1125(d).

56 On 20 February 2001, Law.com reported that more than 700 lawsuits had been filed in the United States using the Act.

57 For an analysis of the ICANN arbitration rules and their relations with court jurisdiction, see Kessedjian (2000b, pp. 69-96).

58 It may be noted that for all generic Top Level Domains (TLDs,) such as .com and .net, there is a concentration of litigation in Virginia since the registrar is located in that State.

59 United States District Court for the Eastern District of Virginia, December 2000.

60 Only three meetings are mentioned here because it is not possible to mention all of them.

61 Http://dsa-isis.jrc.it/ADR/workshop.html.

62 The variety of ADR systems within the European Union is best illustrated in a document prepared by the European Commission in the financial services area. Accessible via the Internet at http://europa.eu.int/comm/internal_market/en/finances/consumer/intro.htm, it allows access to pages for each country, indicating the main features of the ADR system proposed in that country together with the addresses of the authority responsible for maintaining the system.

63 The complete documentation for this meeting can be consulted at www.ecommerce.gov/adr.

64 The documents are available at http://www.oecd.org/dsti/sti/it/secur/act/online_trust/presentations.htm.

65 The statement was released on 18 December 2000. It is available at http://www.ecommerce.gov/joint_statements/EU_ADR1-5-01.html.

66 The first result of this work was the New York Convention of 1958 on the enforcement of foreign arbitral awards. The Convention is now in force in 125 States and is applied satisfactorily in the great majority of cases. The list of States Party to the New York Convention may be accessed at http://www.uncitral.org/en-index.htm. The UNCITRAL rules of arbitration are also very useful for ad hoc arbitration. The 1985 UNICTRAL arbitration model law has also helped harmonize arbitration laws around the globe.

67 This is particularly important when the arbitration process takes place entirely online.

68 See, for example, the seven principles included in the EU Recommendation No. 257/98. Also the joint statement by the United States and the European Union cited above gives some guidelines on common basic principles. A very thorough study of the ODR systems already existing and how they apply the common principles mentioned in the text was released by Consumers International in December 2000 (Consumers International, 2000).

69 The full text of the Uniform Domain Name Dispute Resolution Policy, adopted on 26 August 1999, and the Rules of Procedure are available at http://www.icann.org/udrp/udrp-rules-24oct99.htm.

70 Establihed in October 1998, ICANN is a non-profit, private sector corporation formed by a broad coalition of the Internet's business, technical, academic and user communities. It has been recognized by the United States Government as the global consensus entity to coordinate the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters and the management of the root server system. See http://www.icann.org.

71 Convention on the Applicable Law to Contractual Obligations. See consolidated version OJEC C027 of 26 January 1998.

72 It must be noted that although the Rome Convention and the future Regulations are European texts, they apply to all cases coming before European courts even though no European member States, domestic law is involved. The rationale behind this solution is to unify all conflict rules within the member States so that there are not two sets of conflict rules, one for European cases (how to define those?) and one for non-European cases.

73 This matter was discussed at length at the May 2000 meeting of the Hague Conference on Private International Law. It was decided that applicable law is one of the topics to be kept on the agenda for the work done on legal norms adapted to the information society. See ftp://hcch.net/doc/concl_e.doc.

74 Practice is not uniform in this respect. Some contracts refer to Internet usages (see, for example, contracts proposed by UUNET, Prolink or Strato) or to what is known as "netiquette" (contracts proposed by Club Internet or Exceed).

75 In the security brokerage market, regulators such as the Securities and Exchange Commission (SEC) in the United States and the Commission des opérations de bourse (COB) in France have warned Internet brokers that they may have to comply with security-offering laws in the country where the client is located.

76 See paragraph 2.1.

77 As mentioned earlier, the Rome Convention of 1980 unifies the conflict rules in ten member States of the European Union for all cases where there is a question of applicable law. The parties to the Convention are Austria, Finland, France, Germany, Greece, Luxembourg, the Netherlands, Portugal, Spain and Sweden. Because of the Amsterdam Treaty, the Convention should be transformed into a Regulation which will then apply directly to all member States.

78 For a list of all codified rules as of 1986 see Vassilakakis (1987). Since then, many other countries have codified their private international rules, e.g. Tunisia.

79 Two main conventions may be cited here. The 1955 Convention on the Law Applicable to Sales of Goods (http://www.hcch.net/f/conventions/text03f.html) and the 1978 Convention on the Law applicable to Agency (http://www.hcch.net/e/conventions/text27e.html).

80 See paragraph 2.1.3 above.

81 See the Yahoo! case in France. For case law in the United Kingdom, see Vick et al. (1999, p. 58).

82 The latest meeting held in this regard took place at the World Intellectual Property Organization (WIPO) in Geneva on 30 and 31 January 2001.

83 See the Yahoo! case in France.

84 Everyday information collected over the net brings new stories about inappropriate sales of data banks containing personal data.

85 For example, courts which previously worked under legal norms allowing for public access to court documents are now wondering whether this rule can still be applied without any limitations, in view of Internet techniques (see Groner (2000)).

86 This Convention may be found at http://www.coe.fr/dataprotection/edocs.htm. It is a Convention adopted under the auspices of the Council of Europe which is a different organization from the European Union. The European Community became a party to that Convention with effect from 1999 (http://www.coe.fr/dataprotection/Treaties/amend108e.htm). The European Council has also adopted a Recommendation No.R(99)5 for the Protection of Privacy on the Internet (23 February 1999).

87 Directive 95/46/CE of the European Parliament and Council of 24 October 1995, OJEC L 281, 23 November 1995, p. 31.

88 Proposed Directive of the European Parliament and Council presented by the Commission on 25 August 2000, OJEC C365E, 19 December 2000, p .223.

89 OJEC L215 of 25 August 2000, p. 1.

90 OJEC L215 of 25 August 2000, p. 4.

91 OJEC L215 of 25 August 2000, p. 7.

92 http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp39en.pdf.

93 See the Australian Privacy Amendment Act 2000, finally approved on 22 December 2000 (www.privacy.gov.au).

94 For concerns over corporate actions not respecting principles of privacy see Krebs (2001). See also Weber (2001). Mention should be made of an attempt by Senator John Edwards (Democrat, North Carolina) for the United States Congress to legislate on privacy. He introduced a bill on 29 January 2001, even though in 2000 Congress had considered more than two dozens bills on privacy but had failed to enact laws.

95 Recommendation by the OECD Council of 23 September 1980. See http://www.oecd.org/e/droit/doneperso//ocdeprive/priv-en.htm.

96 This document is published under the reference DSTI/ICCP/REG(97)6/FINAL, accessible on the OECD website, www.oecd.org.

97 DSTI/ICCP/REG(98)5/FINAL, accessible at www.oecd.org.

98 This inventory is published under the reference DSTI/ICCP/REG(98)12/FINAL.

99 This Declaration is included in the Conclusions of the Ottawa Conference, published under the reference SG/EC(98)14/FINAL.

100 See paragraph 22.

101 In this connection, it is important to note that the Geneva Round Table (Committee IV) concluded in similar fashion. See the document mentioned in note 26 above.

102 See http://www.oecd.org/dsti/sti/it/secur/act/online_trust/presentations.htm.

103 For a survey of digital signature law, see http://rechten.kub.nl/simone/ds-lawsu.htm and http://www.mcbridebakercoles.com/ecommerce/international.asp.

104 Already in 1996 the Commission of the European Communities noted: "for e-commerce to develop, both consumers and businesses must be confident that their transaction will not be intercepted or modified, that the seller and the buyer are who they say they are, and that transaction mechanisms are available, legal, and secure. Building such trust and confidence is the prerequisite to win over businesses and consumers to e-commerce." A European Initiative in Electronic Commerce, (COM (97) 157 final, 16 April, 1997); http://www.spa.org/govmnt/govnews.htm.

105 The Internet Law and Policy Forum proposed the following additional principles : respect for freedom of contract and parties' ability to set provisions by agreement; making laws governing electronic authentication consistent across jurisdictions; preventing discrimination and erection of non-tariff barriers; allowing for the use of current or future means of electronic authentication; and promoting market-driven standards. See http://www.ilpf.org/digsig/intlprin.htm.

106 See Smedinghoff and Hill Bro (1999).

107 See OECD (1999).

108 See Kuner and Baker (2000) and Aalberts and van der Hof (1999).

109 Available at http://www.uncitral.org.

110 The United States Electronic Signatures in Global and National Commerce Act follows the minimalist approach. It gives e-signatures the same legal validity as traditional paper signatures and explicitly forbids the denial of an electronic agreement simply because it is not in writing. To prevent conflicting State-level approaches, the law further forbids any State statute or regulation that limits, modifies or supersedes the Federal Act in a manner that would discriminate for or against a particular technology.

111 A number of international organizations, such as the OECD and the ICC, have also been involved in electronic authentication issues. See http://www.ocde.org/dsti/sti/it/secur/ and http://www.iccwbo.org/home/menu_electronic_commerce.asp.

112 The Directive was published on 19.January.2000 in the *Official Journal of the European Communities*. According to article 13, Member States should implement it not later than 19 July 2001. For the full text of the Directive, see http://europa.eu.int/ISPO/ecommerce/legal/digital.html.

113 See Schlechter (1999).

114 See Article 2 (2).

115 See Article 3 (1) and (2).

116 See the Commission Decision of 6 November 2000 on the minimum criteria to be taken into account by member States when designating national bodies responsible for the conformity assessments of secure signature-creation devices. *Official Journal of the European Communities* L 289/42 of 16 November.2000. Available at http://europa.eu.int/comm/trade/index_en.htm.

117 See Article 6.

118 Article 7 provides that where the law requires a person to sign a document, that requirement is met if a method is used to identify the person and indicate his or her approval of the document, and if that method is as reliable as appropriate in the light of all the circumstances, including any relevant agreement.

119 "The MLES was prepared on the assumption that it would be directly derived from Article 7 of the UNCITRAL Model Law on Electronic Commerce and would be considered as a way of providing detailed information about the concept of a reliable "method used to identify" a person and "to indicate that person's approval" of the information contained in a data message. UNCITRAL document A7CN.9/WG.IV/WP.71, paragraph 49.

120 The UNCITRAL Model Law on Electronic Signatures and the Guide to Enactment, as well as the background documentation, can be found at http://www.uncitral.org/en-index.htm.

121 See Gregory (2001).

122 See the preamble to UNCITRAL (2001).

123 The UNCITRAL criteria coincide with the requirements set out in the EU Directive for defining "advance electronic signature".

124 The UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996), with additional article 5 *bis* as adopted in 1998, can be found at http://www.uncitral.org/en-index.htm. A discussion of many of the provisions of the Model Law may be found in UNCTAD (1998). paras. 15-23 and 93-179.

125 According to the information provided by UNCITRAL, as of 17 January 2001, the following countries or territories have adopted legislation based on the Model Law: Australia, Bermuda, Colombia, France, Hong Kong Special Administrative Region of China, Mexico, Ireland, Republic of Korea, Singapore, Slovenia, the Philippines, and the States of Jersey (Crown Dependency of the United Kingdom of Great Britain and Northern Ireland), as well as, within the United States of America, the State of Illinois. See http://www.uncitral.org/en-index.htm.

126 See survey conducted by the Economic Commission for Europe (ECE) published on 22 July 1994 (TRDE/WP:4/R.1096), as revised on 25 February 1999 (TRADE/CEFACT/1999/CRP.2). Available at http://www.unece.org/cefact/.

127 See Articles 39, 40 and 41 of the Vienna Convention on the Law of Treaties, 1969, concerning "amendment and modification" of treaties.

128 See document TRADE/CEFACT/1999/CRP.7 of 26 February 1999. Available at http://www.unece.org/cefact/.

129 See United Nations document A/CN.9/WG.IV/WP.89. Available at http://www.unece.org/cefact/.

130 See the Report of the Working Group at its 38th session, A/CN.9/484, April 2001, pp. 81–86.

131 Directive of 8 June 2000, *Official Journal of the European Communities*, 17 July 2000. The full text of the Directive is available at http://europa.eu.int/ISPO/ecommerce/legal/legal.html#frame. See footnote 27 above.

132 See Recommendation No. 31 of March 2000 (ECE/TRADE/257). The full text of the E-Agreement is available at http://www.unece.org/cefact/. See also "The Model Interchange Agreement for the International Use of Electronic Data Interchange", adopted by UN/ECE WP.4 in March 1995 as Recommendation No. 26.

133 See Recommendation No.32 on E-Commerce Self-Regulatory Instruments (Codes of Conduct), ECE/TRADE/277, March 2001. Available at http://www.unece.org/cefact/.

134 An earlier OECD proposal on basic principles of international e-commerce taxation made reference to developing countries, stating that "any tax arrangements adopted domestically and any changes to existing international tax principles should be structured to ensure a fair sharing of the Internet tax base between countries, particularly important as regards division of the tax base between developed and developing countries" (Owens, 1997). However, this principle was not included in the final set of basic principles agreed upon in 1998 (OECD, 1998a).

135 There are, however, also barriers that could prevent this shift, such as other regulatory obstacles (besides taxation), delivery problems, or cultural and linguistic barriers. To circumvent these, some United States suppliers have started to buy local competitors in Europe (*The Economist*, "A survey of e-commerce", 26 February 2000).

136 For details and facts about EU VAT rules, see European Commission (1997a). The complexity of the existing EU VAT system is considered by business to be a major barrier to developing e-commerce in Europe.

137 This regulation was put in place in 1993 under the "transitional VAT arrangements", with the objective of removing border controls for tax purposes inside the European Community.

138 Guidelines for defining "place of consumption" have been prepared by the OECD Working Party on Consumption Taxes (OECD, 2001a) and are currently being discussed by OECD member States.

139 The United States is again a different case: United States citizens are subject to taxation on their total global income in the United States, no matter whether they are resident in the United States or in any other country. United States taxation law allows them, however, to offset the taxes paid in their country of residence against their United States tax liability.

140 OECD member countries have not yet agreed on what the "core functions" of an enterprise could be.

141 According to *The Economist* ("A survey of e-commerce", 26 February 2000), the United States currently accounts for 90 per cent of commercial websites.

142 For example, if Amazon.com posts its link on another business' website/server, this does not constitute a permanent establishment.

143 In their final conclusions, however, OECD member countries agreed that payments related to transactions that "permit the customer to electronically download digital products for the customer's own use or enjoyment" do not constitute royalties. On the other hand, if the downloaded product is commercially exploited (i.e. reproduced and sold), the payments would be classified as royalties (OECD, 2001b).

144 And even within the EU, VAT differs among member States.

145 Bermuda is currently examining how to attract foreign business in the light of e-commerce, on the basis of its previous success in attracting the insurance industry through its "no tax" policy (Storie and Green, 1999).

146 Detailed information about the products included here (such as their corresponding HS headings), the methodology employed in the data collection and analysis, as well as tables on trade flows, tariff levels and revenues, are provided in Teltscher (2000).

147 Perez-Esteve and Schuknecht (1999).

148 In many of the joint statements which the United States has signed with other countries, it has been underlined that «The role of government is to provide, where necessary, a clear, consistent and predictable legal framework, to promote a pro-competitive environment in which electronic commerce can flourish and to ensure adequate protection of public interest objectives.»

149 UNCTAD (1999).

150 As pointed out by some commentators, the traditional paper-based rules governing the form of legal transactions could be extrapolated by national courts and other national authorities to cover paperless trade. The difficulties of such an approach stem not only from the time needed to extrapolate them but also from uncertainty about its consequences and from the lack of harmonized solutions at an international level.

References and bibliography

Aalberts, B.P. and van der Hof, S. (1999). *Digital Signature Blindness, Analysis of Legislative Approaches toward Electronic Authentication*, November, http://cwis.kub.nl/~frw/people/hof/ds-fr.htm.

American Bar Association (2000)."Transnational issues in cyberspace: A project on the law relating to jurisdiction", www.kentlaw.edu/cyberlaw.

Andrews, S. (2000) *The Consumer Law Sourcebook 2000: Electronic Commerce and the Global Economy*, Washington DC, Electronic Privacy Information Center.

Australian Privacy Amendment Act 2000, 22 December 2000, www.privacy.gov.au.

Bleuel, J. and Stewen, M. (2000). "Value added taxes on electronic commerce: Obstacles to the EU Commission's approach ", in *Intereconomics*, July/August 2000, pp. 155-161.

Boele, K. and Kessedjian, C. (1998). "Internet, which court decides, which law applies?" The Hague, Kluwer Law International, p. 143.

Consumers International (2000). "Disputes in cyberspace – Online dispute resolution for consumers in cross-border disputes – An international survey", http://www.consumersinternational.org.

Economic Commission for Europe (ECE) (1995). *The Model Interchange Agreement for the International Use of Electronic Data Interchange*. Recommendation No. 26, UN/ECE WP.4, March.

Economic Commission for Europe (ECE) (2000). *E- Agreement*. Recommendation No. 31 of March 2000, ECE/TRADE/257, http://www.unece.org/cefact/.

Economic Commission for Europe (ECE) (2001). *Draft Recommendation on E-Commerce Self-Regulatory Instruments (Codes of Conduct)*, TRADE/CEFACT/ 2001/14, 15 January, http://www.unece.org/cefact/.

European Commission (1995). *Directive 95/46/CE of the European Parliament and Council of 24 October 1995*, OJEC L 281, 23 November 1995, p. 31.

European Commission (1997a). *VAT in the European Community*, XXI/541/97, EC, DGXXI, January.

European Commission (1997b). *A European Initiative in Electronic Commerce* (COM (97) 157 final, 16 April, http://www.spa.org/govmnt/govnews.htm.

European Commission (1998). *Financing the European Union. Commission Report on the Operation of the Own Resources System*, DGXIX, October, www.europa.eu.int/comm/dg19/agenda2000/ownresources/html/index.htm.

European Commission (1999). *Indirect Taxes and E-commerce*, Working Paper, Working Party No. 1, DG XXI, June.

European Commission (2000a). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EEC) No. 218/92 on administrative co-operation in the field of indirect taxation (VAT) and Proposal for a Council Directive amending Directive 77/388/EEC as regards the value added tax arrangements applicable to certain services supplied by electronic means*, COM (2000) 349 final, 7 June.

European Commission (2000b). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *Official Journal of the European Communities* L 178, 17 July, http://europa.eu.int/ISPO/ecommerce/legal/legal.html#frame.

European Commission (2000c). Decision of 6 November 2000 on the minimum criteria to be taken into account by member States when designating national bodies responsible for the conformity assessments of secure signature-creation-devices, *Official Journal of the European Communities* L 289/42, 16 November, http://europa.eu.int/comm/trade/index_en.htm.

European Commission (2000d). Proposed Directive of the European Parliament and Council on the protection of personal data, *Official Journal of the European Communities* C365E, 19 December, p. 223.

Federal Trade Commission/Department of Commerce Seminar (2000). *Joint Workshop on Alternative Dispute Resolution for Online Consumer Transactions*, 6 and 7 June 2000, Washington, DC, http://www.ftc.gov/bcp/altdisresolution/index.htm.

Goolsbee, A. (1999). *In a World without Borders: The Impact of Taxes on Internet Commerce*, National Bureau of Economic Research Working Paper No. 6863, Cambridge, MA.

Gregory, J. (2000). "UNCITRAL meeting on electronic signatures", October, http://rechten.kub.nl/simone/gregory.htm.

Groner, J. (2001) "Court consider privacy perils of electronic filing", *Legal Times*, 16 January.

Hague Conference on Private International Law (1999). *Geneva Round Table on the Questions of Private International Law raised by Electronic Commerce*, September, http://hcch.net/doc/gen_pd7e.doc.

ICANN (1999). *Uniform Domain Name Dispute Resolution Policy and Rules of Procedure*, 26 August, http://www.icann.org/udrp/udrp-rules-24oct99.htm.

Kerrigan, A. (1999). "Taxation of e-commerce. Recent developments from a European perspective", in *Wirtschaftspolitische Blätter*, 5/1999, pp. 439–447.

Kessedjian, C. (2000a). "Aspects juridiques du e-trading: règlement des différends et droit applicable", in Thévenoz, and Bovet, *Journées 2000 de droit bancaire et financier*, Bern, Stämplfli 2001, pp. 65–97.

Kessedjian, C. (2000b) "Internet et le règlement des différends", in Grosheide, F.W. and Boele-Woelki, K. (eds.), *Molengrafica* 1999/2000, Koninklijke Vermande, pp. 69–96.

Krebs, B. (2001) "Self-regulation champions dig own graves", *Newsbytes*, 30 January.

Kuner, C. and Baker, S. (2000). "An analysis of international and digital signature implementation initiatives". Study prepared for the Internet Law and Policy Forum, September, http://www.ilpf.org/digsig/analysis_IEDSII.htm.

Lukas, A. (1999). *Tax Bytes: A Primer on the Taxation of Electronic Commerce*, Cato Institute for Trade Policy Analysis No. 9, Washington, DC.

OECD (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September, http://www.oecd.org/e/droit/doneperso//ocdeprive/priv-en.htm.

OECD (1997). *Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet*, DSTI/ICCP/REG(97)6/FINAL, Paris.

OECD (1998a) *Electronic Commerce: Taxation Framework Conditions*, DAFE/CFA(98)50, www.oecd.org/daf/fa/e_com/ottawa.htm.

OECD (1998b). *Electronic Commerce: A Discussion Paper on Taxation Issues*, 17 September, http://www.oecd.org/daf/fa/e_com/discusse.pdf.

OECD (1998c). *International Workshop on Privacy Protection in a Global Networked Society*, DSTI/ICCP/REG(98)5/FINAL, Paris.

OECD (1998d). *Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of Privacy Guidelines on Global Networks*. DSTI/ICCP/REG(98)12/FINAL, Paris.

OECD (1999). *Inventory of Approaches to Authentication and Certification in a Global Networked Society*, October, http://www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)13-final.

OECD (2000). *Clarification on the Application of the Permanent Establishment Definition in E-commerce: Changes to the Commentary on the Model Tax Convention on Article 5*, December.

OECD (2001a). *Consumption Tax Aspects of Electronic Commerce*. A Report from Working Party No. 9 on Consumption Taxes to the Committee on Fiscal Affairs. Draft for public comment, February.

OECD (2001b). *Tax Treaty Characterisation Issues Arising from E-Commerce*. Report to Working Party No.1 of the OECD Committee on Fiscal Affairs, February.

Owens, J. (1997). "What chance for the virtual taxman?" in *OECD Observer*, No. 208, October/November 1997, pp.16-19.

Perez-Esteve, R. and Schuknecht, L. (1999). *A Quantitative Assessment of Electronic Commerce*, WTO Working Paper ERAD-99-01, September, Geneva.

Schlechter R. (1999). "Electronic Signatures: The European Community Approach", paper submitted to the UNCTAD Expert Meeting on Capacity Building in the Area of Electronic Commerce: Legal and Regulatory Dimensions, 14-16 July, Geneva.

Smedinghoff, T. and Hill Bro, R. (1999). "Moving with change: Electronic signature legislation as a vehicle for advancing e-commerce", *John Marshall Journal of Computer and Information Law,* vol. XVII, no. 3, Spring 1999, p. 723.

Storie, B. and C. Green (1999). *Will E-commerce succeed in Bermuda?* Discussion paper, Bermuda, William R. Storie & Co. Ltd.

Teltscher, S. (2000). *Tariffs, Taxes and Electronic Commerce: Revenue Implications for Developing Countries*, UNCTAD Study Series on "Policy Issues in International Trade and Commodities", No. 5, UNCTAD/ITCD/TAB/5, Geneva.

UNCITRAL (1996). *Model Law on Electronic Commerce with Guide to Enactment (1996), with additional article 5 bis*, http://www.uncitral.org/en-index.htm.

UNCITRAL (2001). *Draft UNCITRAL Model Law on Electronic Signatures and the Draft Guide to Enactment*, http://www.uncitral.org/en-index.htm.

UNCTAD (1996). *Incentives and Foreign Direct Investment*, UNCTAD/DTCI/28, Current Studies, Series A, No. 30, Geneva.

UNCTAD(1998). "Electronic commerce: Legal considerations", SDTE/BFB/1.

UNCTAD (1999). "Legal dimensions of electronic commerce", TD/B/COM.3/EM.8/2, para. 53.

University of Tennessee (2000). "E-commerce cuts into State tax revenues". Press Release, 27 January, University of Tennessee, Knoxville, Tennessee.

Vassilakakis, E. (1987). "Orientations méthodologiques dans les codifications récentes du droit international privé en Europe", Paris, LGDJ.

Vick et al. (1999). "Universities, defamation and the Internet", *Modern Law Review*, 1999, p. 58.

Weber, T. (2001). "Network solutions offer for sale of its database of domain-names", *Wall Street Journal*, 16 February.

Chapter 7

MANAGING PAYMENT AND CREDIT RISKS ONLINE: NEW CHALLENGES FOR FINANCIAL SERVICE PROVIDERS

A. Introduction

E-finance or e-payments or online payments are interchangeably used to describe the process of finance and payments mainly using the medium of the Internet. At the onset of e-commerce in 1994, the Internet population had at its disposal approximately 3 million host computers around the world. By the end of 2000 the number of hosts worldwide had risen to 93 million. Yet online retail sales still represented volumes equal to only 1 per cent of consumer spending in the United States. However, the rapid growth of online sales as well as online payments suggests that we are witnessing the beginning of possibly revolutionary changes in the world economy.

The main Internet-based payment methods are credit cards, regardless of the fact that even wealthy online consumers from most developed countries are not comfortable with communicating their credit card numbers over the Internet. Although there have been many candidate systems offered to fill the payments gap for business-to-consumer (B2C) e-commerce, not many have been adopted to any significant degree, and it may take some years before the industry converges on a standard in this area. It is really only since 1999 that the private sector in OECD countries and some emerging economies have started to get very interested in the area of business-to-business (B2B) e-commerce, and the jury is still out as to what will be the payment method of choice in this environment.

At the same time the main "bricks & mortar", i.e. traditional, banks, in facing up to the challenge of the newly emerging "clicks only", i.e. Internet banks, have developed considerable e-banking activities and have become "bricks and clicks" banks. Moreover, as a result of a crisis of trust vis-à-vis purely Net banks, consumers' preference has been for the "bricks and clicks " banks. According to one estimate, the banking industry in developed countries will grow at a rate of 3 per cent till 2003, while the Internet banking segment will grow at a rate of 25 per cent annually. Other projections suggest that, in the coming five years, half of the banking and 80 per cent of the brokerage in the developed countries will go online. The share of e-finance in developing countries might vary between 20 and 35 per cent for e-banking and between 15 and 40 per cent for e-brokerage, with higher projections in the event of a better policy, regulatory and institutional environment.

The banks of developed countries are expecting this exponential growth of online banking for both households and corporations and are actively preparing themselves. The e-commerce preparedness of various groups of developing and transition economies, especially within the financial sector, will also depend on their policy environment, their institutional set-up, and the determination of both private and public financial institutions to build up their e-finance capacities. Many of them take the Internet as a chance to catch up with the developed financial services providers, thus combating the international digital divide. However, well coordinated international co-operation will be needed to help the developing and transition economies to achieve this goal.

This chapter is mainly devoted to online payments and hence to the problems of developing secure payment techniques and technologies and risk management on the Internet. It also tries to identify the problems of current and future participation of developing country operators in online payments. For greater understanding of the modes of payment that can be used on the Internet, the chapter briefly highlights the conventional payment methods, including physical or electronic transfer of money, within existing electronic bank transfer systems, with or without use of the various credit, debit and other cards or checks, etc. The overview of conventional payment systems also makes it possible to identify the similarities and differences between offline and online payments. The purpose of this is to draw policymakers' and practi-

tioners' attention to issues involved in developing various online payments systems in the Internet, with particular emphasis on problems specific to the developing and transition economies.

B. Conventional and electronic payments prior to Internet

1. Cash

Cash currently represents 80 per cent of day-to-day transactions. Being versatile, its use does not require a financial intermediary, and it can be converted at a rate close to its announced value as long as it has a serious central bank, Government and developed economy behind it. The dollar, as the most usable and accepted cash in the world, sometimes even pushes out local currencies from circulation — the well known phenomenon of dollarization seen in many third world economies. In the latter, cash is used in all domains, including inter-enterprise payments, predominantly within the framework of the informal economy. Lack of trust and propensity to hide incomes from tax authorities could keep cash for quite some time as an important traditional payment method servicing both traditional and Internet-based commerce in those countries. In more transparent developed economies, cash continues to be an important payment instrument in business-to-consumer and person-to-person low-value transactions.

Cash is not without its problems, however. The costs incurred by central banks to produce and maintain the national stock of notes and coin greatly exceed the seigniorage revenues for the right of issuing them. It is open to attack from counterfeiters. It can be stolen. Its anonymity makes it attractive to citizens who wish to keep their transactions private, it is equally attractive to organized crime, and its use in large value transactions is often associated with tax evasion or money laundering.

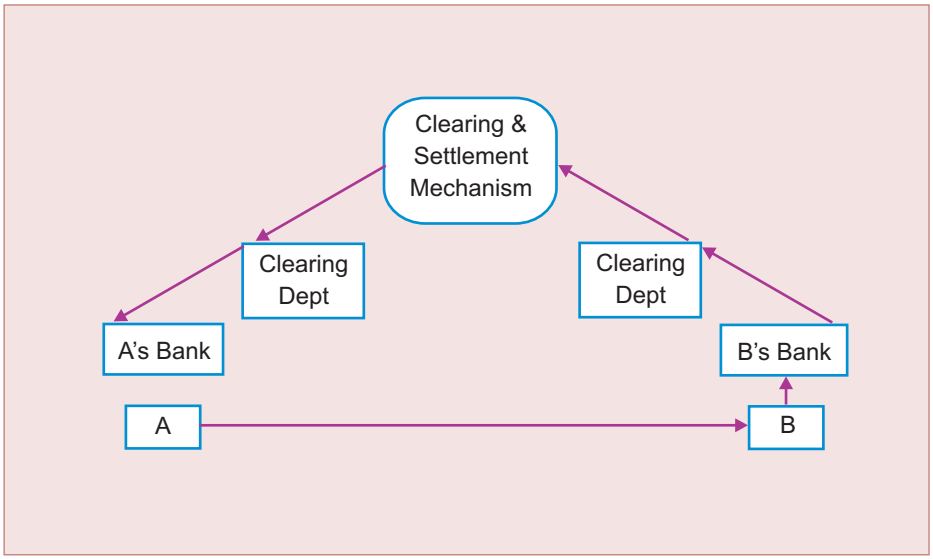
2. Money orders, checks, drafts, notes, bills of exchange

Higher value transactions need more security than cash can provide. Hence the importance of modern financial intermediaries transferring value mainly for their clients through proprietary electronic means of communications or so called Intranets. These modes of payment involve money orders, i.e. bank transfers on the orders of clients, or documents issued in paper and electronic forms, mainly by banks, such as checks, drafts, bills of exchange, promissory notes, documentary collections and credits. Drafts and notes might be issued for immediate payment (sight draft) or represent a promise to pay at some future date and hence giving a financing opportunity to the debtor (term draft). Drafts, including bills of exchange (instructions to pay) and promissory notes (promises to pay), are negotiable, i.e. they are transferable instruments where the beneficiary (normally a company) might through the secondary market (acceptance market) discount the instrument and pass the right to collect to another beneficiary (normally a financial intermediary). The latter might then opt to resell the portions of an underwritten risk to other financial intermediaries (forfaiting market). Afterwards the debt instrument might have its own autonomous life, i.e. change hands in the secondary market until the payee honours the debt.

Drafts and notes are instructions to the payer's bank or a promise to transfer funds to the payee. They are fundamentally dependent on the presence of financial intermediaries, usually banks, as well as clearing and settlement mechanisms created by the latter. In its most simple form involving two banks, a check clearing process is as portrayed in chart 9. The bill of exchange is a similar instrument and is widely used to finance trade in so called documentary collection.

The check and other negotiable money instruments can be used as payment vehicles to transfer values of any amount. They involve at least one financial intermediary and might be associated with a considerable amount of paper processing, i.e. elapsed time and transaction costs. This effectively makes them impractical for very small transactions. The check, as a promise to pay, depends on quite a degree of trust being established beforehand between the two parties. The seller in this case might demand evidence of an asset, collateral or surety from the buyer and will try to include the right to realize the collateral in a contract. It is important also to mention the risk associated with "not sufficient funds" (NSF) or a "returned-item" or bounced check. Even though the incidence of checks being returned is very small, the fact that it can happen at all makes the risks associated with checks rather high for many transactions, particularly where goods are delivered immediately and to high risk destinations.

Chart 9
Check clearing process



Another way to pay is to use a credit transfer or giro payment. Whereas a check represents a "pull" payment with the paper check pulling funds from the source account through the clearing network into the destination account, the giro does the reverse. Funds are "pushed" from the source account to the destination account. The credit transfer cannot be initiated unless the funds are available and this greatly reduces risks associated with the payment. Post offices are usually the key players in giro payments. They have their own accounts system and in this case they play a role of financial intermediary between the payer and the payee. While checks are very popular in the United States, the giro payments are particularly characteristic for Europe. Among the reasons for giro payments is consumers' desire to keep control over their bank accounts and plan their payments schedule in light of their own preferences. However, by "disintermediating" banks as direct payers, retail consumers tend to be late in their payments.

Where the bank details of the payee are known in advance, it is possible to make electronic transfers between bank accounts using the so-called automated clearing house (ACH) networks. In fact in the United States and Canada funds can be "pushed" as well as "pulled" by ACH debits and credits. These organizations grew out of the systems that were developed to process checks clearing and are now used by consumers for recurrent payments to regular service providers (utilities, telephone, residential charges, etc) in the form of direct debits. They are also used extensively by businesses to pay their regular suppliers and by Governments to issue all kinds of payments to individuals and corporations. In the United States, the system is operated by the National Electronic Payments Association (NACHA), and most countries in the developed world have a similar system. Indeed, it is quite common to have multiple systems of this sort operating in a single country – some operated by the central bank, and others by consortia of leading banks.

In 1999, the average value of a payment made through the ACH system was approximately $1,500 and settlement was made overnight. Where the value of the transaction is significantly larger, a different class of payment method is typically used which is referred to as a 'wire transfer'. One example of this is the FEDWIRE system operated by the Federal Reserve in the United States. This offers the facility to make immediate payments, with settlements performed by transferring funds between accounts maintained by the member banks with the Federal Reserve. In 1999, the average value of each transaction in the FEDWIRE system was $4.3 million. It is thus used principally for major business-to-business and also business-to-Government transfers.

When such payments are to be made internationally, the messages relating to wire transfers are typically carried on the networks of the Society for Worldwide Interbank Financial Telecommunications (S.W.I.F.T.), a huge bank cooperative including 7,000 financial institutions from 190 countries. The magnitude of payment and transfer traffic in the S.W.I.F.T.

proprietary electronic system or Intranet is impressive, exceeding $5 trillion daily, with the settlement and risk management functions being handled by correspondent bank relationships. While bank payments represent more than two-thirds of S.W.I.F.T operations, the system is also active in securities settlements. S.W.I.F.T. has also big e-commerce-related plans and programmes, including Bolero, TrustAct and others. Last year it announced plans to move to more open Internet Protocol (IP) messaging and network services.[1]

3. Debit and credit cards[2]

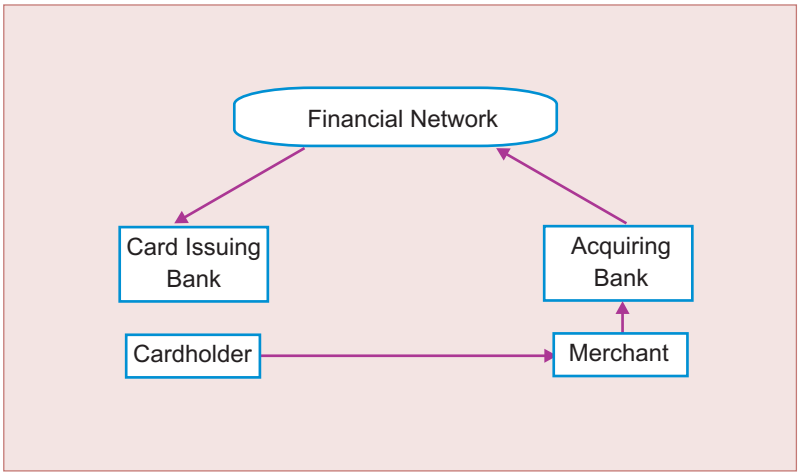
One can find the roots of credit cards in the establishment of 'shoppers' plates' aimed at simplifying payments for affluent customers of retail establishments. The possibility of transmitting communications electronically gave a huge boost to the card industry in recent decades.[3] As a result, an enormously popular, globally acceptable payment instrument has emerged embodied a plastic card with a magnetic strip making it possible, through various electronic devices, to identify the card number and receive authorization from the bank to make the payment. For the system to operate, the potential cardholder must approach a 'card issuing' bank or company and get a physical card that will allow transactions to be made. In some cases it involves opening a related bank account. Without appropriate restrictions, the possession of a card confers unlimited spending power on its owner. In the majority of cases, though, the card-issuing bank will assign a 'credit-limit' to the cardholder based on an examination of his creditworthiness. The cardholder can either retrieve cash using automatic telling machines (ATM) at banks or card associations or purchase goods and services from merchants electronically linked either with the authorizing card association or the bank. While a debit card involves direct pulling of money from an account and is limited by the availability of money in the account, a credit card gives the possibility of a credit limit and hence short-term financing for a cardholder. Hence credit card fees are much higher than those for debit cards. To some extent, a debit card is similar to an electronic version of a check. Typically, the debit cardholder needs to enter a pin (his individual code) at the point of sale, verifying at least that the card is not stolen and whether sufficient funds are available. In the case of credit cards, merchants demand a written signature from a cardholder, which they normally compare with that on the card. So far, the more popular card-related payment mode is the credit card.

In most developed countries, the process of acquiring a card is quite routine and indeed customers are often bombarded by advertising from different companies offering them credit cards. In the majority of developing countries though, the card infrastructure is underdeveloped, credit cards are sometimes hard to get, and in some countries tight restrictions are placed on their usage. Those restrictions derive from exchange controls in countries with scarce foreign exchange reserves and suffering from various forms of capital flight.

At the other side of each credit card transaction is a "merchant". Once again, achieving "credit card merchant" status involves opening an account with a bank that will 'acquire' transactions on behalf of the business. Once the account is set up, the merchant has the ability to charge arbitrary amounts to any credit card that has been issued anywhere in the world. Clearly, this represents a major opportunity for fraud in the short term, and acquiring banks will often subject a business to strict checks before permitting them to operate as a merchant, particularly if they intend to carry out business across the Internet. In the United States, these checks are not very stringent, but they are much more so in most European countries, whilst in some developing countries, companies may have extreme difficulty in gaining credit-card merchant status. In developing countries or regions where telecommunications facilities are not available or where dial-up telephone connections are very expensive, the authorization step may just be a simple check of the credit card number against a periodically updated blacklist. Often merchants operate under quite complex policies to balance the risk of fraud against the cost of verifying the transaction. This may involve going through authorizations only where a transaction value exceeds a 'floor-limit' or carrying out an online authorization randomly for one in every 10 transactions. The costs involved in processing credit card transactions are considerable. Typically, these are recovered by a per-transaction levy on the merchant. The charges depend on the acquiring bank and also on the level of risk associated with the business.

Chart 10 shows the information flow when a credit card transaction is made. The cardholder presents the card details to the merchant. The merchant can authorize the transaction prior to actually making it.

Chart 10
Information flow in a credit card transaction



This is done through a connection either directly to the merchant's acquiring bank or to a technology provider acting on its behalf. The acquiring bank can authorize this transaction using a financial network which has access to the data of card-issuing banks worldwide. The transaction can have two steps – an authorization step (this is used frequently by hotels at the beginning of a guest's visit) and a later 'capture' step where the previously authorized transaction is completed. Alternatively an authorization-and-capture step can do everything in a single action.

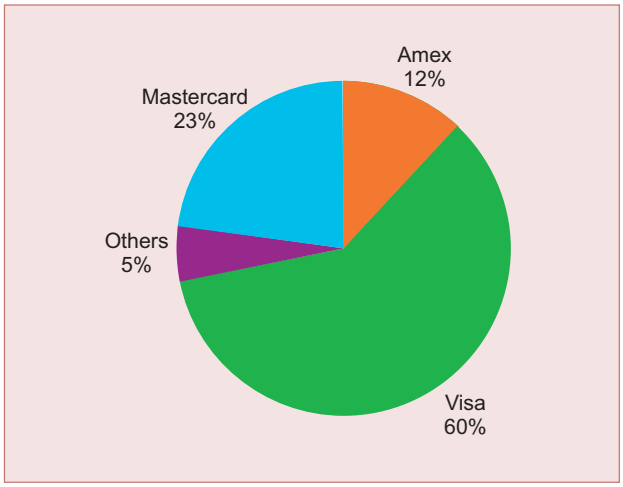
One credit-card usage scenario that is interesting because it serves as the background for Internet credit card transactions is the so-called Mail Order Telephone Order (MOTO) transaction. Under this scenario, merchants are allowed to accept orders by post or over the telephone, with the customer simply quoting the credit card details verbally. Under this scenario — also called "Card-Not-Present" — the merchant is unable to tell if the customer has the card in his or her possession, nor can the signature be verified. Some simple safeguards are put in place regarding the address to which the goods can be dispatched and, in the event of the customer later disavowing the transaction, the merchant must bear the cost.

The costs involved in processing credit card transactions are considerable. Typically, a merchant that has been trading profitably for years will be able to negotiate a better rate than a start-up company. Any company that trades on the Internet is regarded as being 'risky' and is typically subject to higher charges. Generally there is a fixed fee of around $0.10–0.50 and a percentage of the transaction of around 1–5 per cent. This effectively means that credit card transactions are not worthwhile for transactions less than $10.

The great strength of credit cards is their global acceptability. Since the processing of transactions across the financial networks takes care of the currency conversion, merchants will receive funds in their local currency while the cardholder is levied in his own currency. Naturally the country of a cardholder should accept currency convertibility at least on current account. The global recognition of the two major brands (Visa and MasterCard) and also others such as American Express, Diners Club, Europay and Discover reassures merchants that the payment will be honoured. On the downside, rogue cardholders and rogue merchants quite easily perpetrate fraud, particularly where the authorization process does not go online to verify each transaction with the issuing bank.

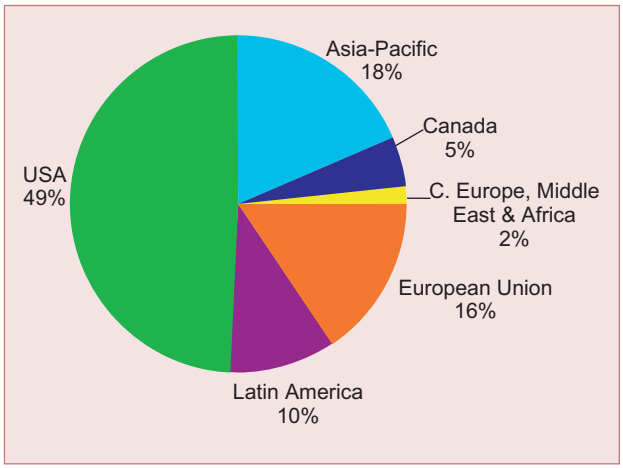
The two leading brand names are Visa and MasterCard, which account for 75 per cent of the general–purpose credit and charge cards market. Like S.W.I.F.T. they are associations involving mainly banks. At the same time they have very strict procedures for accepting a bank as a Visa or Mastercard issuing member bank. In 1970, Visa was confined to the United States, with 243 members, and was covering payments worth $3 billion with 30 million cards. In 2000, it was accepted by 19 million brick and mortar locations in virtually all countries and territories and was servicing payments traffic of around $1.6 trillion with more than 1 billion cards, of which the overwhelming majority were credit cards[4]. One of the principal reasons for the success of these two 'card associations' is that they are owned and operated by banks from

Chart 11
Major international credit cards companies market shares in 2000



Source: www.visa.com

Chart 12
Global distribution of VISA cards in 2000



Source: www.visa.com

all over the world. It is these local banks that manage the relationship with the cardholders, while the card associations provide the global branding and also the common infrastructure that registers the payments traffic and links the banks that operate the system with the merchants and consumers. Other card issuers with much smaller shares of the market include American Express, Diners Club (owned respectively by American Express Bank and Citibank), Discover and others. In mid-2000 American Express initiated a United States antitrust lawsuit, considering Visa and Mastercard to be monopolies. The latter were blamed for collusive practices preventing their bank members from issuing rival cards. It is too early to draw conclusions on this matter, as the legal ruling has yet to be made. The propensity of consumers as well as merchants to go for the most widely accepted cards could explain high entry barriers and tough conditions for smaller players. So on the one hand monopoly charges and collusive practices should be prevented, while on the other users might still want to go for universally accepted and non-fragmented payments systems.[5]

4. Geographical variations of conventional non-cash payment systems

After the above presentation of conventional payments systems other than cash, it would seem useful to indicate geographical variations in their use.

As the table 24 shows the degree of adoption of different payment systems differs markedly between countries. In the United States, for example, checks represent 70% of all non-cash payments, payment cards come next with 25 per cent while the use of credit and debit transfers is quite infrequent. 84 per cent of all checks in the United States are issued by enterprises. This is almost the reverse in Germany, where payment card usage is extremely low compared with other developed countries and giro credit transfers are used for more than half of non-cash transactions.

When comparing developed countries, many of the differences can be explained by the historic evolution of payment systems over time. For example, the popularity of giros in many European countries can be explained by the involvement of post offices in providing payment services over many years. In considering the developing countries, however, the overall financial infrastructure tends to be poor. Since checks are perhaps the most basic payment instrument that a bank can offer, these tend to be available everywhere and attract widespread usage. Moreover, for example in Latin America, a check might be endorsed many times thus becoming a pseudo currency note. In such countries payment cards are used only in particular industries or they are not issued at all. Thus out of the 1 billion Visa cards that have been issued throughout the world, Central Europe, the Middle East and Africa account for just 2 per cent. And finally unusual local factors often lead to a payments situation that is anomalous compared with other, similar countries. For example, Turkey has embraced the use of payment cards almost to the exclusion of other forms of payment.

Table 24
Geographical variations of consumer preferences in non-cash payment methods by country in 1998
(Percentage)

Country	Use of checks	Use of credit tTransfers (Giros)	Payment cards	Direct debits
United States	70.0	3.7	24.3	2.0
Netherlands	1.9	45.0	24.5	28.5
United Kingdom	28.0	19.3	33.1	19.4
Germany	4.8	50.6	5.1	39.5
Turkey (1997 figures)	6.9	2.6	83.9	-
Namibia (1996 figures)	75.0	14.0	Not provided by local banks	9.0
Angola (1996 figures)	75.0	25.0	Not provided by local banks	-

Source: Bank for International Settlements.

5. Payments protection by financial intermediaries: secured notes, documentary credit, credit insurance, factoring, and others

Where trust is a problem, a planned transaction or project may be at risk, and delays or even defaults may occur in dispatching goods and services as well as in reciprocal flows of payments. In such a case, the parties may have to resort to various systems of third party protection by banks, credit insurers, factors and others. The financial services sector has developed an array of risk management instruments including bank, insurance, derivative and combined products. Some typical examples are described below.

A basic example of bank-related protection could be check guarantee cards, which indemnify the payer against risks as long as the transaction size is small and some fairly rudimentary security checks are made at the time of the transfer. For larger transactions, a customer's bank will often sign the check itself, converting a simple check into a cashier's check (drawn on itself) or teller's check (drawn on another bank). Those instruments are also called bank drafts.

In more risky situations, sellers accept only the so-called letter of credit (L/C), which is an obligation of the buyer's bank to pay to the seller's bank on condition of scrupulous adherence by the seller and its bank to the related documentary requirements (bill of lading, cargo insurance, other certificates, etc). That is why the L/C is also called documentary credit. The L/C is stricter in its requirements than documentary collection based on instruments like bills of exchange. In a similar arrangement called factoring, the factor (usually a specialized department of a bank) discounts sellers' receivables, mainly without recourse to the seller. Meanwhile the correspondent and related to the buyer factor handles the payment and related risks. This technique is reminiscent of a mix of a L/C with the acceptance or discounting business.

The money order or so-called open account payments can be protected by a technique called credit insurance – a good instrument to encourage and diversify exports and bear the risk of going for new markets. After receiving goods, the buyer should normally give a money order to his bank to pay against the seller's invoice. The main credit insurance products are short-term policies protecting the supplier from default on the part of the buyer in paying his trade debt due to commercial (related to the buyer himself) and political (related to the buyer's country) risks. Credit insurance thus creates sufficient security for sellers to dispatch their goods and services to mainly foreign buyers on open account, *inter alia* providing the latter with short-term trade credits.

Various arrangements have been developed to pre-finance suppliers and structure performance related risk, including pre-shipment financing, structured financing, warehouse receipts financing, etc. In the majority of the above cases, the promise to pay comes from or is guaranteed by a much more trusted third party, i.e. a bank or a credit insurer and hence greater risks can be taken by the payee to ensure that transactions and related payments are completed successfully. It is important to stress here that the same third parties have also developed instruments to protect risks related to non-performance of the seller, thus making sure that the good payer will not suffer from failure to deliver according to the terms of the sales

contract or that of a project. Bonding is the most accepted means of protecting the buyer.

Recently the world financial community witnessed a phenomenal growth of financial instruments called derivatives. The global daily turnover of counter and exchange-traded derivatives reached $2.7 trillion in 1998.[6] On an annualized basis this is 20 times more than the world GDP. According to the Bank of International Settlements (BIS) these instruments comprise mainly financial contracts "the value of which depends on the value of one or more underlying reference assets, rates or indices" and are in the form of so-called "forward contracts, options or combinations thereof".[7] Being basically bets designed to protect the contracting party or make a gain for him from fluctuations in future prices they can exist if there is enough appetite to ensure the opposite bet is made and thus balance supply and demand in the derivatives markets. So while other instruments protect parties to financial contracts from non-payment or non-performance risks, derivatives were designed to manage the risks related to price fluctuations, including the exchange rate risk in cross-border operations. In other words, decisions related to the prices, choice of the currency and the timing of its real conversion are very important.

C. Making payments online

The term online payment is now part and parcel of e-commerce terminology. However the scope of the term varies depending on whether the reference is made only to the Internet or whether it also includes electronic payments made through the proprietary electronic networks or the so called Intranets described above.

Some experts define online payments in a technology neutral manner and would include in it all payments where the transaction information is transmitted electronically, the payer and the payee are directly involved in the transaction, and the necessary information to authorize the payment is part of the transaction information exchange between the payer and the payee. In this case, the technical channels, as well as the format and the payment instrument are not essential to characterize online payments. Thus in the United States and some other countries, electronic transfer of money described above is considered online. In other countries and primarily in the developing world, the term online payments relates only to the electronic transfer of funds over public or private networks based on the Internet and related technologies (for more details on e-commerce definitions, see chapter 1).

The main purpose of this chapter is to help developing and transition economies to identify Internet based online payment mechanisms and networks. So, without going into the debate on the definition of online payments, this report, limits the scope of the analysis in this section to the payments involving the Internet.

The survey of conventional payments presented in the previous section is based on the sequence of their historical evolution, moving from cash to negotiable money orders and then cards, including many proprietary electronic payments networks such as S.W.I.F.T, credit card associations' networks and others. The short history of the Internet has rather shown a reverse movement: online payments started with credit card related consumer purchases online and then went into a variety of electronic checks and other documents with the use of electronic signature and combined instruments such as smart cards. At the same time the cash function migrated to the stored value or prepaid cards (electronic purses) and software products (digital cash)[8]. In smart cards the stored value is still one of its main functions, as the multipurpose chip still needs some time to become popular. One might presume that, as in the case of conventional payments, different kinds of online payments will evolve, with considerable geographical variations in their usage.

According to numerous surveys, consumers so far prefer solid financial institutions with combined online and offline skills, and the leading banks are taking the challenge of online payments very seriously. For the moment the industry lacks standard online payments technologies and is still in the stage of choosing between competing models and solutions. Many solutions did not live up to expectations, while others needed development and marketing efforts. Thus according to a GartnerGroup survey, electronic wallets represent less than 1 per cent of online payments. Equally, smart cards were announced as the future device for online payments due to the ability of their chips to combine high security, storage of much more information, specific risk management tasks and other characteristics. However for the moment they are used more as prepaid card devices than as multifunctional applications.[9]

Thus this section will first look into business to consumer (B2C) online payments and will then analyse business to business (B2B) online payments mechanisms. The presentation of those methods under either the B2C or the B2B heading does not preclude their applicability for any purpose but merely reflects their main area of use at present.

1. Business to consumer (B2C) online payments

B2C e-commerce, which started from just a trickle in 1995, grew dramatically to somewhere between $23 billion and $109 billion in 2000[10]. Some of the sectors that proved popular include books (e.g. amazon.com), apparel (Land's End, Gap, Victoria's secret), computer products (Dell, Gateway) and travel (Expedia, Priceline).

Starting from credit card payments through Internet, online payments are evolving into a system where payers might use smart cards combining the functions of all cards and electronic cash or electronic checks, with encrypted electronic signatures or other modes of secure identification of the payer and payee. These systems are used both in B2C and B2B payments. However credit cards were the first online payment instruments and the security in Internet was challenged when credit card holders giving credit card numbers on the Internet were subjected to serious risks from hackers and fraudsters. In fact the analysis of various modes of online payments in this section contains detailed descriptions of different systems defending the security of the payer.

(a) Online payments by credit and debit cards

For various reasons, the most natural way for a consumer to make a purchase over the Internet in the absence of other widely accepted alternatives is to use a credit card. A precedent had already been set over a number of years by catalogue shoppers. Business rules, including the MOTO rules referred to earlier, had been developed to handle transactions where card details were given to the merchant either on a printed order form or over the telephone and there was no possibility to identify the cardholder by at least asking him to sign in the presence of the merchant. For the majority of international shoppers, the currency convertibility problem was solved, and there were already large numbers of people worldwide who could make and accept payments without the need for any sign-up procedure.

The earliest web purchases were made either by insecurely transferring the credit card details in a web dialogue or by resorting to a separate e-mail exchange to complete the payment. The credit card companies were not happy about this method of conveying the details, and the advice they issued to consumers and merchants was not to use credit cards on the Internet until new technologies were developed to allow it to be done securely. However the market largely ignored that advice.

(i) Secure Socket Layer (SSL)

A stop-gap solution arrived in1995, when Netscape incorporated support in its Internet browser software for a technology standard called the Secure Socket Layer (SSL). SSL is still the dominant mode of online payments, especially by credit cards.

A merchant wishing to use SSL to protect credit card transactions must apply to a recognized X.509 Certification Authority (described later) to be issued with a certificate. All Internet browser software comes preconfigured to trust the 20 or so most common certification authorities operating worldwide.[11] A user browsing the merchant's site will interact normally until it comes to the point where the credit card details are to be transferred across the link. At this point, the user's browser will be directed to a web page that starts with HTTPS rather than the usual HTTP. This is a signal to the browser to start a special security dialogue with the browser in which two things happen. First, the merchant proves that he represents the business to which the X.509 certificate is issued, and secondly he agrees on a session encryption key that is used to protect the credit card details and any other financially sensitive information from being intercepted by attackers as they travel across the Internet.

Thus the cardholder is afforded some protection in terms of confirmation that the merchant to whom he is giving his card details exists as a bona fide business, or at least did at the time the certificate was issued. Both the cardholder and the merchant are also protected from eavesdroppers capturing the credit card details from an insecure Internet link. For the merchant there is no protection in terms of ensuring that the card is not being used by someone other than the cardholder, and if the latter denies making the

Chart 13
The Secure Socket Layer protecting a credit card payment

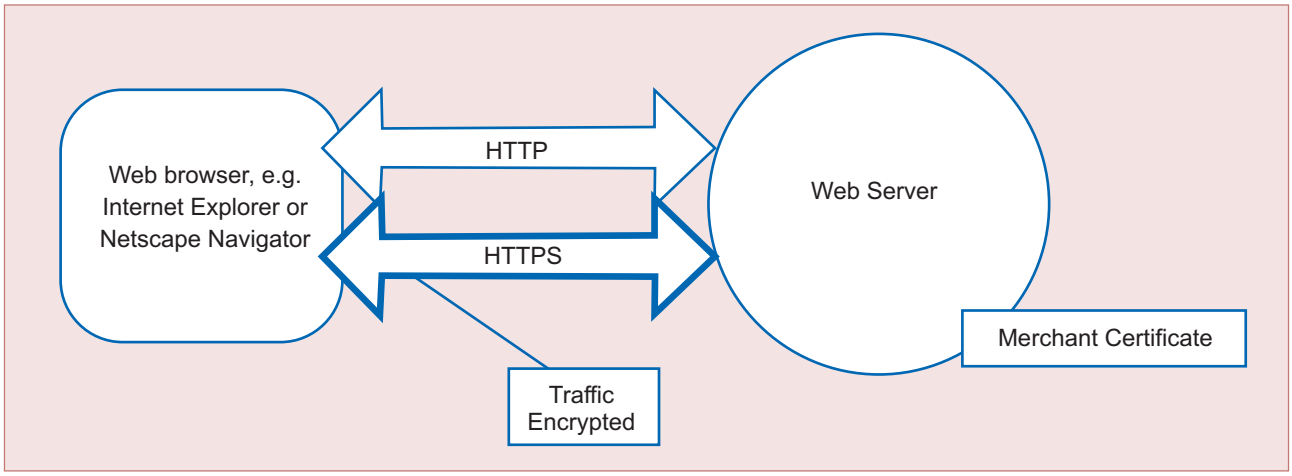
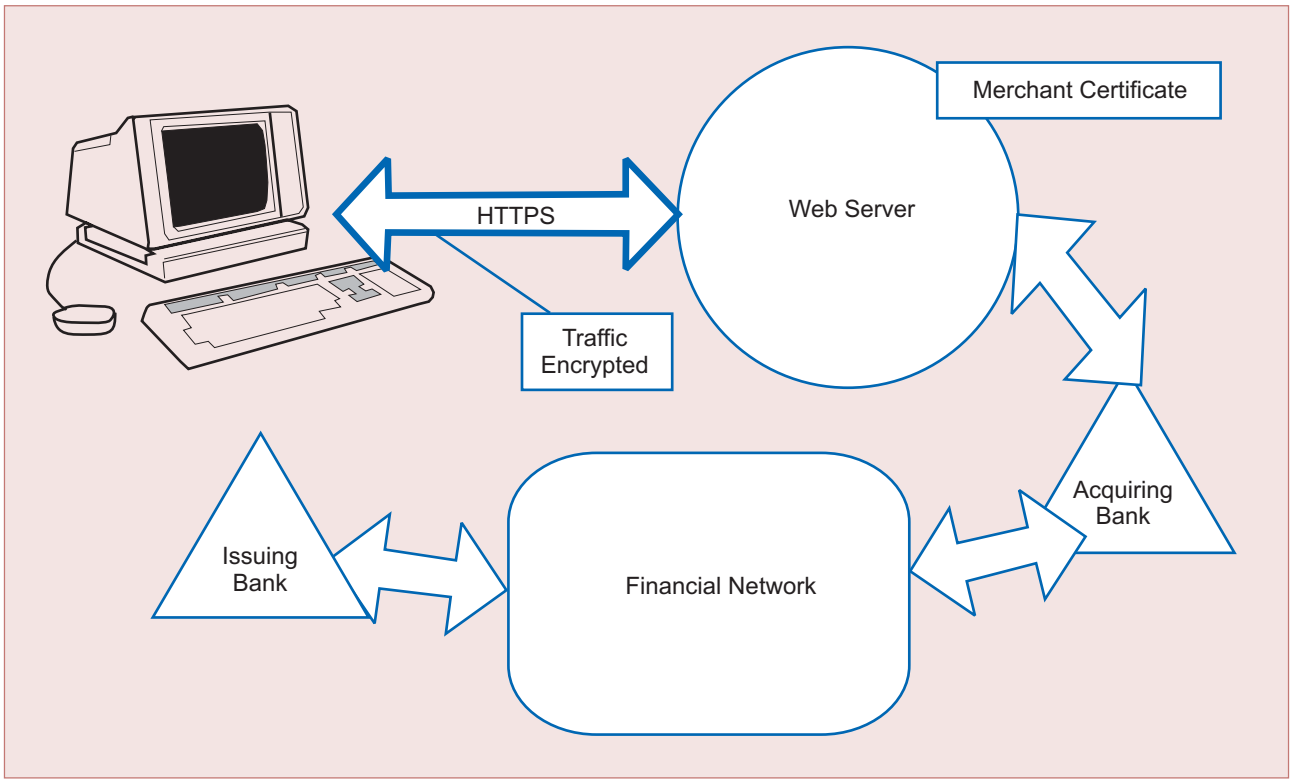


Chart 14
Online authorization of a credit card transaction



transaction, there is way of proving otherwise. The cardholder has no protection against a merchant who may retain the card details and subsequently charge multiple transactions against the account. If the merchant site stores the card details online, they make themselves vulnerable to attackers breaking into their site to gain access to those details[12].

In order to streamline the process of making credit card transactions and also to allow each individual transaction to be authorized, merchants generally equip themselves with an online connection to their acquiring bank or to an entity operating on its behalf. This process has been taken further by companies such as iTransact, which operate links to the financial network on behalf of many hundreds of online merchants. Using their services, the B2C merchant can interact with iTransact's web site during the purchase to get authorization and complete the transaction in real time. Merchants are required to hold accounts in developed country banks, and transactions are denominated in US dollars or other leading hard currencies. Every other component of the system, including the merchant web site, can be located elsewhere.

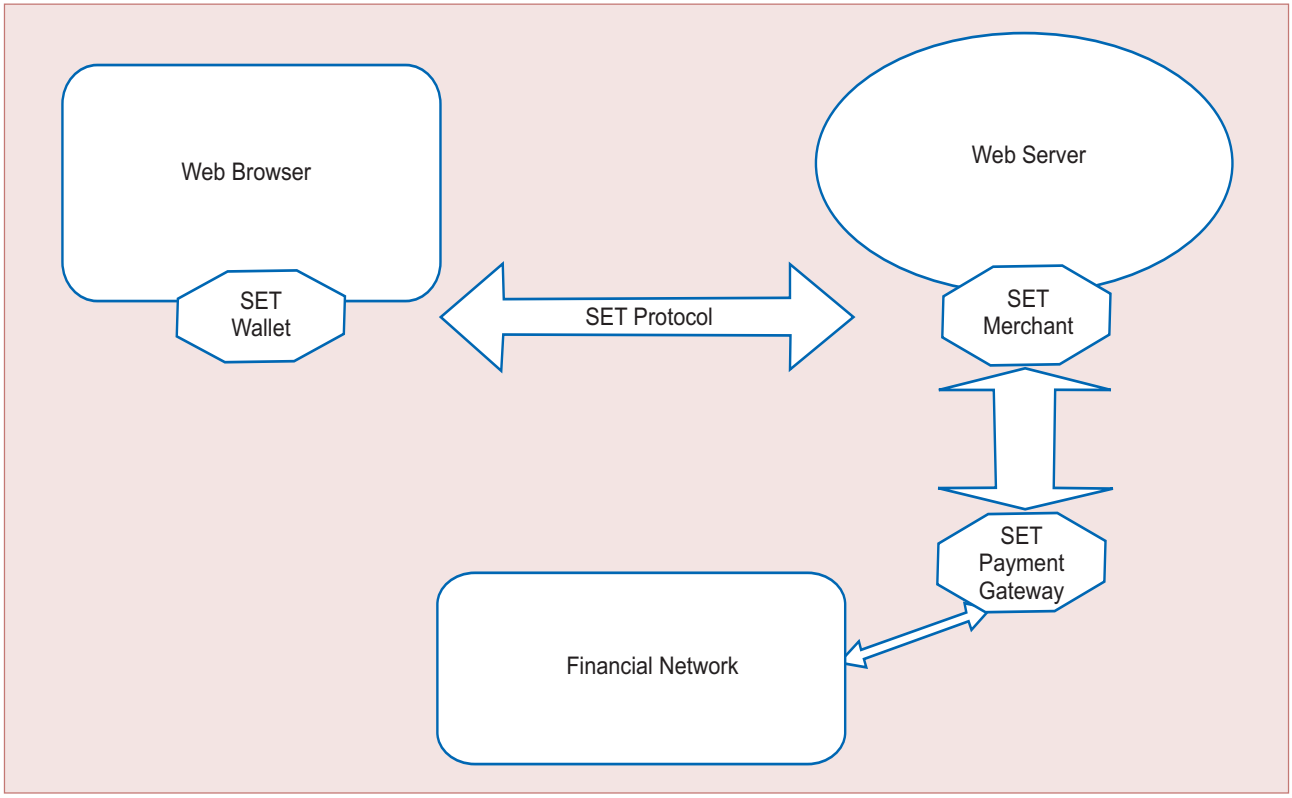
(ii) Secure Electronic Transactions (SET)

Although the use of SSL, with or without online authorization, is for the moment the most common means of making credit card transactions, a more advanced technology is available in the form of a security standard called Secure Electronic Transactions (SET). This was developed principally by the two major credit card companies, Visa and Mastercard, in 1996, with the support of many major technology providers, including IBM, and other card brands including American Express. It is a comprehensive solution to all the practical risks that are encountered in any credit card transaction. SET was introduced primarily to prevent rogue merchants from misusing credit card information. It hides the credit card number from the merchant but leaves him with the important ability to verify that the card is good and that the authorization is good.

Special wallet software is used by the cardholder that is partially or totally integrated into the web browser's software. The wallet software is loaded with the card details and also with a certificate that is issued to the cardholder by the issuing bank. When a credit card transaction is to be made, the wallet software composes an encrypted payment request which is sent via a SET module running on the merchant's web site and from there to an SET payment gateway run either by each acquiring bank or by the credit card company itself. The SET standard underwent a one year public review period and is thought to be highly secure and efficient at guarding against all anticipated risks due to stolen cards, rogue merchants and rogue cardholders.

The main problem with SET lies in its complexity. Three independent pieces of software need to be in place and working together well before a single transaction can be carried out, and certificates must be issued to each of the three parties (buyer, seller, bank) to allow them to securely identify each other. Banks began to pilot SET at the beginning of 1997, but this was done mostly on a regional basis (which does not fit well with the global way in which the Internet operates) and these pilots achieved limited success in terms of persuading large populations of users and merchants to change over to the new system. As of early 2001, SET has still achieved little market penetration and its proponents are beginning to experiment with so-called 'light' versions of the standard that involve less complexity.

Chart 15
The Secure Electronic Transactions Protocol



(iii) Controlled Payment Numbers (CPN) and other systems of securing card-based payments

There are also several transaction processing systems which add security and do not require merchants to keep separate transaction terminals or processing software. For example, one system that offers extra security over SSL is a technology referred to as a Controlled Payment Number (CPN) or One-Time Credit card Number. In a normal web based credit card transaction secured by SSL, the user supplies credit card details to the merchant, allowing the latter to make a charge against his account. The problem is that if an attacker gains access to this information, he can use it to make bogus transactions. The cardholder also has no protection against rogue merchants who make multiple transactions or charge amounts other than those agreed.

Users of CPN can gain some protection against this kind of fraud. The system works by cardholders installing an application on their local workstation, which they invoke whenever they do an online purchase. This software asks them for a maximum value and a time period for payment and then contacts their bank online. The bank generates a number that looks like a normal credit card number, but in fact is not associated with a real card. This number is given to the merchant in place of the normal number. The merchant is unaware that there is anything unusual about the number, and when authorization is sought, it will be forthcoming provided that the amount of the transaction is less than the maximum specified by the user. Any subsequent transactions using this number will be refused.

This system is compatible with existing banking applications and in particular the payments infrastructure of merchants' servers. Apparently it involves low cost and easily adaptable software. In a nutshell it is centered on cardholders propensity to control the transaction and protect their real card numbers. Here the cardholder never transmits his credit card number. Instead he or she might give a single purchase number for one transaction or for a specific series of payments. The payer himself sets the value and time limit for the purchase and the identity of the payee. CPN permits the bank in relationship with its customer to act as a portal for the two-way information flow. Another claimed CPN strength is its versatility. It can be used not only with cards but also with personal bank accounts. It is allegedly also compatible with emerging biometric and voice activated identification systems.[13]

The downside is that it requires cardholders to install special software, to register with their bank to use the CPNs and then to have online dialogues with their bank every time a purchase is made. This technology was first brought to the market by Orbiscom in early 2000 and their system has been deployed by Discover Card and MBNA (a major international credit card issuer) among others. Somewhat similar systems have also been announced by American Express for their United States cardholders and by Cyota Inc in Israel.[14]

(b) Electronic money or cash-like systems

According to a recent publication of the Committee on Payment and Settlement Systems of the Central Banks, members of the BIS, electronic money refers to "prepaid products in which a record of funds or value available to the consumer is stored on a device in consumer possession".[15] Prepaid cards, sometimes called electronic purses, as well as prepaid software products, also called digital cash, are examples of electronic money, which uses the Internet as a medium for a transfer.

Since cash is used for approximately 80 per cent of retail consumer transactions, one would expect that there would be great demand for this service in electronic commerce transactions. However the market reaction to some of the earlier cash-based systems was less enthusiastic than expected.

The example of eCash from Digicash BV is instructive in that respect. This company launched and deployed a software-based system that allegedly allowed individuals to make arbitrary fully anonymous transfers of value between each other in a range of currencies. E-cash was rolled out in many countries around the world in conjunction with local partners (e.g. in the United States with Wells Fargo bank, in Germany with Deutsche Bank, etc), but in most cases it was not a big success. Afterwards the company refocused on a portfolio of payment solutions including a person-to-person (P2P) transfer method. Finally, due to many difficulties it had to file for bankruptcy.

Many other systems, including e-gold, Papal, Webmetering and others, are still being tested. Although many of them claim to be cash-like, most

of them fall into the category of account-based systems, where the payment is simply a transfer between identified accounts on the provider's system. Most of them still lack convenience and hence general acceptance.[16]

The future of digital cash might lie in combined solutions where a prepaid or charged device is a part of a smart card which includes also the roles of credit and debit cards. The following paragraph explore smart cards further.

(c) Smart cards: combining e-cash, e-cards and more

In conventional bank-mediated transactions, the trend for retail point-of-sale systems is away from paper-based instruments such as cash and checks and towards electronic payment effected with a card. Most of the cards in use today are based on magnetic strip technology with some rudimentary account identifying information recorded (insecurely) on a magnetic strip on the back of the card. The banking industry is in the process of transitioning to the next generation of payment cards based on the smart card or chip card technology. The main catalyzers of this process include the card associations such as Visa, Mastercard and Europay who are actively pushing their bank members towards the adoption of smart cards. At the same time equipping the merchant with a combined magnetic strip and smart card reader device incurs additional expenses. There is also the risk factor that is peculiar to each country or region. The nature of the customer/merchant base or the availability of an inexpensive network or telecom services to enable online authorization strongly influence the credit card associations' plans to introduce new non-magnetic strip i.e. smart card technology.

The smart card is a plastic card with a chip securely embedded in the card. When inserted into a card reader, this chip powers up and is able to have electronic dialogues with the card reader device. One advantage of the chip is that it can carry 100 times more information than the traditional card in a form that cannot be copied. The chip on the card encrypts data before sending it to the card reader, making it very difficult to break the security, while secret quantities like cryptographic keys never leave the card. Another advantage which partially derives from the first is the possibility to have various functions in one chip, including the functions of credit, debit and prepaid cards, as well as the functions of secure Internet shopping, mass transit applications, identification services, merchant loyalty programmes etc. Thus, by having just one smart card, the client can run multiple operations with his bank and third parties. On the down side, the cards are more expensive to produce and are vulnerable to attacks from card reader hardware that has been subverted.

The electronic purse is related to electronic money or prepaid card related applications and could be a part of chip-card technology. Here value is loaded into the smart card for later spending. There are two main efforts ongoing in this area, the first by Mondex International and the second by a consortium led by Visa called the Common Electronic Purse Specification (CEPS). The difference between the Mondex system and the Visa/CEPS initiative is that Mondex does not require overnight transaction bank clearing. The value is immediate and saves the banks from processing a massive volume of petty cash transfer transactions. Of the two, the Mondex effort is more mature and has been in common use since 1992. The Mondex system offers a means of transferring value from one card to another. A person can transfer value from his card to that of his friend by simply inserting both cards into a hand-held value-transfer terminal. Similarly bricks-and-mortar merchants can use a point-of-sale terminal containing a merchant card into which the buyer inserts the Mondex card to allow the transfer to take place. The Mondex card is currently licensed in over 80 countries around the world, including several in Sub-Saharan Africa. Pilot experiments have been conducted on the use of this system to purchase across the Internet, but no large-scale scheme has yet been attempted.

In 2000, all major credit card associations rushed to announce their new smart card initiatives. It is interesting to note that the strength of Mondex pushed Mastercard, which normally cooperates with Visa, to strike up a partnership with the former and thus promote Mastercard's own new chip operating system platform called Multos or the Complete Chip Solution. The Multos operating system, referred to in the technical press as "the Windows of smartcards", was developed by Mondex International in London. It is currently the base operating technology of the Mondex Purse smart card and the American Express Blue (smart) Card. Multos is an "open" technology and is owned by Mondex but is governed by the Maosco Consortium that has 14 industry members.[17] The partnership also includes American Express, EMV Credit/Debit Chip programmes and others.[18]

Meanwhile American Express and Compaq have linked their smart card programmes by using American Express blue cards together with the Compaq Smart Card Keyboard suitable primarily for individuals and small businesses.[19] In December 2000, Visa in turn launched together with IBM and Phillips Semiconductors, its low-cost smart cards supported by four major smart card manufacturers. The so-called Visa Price Breakthrough is proposing to its member banks open platform multi-application smart cards for a price of three dollars instead of the average price of a microprocessor chip card of around six dollars. Based on Java Card 2.1 and the Open Platform 2.0 specification, the card initially proposes credit/debit functions and other applications. The latter could be loaded in the read-only memory (ROM), while there will also be room for other multiple applications in the so-called erasable memory compartment (EEPROM), giving issuer banks the possibility of proposing secure Internet access, loyalty programmes and other options.[20]

One of the difficulties of using smart card based payment methods for e-commerce is that each user terminal must be equipped with a smart card reader. Although many thought that this hardware would become part of a standard specification PC, this has not yet happened. Nevertheless Visa has announced that smart cards will represent more than 30 per cent of its cards in five years and 70 per cent in 10 years. Although that statement seems for the moment to be a bit strong, the pace of technological advance and the pressure to address the issue of fraud might create smart card momentum.[21]

(d) Internet banking

In many OECD countries, bank customers are more and more encouraged to use the Internet for all their bank related operations. A client operating through a PC linked to Internet opens the special e-banking site of his bank and then, using a set of special secure numbers, gets access to his bank accounts and has the opportunity to consult them, as well as to make all necessary payments and transfers from his personal accounts. For example, in the case of UBS e-banking, the client enters his e-banking contract number, the password in numbers (PIN) and an individual number for each transaction. When the transaction numbers are exhausted the bank sends him a new set of numbers for his individual transfer sessions.The downloaded bank software programme can also be utilized offline, for example for preparing the payment orders offline and then making the actual order online. The client receives all numbers separately, mainly by mail. The bank also provide clients with similar facilities in its premises so that clients can use bank equipment such as an ATM or a special facility linked to the main terminal facility called Multimat, permitting them to effect the same account examination, payment and transfer operations without consulting the bank staff.[22] Variations of above model are proposed to their clients by many banks in OECD and some emerging economies.

(e) Other systems

(i) Electronic Mobile Payments Systems (EMPS)

A variant of smart cards may play a role in the emerging area of mobile commerce (m-commerce). Since all GSM digital phones contain a smart card (referred to as a Subscriber Identity Module or SIM), and there are expected to be billion mobile phone subscribers in the world by 2002, this represents a huge user base. Yet it is far too early to say what form the mobile Internet will take and whether the presence of a SIM will be influential in determining consumers' modes of payment in this environment.

One example of this approach concerns the pilot project of Meritanordbanken, Nokia and Visa aimed at making payments from a mobile phone. The system uses the Wireless Applications Protocol (WAP) to access Internet sites and the smart card based SIM to assist in securing payment. Mobile phones can also be used to get online financial news, especially on forex and share prices, besides making basic online payments and transfers. Supporters of this model from Nordic countries believe in the future of m-commerce as a main vehicle of e-commerce. Some call it me-commerce (mobile e-commerce).

(ii) Interactive television (iTV)

iTV is considered to be one of the future channels for bringing e-commerce, including simple forms of e-banking and e-finance, to households. Linked to the Internet through digital TV packages, iTV involves a simplified screen and remote control and is easy to use. However, it might be limited to services proposed by a given ISP. Given the relaxed position approach of TV viewers, financial service providers would most probably choose iTV for basic financial advice rather than for complex interactive financial

transactions. However, the success of TV sales channels suggests that TV-e-marketplaces will grow in popularity and might present merchants and buyers with value transfer opportunities that compete with PC based channels of e-commerce. As a result, companies supplying iTV technology and services might have unique opportunities to supply an exponentially growing market.

(iii) Shared account based systems

Most of the technology involved in a credit card transaction is required because the merchant and buyer have accounts with different banks (possibly in different countries) and each transaction involves both a check for funds availability and ultimately a transfer between banks. Pooling big groups of users so that they hold accounts with the same entity greatly simplifies transfers. When a transaction is to be made, this one entity is contacted and requested to transfer the funds from the buyer's account to the seller's account. There are numerous systems of this type available on the Internet, most of which are operated by companies that are not banks or financial institutions. Two that are worth mentioning due to their substantial customer bases are Yahoo PayDirect[23] and PayPal[24]. These systems all have links to conventional payment systems, e.g. bank accounts or credit cards to inject or withdraw money from the system, but conceptually any method can be used. Indeed some systems, e.g. PocketPass[25], allow the account to be primed with cash by buying a prepaid card in a store.

The difficulty these systems have in succeeding is that they essentially create relatively closed pools accessible only to people who have registered to use their service. Since, initially, only a few merchants accept those circuits, it makes them less attractive for buyers. This chicken-and-egg problem has caused many companies to fail in providing payment services. Nevertheless, for countries where the existing financial infrastructure is poor and the alternatives are few, such account-based systems may be highly practical, provided that the common system is under adequate regulatory control to ensure protection of the account holder's money.

(iv) Charging to the telephone account

The regulatory changes permitting telecommunications (telco) providers to charge customers for services unrelated to telecommunications has opened a possibility for telco companies to compete or cooperate with financial service providers in rendering payments services. The charges for goods and services go to the authorized telco account in a way similar to a credit card related process and then the telco enters those charges into the monthly telephone bill presented to the customer. The simplicity of charging for consumer goods through telephone bills and the fact that more people have telephone than a banking relationship adds to the competitive pressure on banks and credit card companies as providers of retail payments services. In fact history has already shown a working model — the Minitel in France.

(f) Considerations for credit card and other online B2C payments for developing countries

One lesson that has been learnt from the early years of e-commerce is that merchants must adopt a method of payment that is easy for their customers to employ. Many payment methods have failed due to the need for complicated signup procedures or the need to set up accounts.

Where the customer base for a given product or service already uses credit cards for conventional commerce, cards serve as an ideal method for online transactions. Although there is widespread unease about the security of typing credit card details into web forms, the use of SSL on a merchant site seems to allay most people's fears and the prospect of SET becoming available in the medium to long term should significantly reduce both the perceived and real risk of fraud.

In a scenario where companies and individuals located in developing countries are selling products and services to those in developed nations, the credit card may prove to be extremely effective. Although the transactions do demand financial infrastructure, this can be provided by third parties in countries with developed and robust financial systems and no limitations in respect of currency exchange. Moreover, given the competitive exchange rates proposed by credit card companies to their customers, the latter do not worry too much about the currency denomination of the sales contract, although for the buyers convenience, the currency used in the transaction should be that of the customer rather than that of the merchant.

Wire transfer can be used to transfer aggregate amounts back to domestic bank accounts at regular

intervals. Similarly, the provision of the web site that offers the goods for sale can also be outsourced to a global data center provider close to the core Internet with its content being managed by personnel from the originating country.

Where transactions are intra-country, it is important to choose methods of payment that are appropriate to the local population. In countries where the local banks do not issue credit or debit cards, these would be a very poor choice as an online payment method.

A major impediment to B2C e-commerce and online payments is the system of informal relations between local traders and the retail customers in developing countries. Being used to personalised relations, those clients would have to overcome more psychological hurdles than their Western counterparts when resorting to the Internet. Only price differences and a sort of personalised after sales service could help to overcome that hurdle. As the informal economy might persist as a considerable share of national economies in many developing and transition economies, large amounts of unregistered cash balances with consumers could still be used to effect offline payments for goods and services ordered through Internet.

2. Business to business (B2B) online payments

B2B and B2G transactions differ from B2C transactions in that they involve a more limited and stable number of participants in a given business chain or a given government procurement operation. However, in one-to-one transactions, the use of cards or checks as a means of online payment for the delivery of goods and services is generally based on the same type of procedures as in B2C transactions. The reason for considering checks under the B2B heading is that commercial checks represent the bulk of checks, they involve large sums and might have long-term future in B2B e-commerce.

The similarity of B2B and B2G transactions is also based on the use of common contractual relations and payments instruments, as well as on the fact that parastatals act as common corporates or contractual parties within a framework of similar contractual rights and obligations. Differences arise only in the legal treatment of defaults and bankruptcies and have little to do with online payment techniques per se. As far as procurements of government agencies are concerned, they are treated in the chapter 5 on e-government of this report. Thus, for the sake of simplicity, here reference will be made only to B2B online payments.

In the years prior to the Internet revolution, the electronic data interchange (EDI) community was addressing the problem of automating the exchange of trade-related documents between companies. This activity experienced an annual growth rate of around 70 per cent, with the number of EDI users in the United States growing from under 2,000 in 1987 to over 31,000 in late 1992, even though many of the standards to be used for document content and transfer had not garnered widespread support. [26]

When the Internet, in the form of the World Wide Web (www), began to achieve consumer acceptance, the initial wave of e-commerce was driven by the sale of goods to consumers, i.e. the B2C sector. Around 1998, many companies, including some from the EDI community, turned their attention to the huge amount of trade that takes place between companies. Many of the ideas that had been present in the EDI community achieved a new expression with Internet users. New standards for documents have come to the fore — some derived from older EDI standards such as EDIFACT and others that started from scratch using new syntaxes involving XML. The technology and banking communities have also turned their attention to how B2B transactions should culminate in payment.

One of the things that differentiate B2B trading from the consumer market is the fact that the relationship between suppliers and buyers is typically long-lived. Where B2B e-commerce can really make a difference is in bringing together larger groups of traders in an environment that increases choice and stimulates competition (for detailed analysis of various kinds of e-marketplaces, see chapter 4).

(a) B2B e-commerce platforms: from initial participation to payment

A number of specialist companies as well as the more established companies have produced e-commerce platforms that contain all of the ingredients that go to making up Internet sites geared at business-to-business trading. These software suites focus on carrying out a set number of functions, as described below.

(i) Filtering participants

Most B2B commerce sites require a new member to sign up, giving details of their companies. While the initial contact takes place online, there is generally some kind of a vetting procedure before membership is granted. For example, WorldofFruit (www.worldoffruit.com — a site that allows companies in the fruit industry to trade with each other) grants membership only to established companies with annual revenues in excess of $1 million, whereas Ingredientsnet (www.ingredientsnet.com — a site that focuses on the food ingredients industry) requires applicants to have been in business for at least a year with satisfactory credit ratings. These simple checks massively improve the climate of trust that can exist between members of these sites, but fall short of what might be needed to support a financial transaction of a considerable size.

(ii) Networking supply and demand

Easy interfaces are provided to buyers and sellers to specify their requirements or the details of what they are offering or wanting. One of the major advantages of an e-commerce environment is that it can bring an offer to the attention of many more players than would be possible without the use of the Internet. In fact one of the earliest UNCTAD e-commerce initiatives was the so called UNCTAD Global Trade Point Network (GTPNet). The main rationale behind the GTPNet was facilitating SMEs' export potential by giving them an opportunity to offer their products and services through the GTPNet, which became one of the most frequently visited sites on the Net. Similarly CommerceOne links all of its eMarketSites and thereby their buyers/suppliers together in what they refer to as the Global Trading Web(GTW) to accomplish a similar objective.

(iii) Price negotiation

Online tools are typically provided to facilitate price setting either as a result of a one-to-one negotiation or through the use of an online auction. Payment-related parameters can also be agreed upon at this point. Thus Chematch (www.chematch.com — a petrochemical B2B portal) allows the parties to specify the terms of delivery and also whether letters of credit or other modes of payments will be required. An evolution in purchasing is now occurring whereby buyers are initiating reverse auction, requiring suppliers to bid down in order to secure business contracts. This evolving style of purchasing is proving very successful and is being heavily promoted by the e-marketplaces.

(iv) Payment

Although some of the software suites for e-commerce do have components that help with payments, most of the B2B e-commerce sites do not yet offer this facility online. Since the amounts of each transaction can be quite large (Chemmatch has already had over $425 million transacted with the average transaction exceeding $500,000) companies often resort to appropriate conventional i.e. offline means to effect the payment. However, given the trend, one could presume that this will change. In fact many of the technology providers operating in this market are active participants in the efforts described below to bring these more conventional proprietary electronic high-value payment methods to the Internet.

High-value B2B payments are almost always bank-mediated, and for these systems to move to the Internet, they need to garner the support of the banking industry as a whole. The bankers' communities of both developed and developing countries are usually the leaders in setting the national agenda for the development of Internet trading standards.

(b) Electronic checks: a case for using digital signatures and PKI

It is instructive to look at the initiatives undertaken in developing electronic checks. For some years, many financial service providers grouped in associations or consortia have been working on a specification for electronic check-based payment with a view to developing primarily B2B payments solutions. One of the leading consortia in that respect is the Financial Services Technology Consortium (FSTC) of the United States - an organization made up of the main American banks and banking technology providers. Formed in 1993 to enhance the competitiveness of the United States financial services industry through the use of technology, it made considerable progress in its attempt to make the electronic check a common online payments instrument.

An electronic check is a document containing fields identical to those on a paper check with appropriate digital signatures being added when the check is first issued by the payer and also when it is endorsed by the payee. A pilot run by the United States Treasury

and Department of Defense using these checks started in mid-1998, and a new syntax for expressing the check, called the Financial Services Markup Language (FSML), was defined.

Electronic checks expressed in FSML may be exchanged by trading partners in future B2B exchanges. Before these can be processed, though, the banks involved must have the appropriate technological infrastructure to process them and to use the information contained therein in order to effect the inter-account and inter-bank transfers required. The FSTC has laid out an architecture to upgrade a bank's existing technology, to simplify the ACH (and eventually ECP) based interface, and hence to add the capability to handle electronic checks issued and transferred between organizations on the Internet.

Electronic checks are one of the examples which can exist only if secure digital signatures can be applied and thus make them acceptable as an online payment method.

(i) Digital signatures

Digital signatures are produced by electronically digesting the document to be signed and producing a small unique piece of data that represents an electronic fingerprint of the document's contents. This fingerprint is then encrypted using a secret number called the private key. The encrypted fingerprint is the 'digital signature' and the only person that can sign a document is the holder of the private key.

When any other party wants to verify that the signature is correct, they decrypt the document using a non-secret number referred to as the public key. If the result matches the fingerprint of the document they accept the digital signature as a genuine one. In order to use this technique as a substitute for real signatures, the last element needed is a way to associate a person's identity with a particular private key.

When people travel from one country to another, they assert their identity by producing a passport. This document provides a link between their appearance (and their handwritten signature if necessary) and their identity (name and date of birth). It is accepted at border posts because the passport is issued by a national government trusted by those officials.

The electronic counterpart of this is called an X.509 certificate. It is an electronic document that provides a link between a public key and the identity of a person or company and is signed by an entity that is widely trusted and called a Certification Authority (CA). In fact a triangular relationship emerges between the Certification Authority proper, i.e. a public agency defining the rules and criteria for establishing an "electronic passport", the Registry Authority (RA) accepting and verifying persons and entities requesting an electronic signature, and the Certification Company (commonly labeled the Certification Authority), which actually supplies the above-mentioned private keys to individual users and makes sure that they are compatible with their own public keys.

Once a single CA or an international network of co-operating CAs that is widely trusted is established, it is possible for people to send signed digital documents such as electronic checks to each other. By including the X.509 certificate with the document, they allow the recipient to verify the signature on the document.

(ii) Public Key Infrastructure (PKI)

A network of cooperating Certification Authorities, Registry Authorities and Certification Companies is often referred to as a public key infrastructure (PKI), and the slow acceptance of this network and the related electronic signature and personal identification technologies has been one of the factors delaying the widespread acceptance of electronic checks and other signed documents that will be essential for B2B e-commerce.

The deployment of PKIs takes a considerable amount of time, and it only becomes useful when very large numbers of users have both the awareness of the contribution it can make to building trust online and also software that supports the verification of online signatures. It is also true that, just like passports or any other identification scheme, systems need to be put in place to cover the full lifetime of the identifying document, including coping with renewal, loss, confiscation or revocation, etc. Clearly, where transactions worth many millions of dollars may be at stake, important issues of liability and negligence might arise for those involved in ensuring the security and reliability of the PKI.

According to one source, the global electronic certification market is highly concentrated and is controlled by three companies, namely VeriSign of the United States, Globalsign of Belgium and Thafte of South Africa.[27] The information on market shares here is

based on the estimates of a private source and could be contested, but apparently the market is a heavily concentrated. Certification authorities are also often operated by major postal or telecommunications entities in individual countries. A good example of this is the United Kingdom, where the Royal Mail operates the ViaCode CA and British Telecom competes with them to operate the BT Trustwise service. In Argentina, the Government operates a digital signature infrastructure directly. It is important to note that, for trust to be established across a network, both users of the service must be signed up with the same certification authority. However, in general, these certification authorities do not work together, and the scope of their service is extremely restricted. However it is true that most PKIs that have been built so far have been general-purpose in nature and often limited in their scope to a single country.

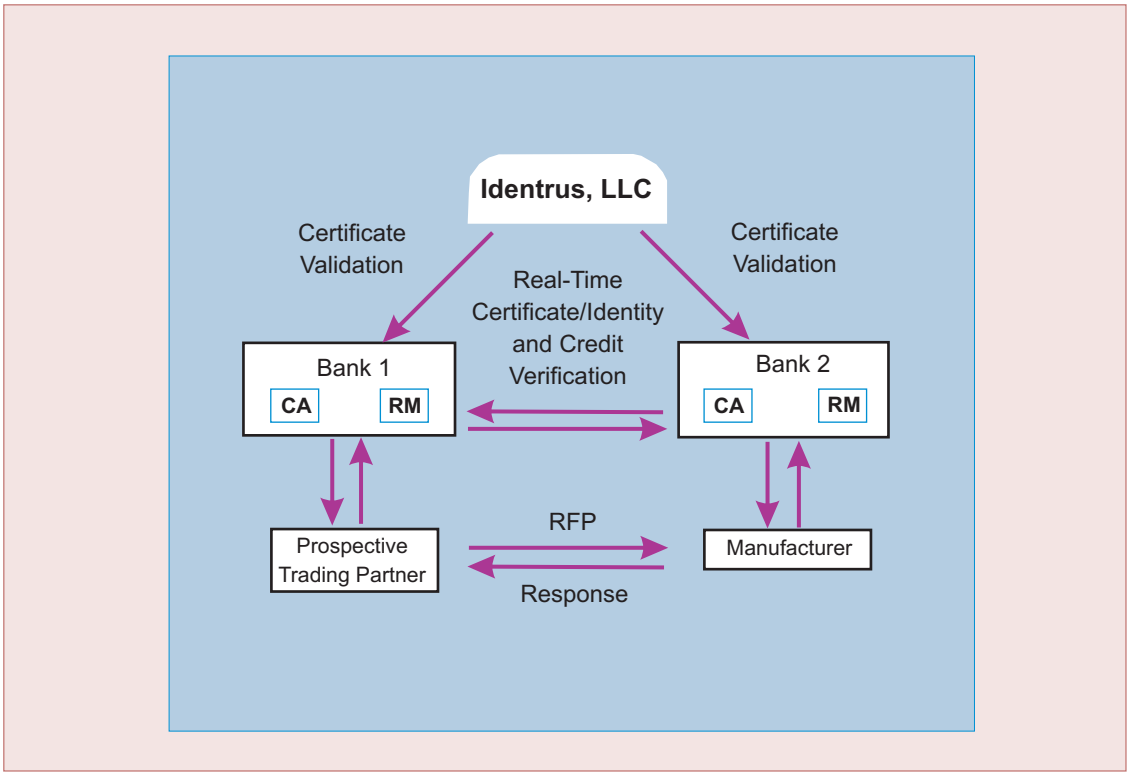
An example of a global PKI formed by financial institutions to enable secure online payments of all kinds is the IDENTRUS consortium. Following an initiative that began in November 1997, Identrus™ LLC was launched in April 1999 by its founder members: ABN AMRO, Bank of America, Bankers Trust (since acquired by Deutsche Bank), Barclays, Chase Manhattan, Citigroup, Deutsche Bank and Hypo Vereinsbank. The purpose of this initiative was more precisely to set up a system to allow the circulation of electronic documents in online payments. As chart 16 shows, Identrus LLC operates a common root certification authority on top of local CAs operated by the member banks around the world. Trading partners can exchange signed trade documents with each other using any Internet-related mechanism and these documents can be verified against an identity certified by a trusted banking entity.

In sum the complexity of PKI and various initiatives and systems in this area raises issues of their interoperability, customization, pricing, governance and oversight.

(c) B2B Internet banking

Pending the wide availability of electronic checks, one method of making large business-to-business payments that is becoming increasingly popular is to employ Internet banking. Bank-mediated transfers such as ACH debits or credits, as well as domestic and international wire transfers, which had hitherto required a paper request, can now be initiated directly by companies. This trend pre-dates mass Internet usage and was initially called business banking, where

Chart 16
An e-commerce exchange making use of Identrus certification services



high-value clients were issued with special software which, using a dial-up connection, could monitor the status of their account and also initiate payments. Placing a web base at the front end of this service allows it to be made available to a wider range of banking clients.

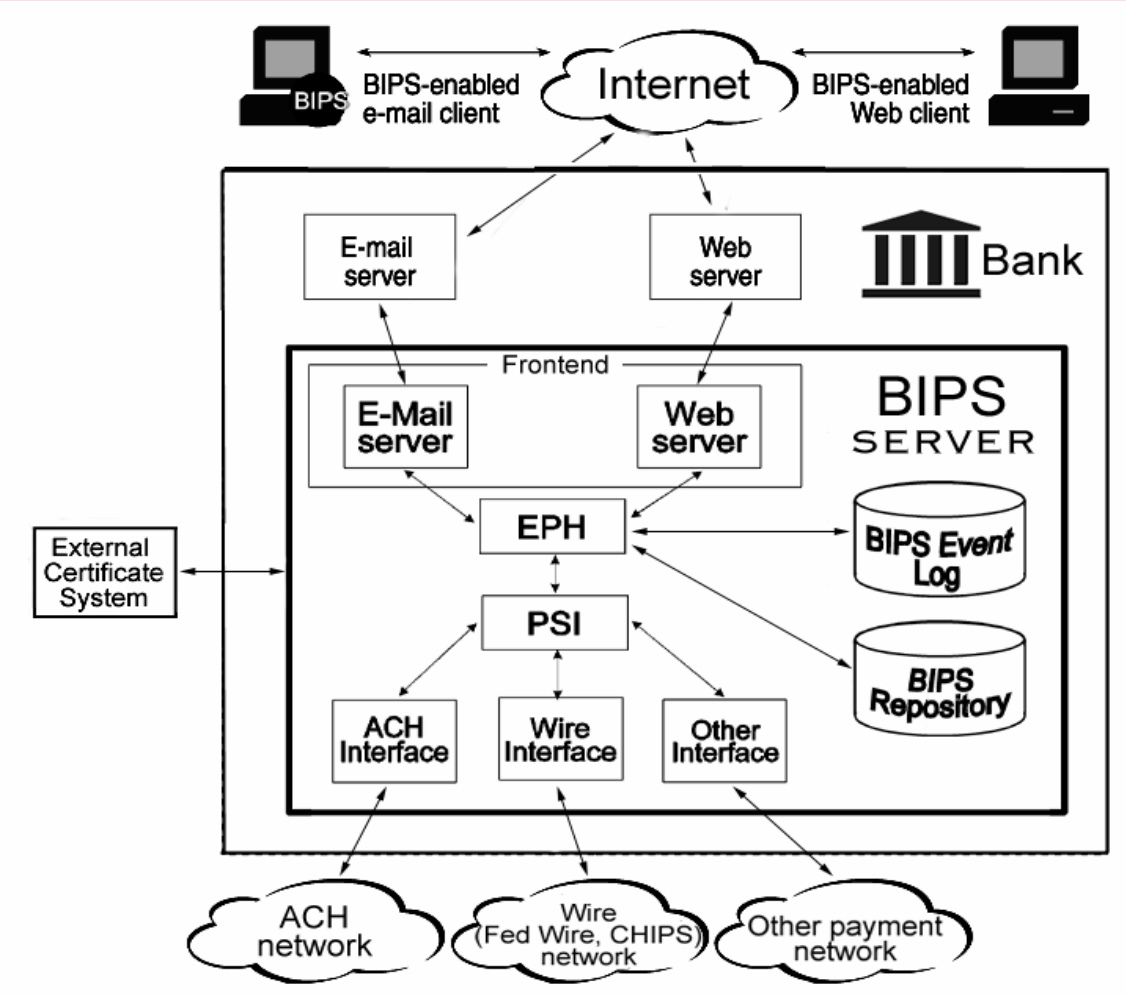
Many B2B e-commerce exchanges serve principally to bring together the transacting parties. Once the deal is arranged and the price agreed, the parties can then effect payment using an Internet banking service. This is a system to which all parties are already accustomed and works well even though the payment process is not integrated with other parts of the transaction.

(i) FSTC Bank Internet Payments System (BIPS)

In 1996, the United States Financial Services Technology Consortium (FSTC) initiated a project to come up with a very general way to allow companies easier access to payment services. Their approach involved making as few modifications to the existing United States banking systems as possible. Chart 17 shows how the Bank Internet Payment System (BIPS) acts as an Internet 'frontend' to the existing ACH, wire transfers and other bank networks. Messages such as 'payment requests' can be initiated by either e-mail or web-based software. A Public Key Infrastructure (PKI) is assumed to exist, and this component could be provided either by the Identrus or similar projects described earlier.

BIPS was demonstrated in a number of projects involving Glenview and Mellon banks in the United States in August 1998, but there has been no public progress beyond that. This may change as the Identrus PKI becomes more widespread, enabling many more users to make use of BIPS or BIPS-like services.

Chart 17
The Bank Internet Payment System (BIPS) architecture



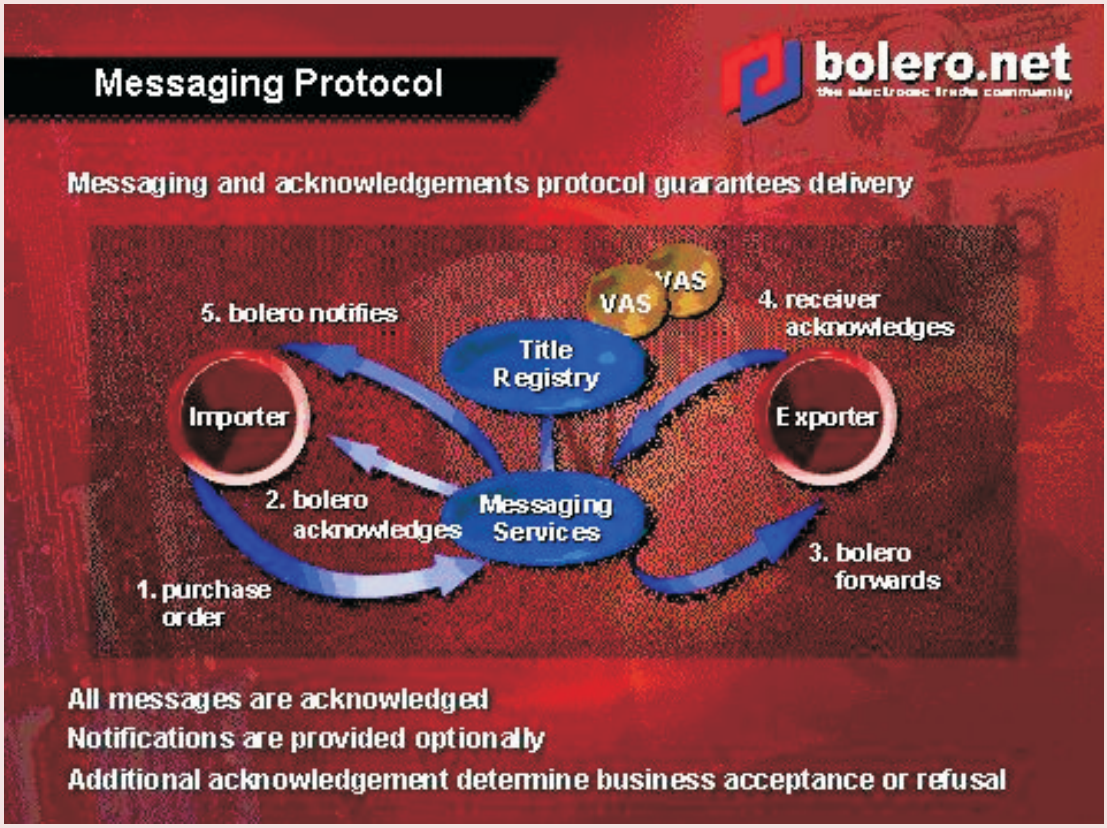
(d) E-Finance for international trade in EDI-like systems

The predecessor of today's B2B e-commerce phenomenon was the Electronic Data Interchange movement of the late 1970s and early 1980s. Prior to the widespread adoption of the Internet and before the World Wide Web was invented, companies that did regular trading with each other were focused on two things. Firstly, great efforts were made to standardize common electronic versions of standard business documents such as invoices, purchase orders, statements of claim (for the insurance business) and a host of others. This had quite a degree of success and led to the adoption of the Electronic Data Interchange for Administration, Commerce and Trade (EDIFACT) syntax and supporting message standards. Secondly, the communities built private or quasi-public networks to allow trade documents to be conveyed. The most highly evolved of these networks supported a derivative of X.400 e-mail referred to as X.435 which had many extra messaging facilities specifically targeted at the EDI user. These networks were referred to as value added networks (VANs).

The emerging model for B2B e-commerce at the beginning of the twenty-first century takes the form of a web portal site concentrating on bringing trading partners together for online negotiation, contracting, delivery and payments. For many industries, this model has a promising future, as the business community may be better served by having a reliable means of exchanging trade documents in the way it was done in the EDI model.

Few Internet-based platforms are trying to face this challenge. One of them is the www.bolero.net — a company created in 1998 from an alliance between S.W.I.F.T. and TT Club (an insurance association for the shipping industry) which tries to provide a neutral platform for simultaneous interchange and certification of all trade-related documents, from sales

Chart 18
The Bolero system



contracts changes of ownership and in some cases payment.

In the case of Bolero, they have built a private network that allows companies to send trade documents to each other. As chart 18 shows, a central function intercepts all messages to provide an audit trail and also to provide explicit acknowledgements of the delivery of documents. The Bolero community has also defined the syntax for a large number of trade-related documents using XML syntax (the messaging service can verify that a document confirms to the syntax before it is accepted into the system). The Bolero system assumes the existence of a PKI and, in addition to certificates issued by itself, it can handle ones issued by other systems. Although payment is not explicitly supported by the Bolero system, one of the message types that is standardized is the "Payment Instruction". This gives a mechanism for a company to instruct a bank to make a payment across the Bolero private network. In fact, to ensure the secure exchange of documents on its platform, Bolero entered into cooperation with Identrus at the end of 2000. The secure keys issued by Identrus participating institutions should be valid in the Bolero online trade system and at the same time permit the Bolero Multiple Certification Authority (MultiCA) to let entities using their national PKA secure keys gain access to Bolero.net services.[28] At the same time in spite of heavy investment in Bolero, the expected capacity utilization has not yet been achieved and bigger turnovers will be required.

The same is true for a finance platform that is more focused on international trade called www.tradecard.com, developed by a US-based company called Tradecard. The intention here was to replace the traditional bank-based letters of credit (L/C) by a similar online system and bring partners together online. Tradecard gives a possibility to buyers and sellers to negotiate on the Internet using all trade-related documents, including the buyer's electronic purchase order, the seller's commercial invoice and packing list, the buyer's payment assurance, the approved logistic provider's proof of delivery documentation, etc. Once the compliance of all these documents is assured, the payment takes place. Tradecard, as far as payments and trade financing solutions are concerned, is in cooperation with such partners as Mastercard (corporate payments solutions), Coface (credit insurance and information) as well as commercial banks.[29] Some banks, after an initial negative reaction to an online substitute for the L/C, later found the new instrument useful and agreed to cooperate. At the same time, although the announced transaction costs of becoming a member and transacting through the system seem to be rather small[30], Tradecard so far proposes only a substitute for a basic L/C and cannot compete with commercial banks by proposing a full range of L/Cs.

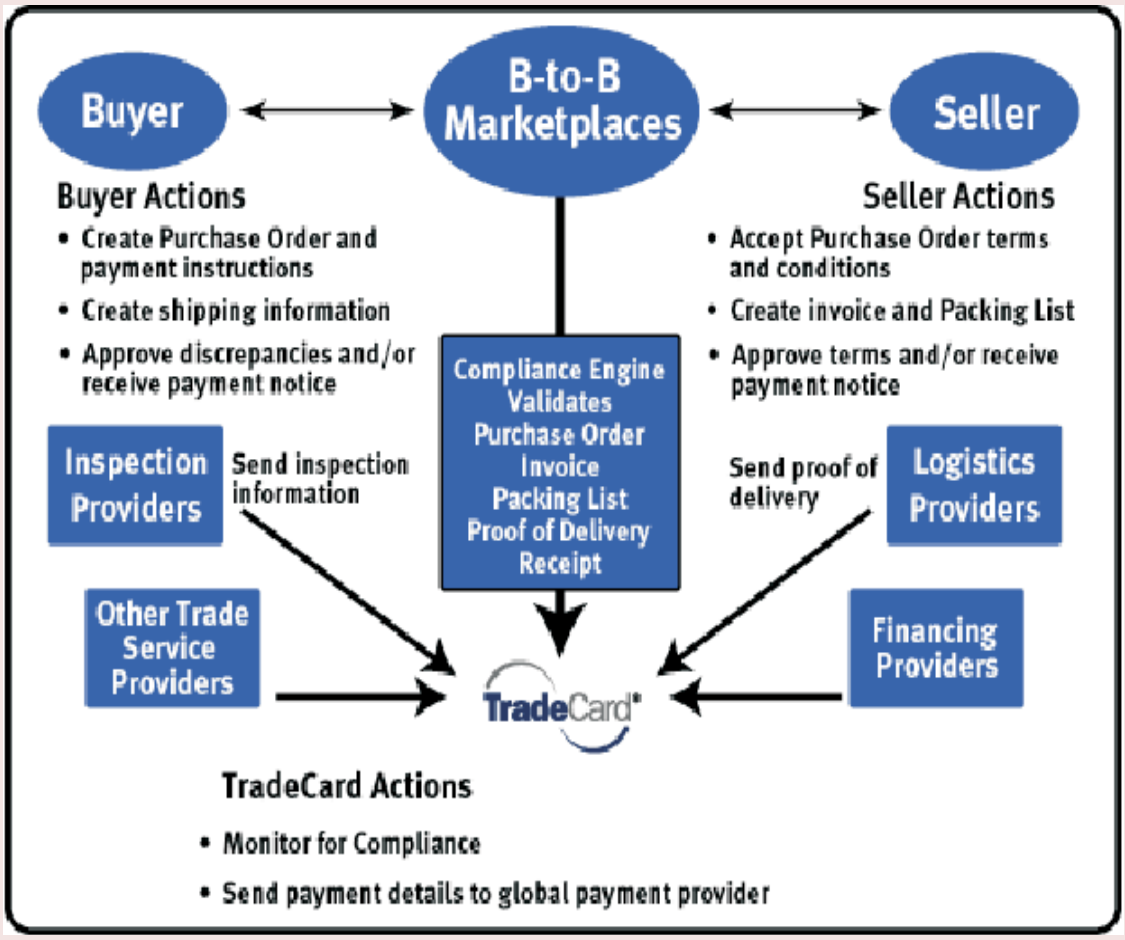
In fact online trade finance platforms are continuing to proliferate. They are a result of strategic alliances and co-ownership of banks and technology companies or represent the innovative know-how of some new start-ups. They include the Internet Trade FinanceExchange (ITF), LTPtrade.net, @GlobalTrade and others.[31] At the same time many of those new platforms are for the moment new ventures and need more liquidity injections.

(e) Online payments risk management by third parties

Up to now, most of the fraud that has been perpetrated online has been related to B2C transactions paid for with credit cards. In the United States, just over 3 per cent of the total volume of transactions are fraudulent, but it is suspected that in the Internet world, this percentage is very much higher. In some countries the so called charge-back ratio — the percentage of credit card transactions that are later denied by the cardholder — exceeds 50 per cent. This fraud rate is likely to persist and perhaps increase as long as the predominant security technique is SSL. If SET or some stripped down version of it were to be deployed, this figure could be cut down dramatically.

Normally a B2B transaction takes more time than a B2C one and consequently this allows more time for checking. In the future, as the process becomes more automated, more opportunities for fraud will arise. Since the transactions are fewer in number and are of a typically much higher value, the types of criminals attracted to this area will differ from the credit card fraudsters. Since the primary means for asserting identity in such transactions will be the X.509 Certificate, it will be imperative to ensure that this certification process is not subverted. Many countries in the developed world are in the process of enacting e-commerce legislation which sets out the requirements for entities to operate public certification services. In many cases, there are specific provisions included to deal with negligence and consequent liability of certification providers. Users of such services should also develop an awareness of the issues

Chart 19
The TradeCard Architecture



involved and the legal protection afforded to parties contracting with each other using digital certificates.

For a successful B2B transaction to take place, it is not enough for contracting parties to know about each other's existence and credibility. As in the case of the conventional transaction protection by third parties (see section B, subsection 5) the Internet also needs modern tools of risk management. The leaders of industry are moving online to follow their clients and to protect them from political and commercial risks inherent to transactions.

According to one of the biggest global credit insurers — Coface of France — more than 35 million enterprises are going to transact online, and all of them will need to have an image of visibility and credibility on the Internet. To follow them in B2B business, Coface has developed a so called @rating system where enterprises could get various @rating labels depending on the credibility and credit standing of the enterprise and according to the Coface credit information database. The label means that Coface confirms that a given company will honour its debts up to a given sum per transaction. In other words when a company sells to a trading partner which has already got a Coface @label for a given sum, then the former might be insured from the risk of default for that sum. At the same time, the Coface @label could guarantee a trade credit of the same level for the enterprise to finance its exports of goods and services. The labels cover amounts from 20,000 euros to more than 100,000 euros, which corresponds to from 1@ to 3@L respectively.[32] If this system starts to function it might give many third world companies striving to sell abroad but having a problem getting access to pre-export or working capital financing direct access to trade credit on more competitive terms than they might otherwise have received from

local banks. That in turn might improve many developing countries' access to international trade finance and investment resources.

Another example of managing company risk online mainly through providing credit information and decision-making tools online concernes Dun and Bradstreet (D&B) of the United States, the biggest credit information provider in the world. Last year its worldwide operations brought the company $1.4 billion in revenues. The company maintains and constantly updates (one million changes a day) databases on 60 million companies. It has 150,000 clients and is famous for its so called D-U-N-S number. Companies which hold this number are considered good risks by banks and can get trade finance and trade on open account.[33] By 2002, D&B is also planning to move to the Web the activities bringing in 80 per cent of its revenues. Last year D&B joined with American International Group Inc. (AIG), one of the biggest insurers, to propose an online B2B risk management product dubbed Avantrust (SM), targeted mainly at online exchanges, Internet-based market makers and supply chain extranets. It was claimed that functions of the Avantrust platform would include confirming the identity of trading partners, inspecting goods, managing and insuring counterparty risks and insuring delivery. It is also supposed to insure eMarketplace web sites, thus helping them to build liquidity, reduce risk and increase trust between trading partners.[34] Such a massive move online of the above and other credit information, credit insurance and other financial services providers will definitely have a major impact on online third party management of primarily B2B credit and performance risks.

(f) New regional and global payment systems and B2B sites: Challenges and opportunities for developing countries

Many of the examples above involve businesses making bank-mediated payments where the most often cited back-end payment method is the Automated Clearing House (ACH). Although most developed countries and many developing ones do have national ACH-like systems, nowhere are these as open and accessible to industry as in the United States. The fact that each of the systems is strictly national, limits their usefulness for international e-commerce. Some new initiatives may be about to change that.

As part of their preparations for monetary union, the Member States of the European Union put in place a new pan-national high-value wire transfer service called the Trans-European Automated Real-Time Gross Settlement Express Transfer (TARGET) system. This has been in operation since 1999 and allows large real-time transfers denominated in euros to be made between participating countries. A low-value variant of this, called Straight Through Euro Processing (STEP), was launched in November 1999 by the Euro Banking Association. The maximum transaction size is •50,000, with a low processing fee of •0.48. In the future, this could become very important for e-commerce in the euro zone.

At a global level, an initiative spearheaded by NACHA in the United States might give rise in the future to a Worldwide Automated Transaction Clearing House (WATCH).[35] This system, which is due to come into operation in July 2002, will bridge the national ACH systems to provide credit-only transfers in six to eight different currencies as a first step. Once again, this holds great potential as a payment method for global e-commerce.

It is generally thought that the advent of e-commerce will on the whole be beneficial for developing countries. It removes many of the conventional barriers to trade that stem from countries being far from the target market. Because the content of the Internet is not highly divided along national lines and the fact that all content is equally accessible, developing countries can have the same access as their developed counterparts to customers on the Internet.

The economic data so far suggest that the sectors that have benefited most from the introduction of e-commerce are mostly in service areas such as ICT, tourism, finance, publishing and information services, Internet services and other professional services, which were initially of more relevance to developed countries.[36] However the advent of B2B e-commerce could greatly extend the number of services sectors that are and could be of relevance also to developing countries. Computer hardware and software, other types of manufacturing and services, including e-tourism, could be at the forefront of this breakthrough (for more details on e-tourism see chapter 3).

At the same time, the developing countries are still mainly producers of primary goods, semi-manufac-

tures and low-end manufactures, and they should first, capitalize on the many opportunities arising in these sectors. Thus they might take advantage of the fact that many commodity exchanges and large manufacturing systems largely based on subcontracting for procurement are moving online. The competitive terms instantaneously proposed by developing country suppliers to buyers from global e-marketplaces and e-procuring systems should create new business opportunities for them.

Virtually every primary commodity is now served with a B2B e-commerce site. Table 25 shows some representative examples.

Such web sites bring together a community of buyers and sellers based on the products they have to offer or need to purchase rather than the geographic region that they operate in. In that sense, they create a global marketplace to which developing countries should have full access. These sites also may have the effect of causing disintermediation in those markets that could represent both opportunities for developing countries selling to foreign markets and a threat where the flow is in the reverse direction. Developing countries should explore the options available to them to fully participate in and indeed form B2B e-commerce markets in economic sectors that are important to their economies.

As yet, most B2B e-commerce sites support all phases of a transaction but stop short of providing payment services. So, for the present, B2B transactions rely on conventional payment methods. This situation is likely to change in the short term, and one could expect electronic variants of ACH, electronic checks, smart cards, electronic L/Cs and others to be incorporated into the trading dialogues that take place on these marketplaces or integrated foreign trade sites.

Developing countries wishing to be at the forefront of these developments will have to pursue different strategies to support two separate objectives, namely facilitating e-trade with foreign companies and B2B and B2C marketplaces, and starting to develop domestic e-commerce. Where the national payments infrastructure is underdeveloped and has few international linkages, it may be expedient to conclude B2B transactions with the financial transfer taking place between accounts held in countries better connected with trading partners' banking systems. This may involve maintaining business accounts with leading international banks, including for example United States banks giving full access to FedWire, ACH and BIPS-like services, European banks in the euro-zone to access TARGET and STEP services, or banks with a similar level of services in other developed and developing countries.

When it comes to domestic transactions, efforts could be focused on improving the payments infrastructure and conducting initiatives to open up payment services to companies that wish to trade on the Internet. Where it proves to be problematic to institute these changes in national banking systems, consideration should be given to setting up private account-based payment systems that can be used by companies trading on the Internet operating in related areas of business. These private systems would be providing a service akin to private banking and may need regulatory oversight.

In the longer term, developing countries should keep a watching brief on global developments such as WATCH, looking toward the day when a global payments network would be accessible to the majority of developing and transition economies and their companies trading or having prospects of trading on the Internet.

Table 25
Examples of commodity and food related e-marketplaces

B2B e-commerce site	Industry sector
www.forestindustry.com	Forest and wood products
www.chematch.com	Bulk commodity chemicals, polymers and fuel products
www.worldoffruit.com	Global fresh produce industry
www.esteel.com	Global metals supply chain
www.inc2inc.com	Connecting food manufacturers and suppliers of ingredients and packaging
www.rooster.com	Marketplace for farmers, dealers, co-ops and manufacturers to buy and sell the inputs needed for farming

D. Online Payments, Monetary Policy and Financial Stability

Governments regulate conventional commerce to protect both the interests of the parties involved in transactions and the legitimate interests of society at large. Banking organizations and similar financial institutions have their operations overseen by central banks, which have a number of distinct concerns. If a banking organization were to fail or to behave fraudulently this could negatively impact a large section of the population and their savings and could have knock-on effects throughout the entire economy. Clearly, if a non-bank organization is operating either an electronic cash system or one that is based on accounts, it is holding a substantial amount on deposit on behalf of its customers. The European Central Bank (ECB) examined this issue in 1998 and concluded, among other things, that the issuers of electronic money must be subject to prudential supervision and that they should be legally obliged to redeem the electronic money at par value. [37] Historically, the US Federal Reserve has taken a more hands-off approach, opting to let the market for new Internet-based payment methods develop before introducing regulation.[38]

Another concern that regulatory authorities have regarding new methods of payment relates to the effect on a country's money supply of new unregulated organizations issuing cash without recourse to government. The American view on this is that the amounts that are currently stored in electronic purses are so small that they do not constitute any risk. Once again, the European view is stricter and requires e-money issuers to supply the central bank with "whatever information may be required for the purpose of monetary policy". The European Parliament has recently adopted a directive on the regulation of electronic money institutions, which will give legal force to this. [39]

At present, e-finance in developing and transition economies is mainly about the possibilities of the use of online banking and payments for companies participating in B2B e-commerce at the global and regional level. As the residents of those countries are less involved in B2C e-commerce, the questions of e-money, its use and forms are less pressing. However the issues of governance and digital money supply, which are becoming more actual for developed economies, could become equally important for developing ones in the not so distant future. Hence the importance of highlighting the implications of this phenomenon for financial sector governance from the point of view of challenges faced by both central banks and the main payment agents, i.e. commercial banks, themselves.

For central banks, e-money might mean less need for banknotes and hence lower costs related to the issuing and handling of banknotes. The central bank money supply might diminish due to the proliferation of private monies and money substitutes, including client-attracting bonuses such as frequent flyer miles and other purchasing bonuses. The decreasing share of official money might mean less expenditure on its creation and management, but the costs related to the threats of such official money substitution to the stability and credibility of the monetary system could be bigger, as malfunctioning of the various private monies, many of which could be anonymous bearers' instruments, might adversely affect the stature of the national currency and hence its value and exchange rate.

For financial service providers, the risks ahead include business strategy misjudgments, operational issues, legal and regulatory uncertainty and systemic risks. However, even the best private operators have to pass the public's test on the convenience, universality and trustworthiness of their payments instruments. They must also be perceived by digital cash holders as good risks unless the central banks agree to play the role of lenders of last resort and accept from the public the unspent digital cash claims on failed issuers of those monies. In that respect, it will be interesting to know whether lender of last resort arrangements will be provided for the holders of monies issued by the US Digicash venture, which has filed under Chapter 11 of the US Bankruptcy Code.

Other concerns for users include transaction costs, portability and transmitability, and the anonymity of online payment instruments. Thus if various forms of micro and small payments become popular on the Internet, credit card companies will be pressed to adjust their ologopolistic pricing structures downward. While the Internet makes cash easily portable and transmittable, users might have doubts about their anonymity, which might deter them in countries where the informal economy is relatively large and where real cash is still the most trusted and anonymous means of payment.

At the same time, alongside cost and regulatory aspects, one should also stress another important macroeconomic implication: increased use of online payments might increase the income velocity of money circulation and hence decrease the monetary aggregates needed to service a given level of economic activity in a country. An increase in the speed of money circulation, coupled with the sharply decreased transaction costs of online money transfers, might also imply major savings for consumers and financial intermediaries, as well as increasing productivity for the latter. Achieving such a state of development for financial service providers in developing countries implies closer cooperation between local and international financial service providers, as well as concerted technical assistance, including training from specialized international organizations.

Finally, a key parameter of the success of e-finance will be its impact on financial sector stability. Answering the question as to whether online transfer of money increases or decreases systemic risk needs further detailed examination (it is discussed to some extend in the introductory chapter). A preliminary view on this complex issue would be that the impact is positive/neutral. The possibility of transmitting information and payments rapidly through the Internet might greatly contribute to the functioning of early warning arrangements in the international monetary system due to diminishing information asymmetries and possibilities for more precise analysis and fine-tuning. However, unchecked transmission of alarming news could also trigger the herd instinct in a dangerous form of panic, especially from short-term portfolio investors.

The globalized economy raises the issue of how to create built-in buffers and defenses, diminishing the impact of panic waves on the international monetary system. This represents a serious future agenda for regulators and international financial organizations, who will have to think hard about how the world financial sector is going to change its structure. It will pose new challenges for international coordination, given the global character of the Internet. It will be important, by introducing adaptive and flexible regulations and additional prudential buffers, especially for risk-seeking non-bank financial institutions, to ensure the market and operational integrity without impeding the development of e-finance.

Notes

1 For more detail see www.swift.com

2 In this section cards with magnetic strips are reviewed; cards with embedded software chips will be considered under the heading of smart cards in the next online payments section.

3 The first credit card was developed by the Bank of America and was initially known as Americard. Eventually it was transformed into Visa Cards

4 www.visa.com/av/thanksabillion.html

5 "Financial Times" June 13, 2000

6 IMF (2000).

7 BIS (2000a).

8 BIS (2000b).

9 The Banker, 1 February, 2001.

10 Jupiter Communications estimate: $23.1 billion, Activmedia Estimate: $109 billion.

11 The most popular certification authority used for e-commerce applications of this type is Verisign Inc, www.verisign.com

12 In January 2000, a Russian hacker fraudulently obtained a file of of credit card numbers from CD Universe. Initially he attempted to blackmail them for a sum of between $100,000 and $300,000 and when this failed, he published the file on an online site.

13 The Banker, ibid.

14 See www.orbiscom.com, www.americanexpress.com, www.cyota.com

15 BIS (2000b).

16 Mornan-Vaughan and Smith (2001).

17 www.MAOSCO.com

18 MasterCard International (2000).

19 See http://home3.americanexpress.com/corp/latestnews/compaq.asp

20 www.visa.com/av/news/press_release.ghtml?pr_form_edit=365&edit_file=

21 See www.visa.com

22 See www.ubs.com

23 Paydirect.yahoo.com – a division of the Yahoo! Internet portal company

24 www.Paypal.com

25 www.pocketpass.com

26 As reported in Marcella and Chan (1993).

27 Le magazine d'Internet.net, Nu:49, février 2001, p.74

28 See www.bolero.net

29 See www.tradecard.com

30 International Trade Today, November 2000

31 See www.itfex.com, www.ltptrade.net, www.cceweb.com

32 Cazes, Jérôme. "Avec la Solution @rating: L'Afrique sur la route du Commerce B2B". Presentation at the UNCTAD Conference on Building Credit Insurance in Africa and the Mediterranean, Tunis, 23-24 October 2000. See also www.coface.com

33 See www.dnb.com

34 http://investor.dnb.com/ireye/ir_site….dnb&script=460&layout=9&item_id0128344

35 See www.watch.org

36 WIPO (2000).

37 European Central Bank (1998).

38 Gramlich, Edward M. (1999).

39 Directive 2000/46/ELECTRONIC COMMERCE, also known as EMI Directive of the European Parliament and of the Council of Europe, 18 September 2000, on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0046.html

References and bibliography

Bank for International Settlements (2000 a). *Clearing and Settlement Arrangements for Retail Payments in Selected Countries*. Basel, Switzerland, September, 45pp.

Bank for International Settlements (2000 b). *Statistics on Payment Systems in the Group of Ten Countries*. Basel, February, www.bis.org/publ, 133pp.

Bank for International Settlements (1999). *Payment Systems in the Southern African Development Community*. Basel, Switzerland, June, 262pp.

Bank for International Settlements (2000 c). *Survey of Electronic Money Developments*. Basel, Switzerland, May, 104pp.

Bank for International Settlements (2000 d). Committee on the Global Financial System. *The Implications of Electronic Trading in Financial Markets*. Basel, Switzerland. November.

Basel Committee on Banking Supervision (2000). *Issues and Principles for Risk*

Management of Electronic Banking. Electronic Banking Group. November.

Bell, Richard (2000). *Internet Banking: The Bank's Perspective*. TowerGroup.

Needham, MA. July.

BIS (2000a). *A Glossary of Terms Used in Payments and Settlements Systems*. Basel, December 2000, p.14 (44pp).

BIS (2000b). *Survey of Electronic Money Developments*. Basel, May 2000.

Bolero, XML Team (2000). *A White Paper on Bolero XML standards*. 21 August. www.bolero.net/downloads/boleroXML_standards.pdf

CEPSCo (2000). *Common Electronic Purse Specifications – Business Requirement*s, Version 7.0. March. www.cepsco.com/

Claessens Stijn, Glaessner, Tom and Klingebiel, Daniela (2001). *E-Finance in Emerging Markets: Is Leapfrogging Possible?* World Bank Working Paper, forthcoming.

Crockett, Andrew (2001). *Financial Stability in the Light of increasing Importance of Online Banking and E-Commerce,* BIS Review, May

Europay International S.A., MasterCard International Incorporated, and Visa International Service Association (1996). *EMV '96: Integrated Circuit Card Specification for Payment Systems*. June. www.emvco.com/

European Banking Association (2000). *Straight Through Euro Payment System – Impact Document for STEP1 Banks*, Version 0.3. June. www.abe.org

European Central Bank (1998). *Report on Electronic Money*. August, 1998. www.ecb.int/pub/pdf/emoney.pdf

European Central Bank (2000). *Welcome to the World of TARGET*. August, www.ecb.int

Feghhi, J., Feghhi, J. and Williams, P. (1999). *Digital Certificates : Applied Internet Security*. Addison-Wesley, Reading, Massachusetts, 453 pp.

Financial Services Technology Consortium (1998). *Bank Internet Payment System Specification*, Version 1.0. August. www.fstc.org/projects/bips/index.html

Ford, W. and Baum, M. (2001). *Secure Electronic Commerce : Building the Infrastructure for Digital Signatures and Encryption*, 2nd Edition. Prentice-Hall, New Jersey, 612 pp.

Furst, Karen, Lang, William and Nolle, Daniel (2000). *Internet Banking: Developments and Prospects*. Office of the Comptroller of the Currency. Working Paper. September.

Gramlich, Edward M. (1999). Electronic Money in the United States. Remarks before the Electronic Payments Symposium, University of Michigan, Ann Arbor, Michigan, 17 September 1999.

Group of Ten (2001). *Consolidation in the Financial Sector: Summary Report*. January.

Humphrey, D., Dato, E., Tsurumi, M. and Vesala, J. (1996). *The Evolution of Payments in Europe, Japan and the United States : Lessons for Emerging Market Economies*. World Bank Policy Research Working Paper 1676, October. 44pp.

IMF (2000). *Modern Banking and OIC Derivatives Markets: The Transformation of Global Finance and its Implications for Systemic Risk*. Occasional Paper No: 203. Washington, 2000, p.9 (72pp).

Institute for Prospective Technological Studies (IPTS) (1999). *Study on Electronic Payment Systems for the Committee on Economic and Monetary Affairs and Industrial Policy of the European Parliament*. May, European Commission Joint Research Centre, Seville, Spain, 83pp, www.jrc.es/pages/projects/docs/Final-EPS-Vol.1.pdf

ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June, 50pp.

Jones, T. (1996). *The Future of Money as it Affects the Payment Systems in the U.S. and Abroad*. Submission to the U.S. House of Representatives, June.

Kravitz, J. (editor) (1999). *FSML – Financial Services Markup Language*, version 1.5. July.

Kountz, Edward (2000). *Wireless Technologies in Asian Financial Services: Business*

Trends and IT Spending. TowerGroup. Needham, MA. August.

Marcella, A.J. and Chan, S. (1993). *EDI Security, Control, and Audit*. Artech House, Norwood, MA., 212pp.

MasterCard International (2000). *Mastercard Delivers the Complete Chip Solution*. www.mastercard.com

Mondex (2001). How does it work? www.mondex.com

Mornan-Vaughan, S. and Smith, P. (2001). Digital money: have banks lost the plot? *"E-mmerce*", vol. 2, issue 2, February/March 2001, pp 27-29.

NACHA Cross-Border Council Global ACH Working Group (1999). *Concept Paper for a Global Automated Clearing House*, Version 1.4. May. www.globalach.org

National Automated Clearing House Association (2000). *ACH Statistics Sheet – 1989-2000*, www.nacha.org/news/Stats/stats.html

OECD (2001). *Emerging Market Economy Forum on Electronic Commerce*. www.oecd.org/dsti/sti/it/ec/act/dubai_ec/

O'Mahony, D., Peirce, M. and Tewari, H. (1997). *Electronic Payment Systems*. Artech House, Norwood, MA., 254pp.

Schneier, B. (1996). *Applied Cryptography*, 2nd Edition. Wiley, New York, 758 pp.

UNCTAD (2000). *Building Confidence: Electronic Commerce and Development*. United Nations Publication, Sales No. E.00.II.D.16, 175pp.

University of Texas (2000). *The Internet and the Future of Financial Markets*.

Visa International (1999). *Visa, Nokia and MeritaNordbanken Group to Pilot Mobile Payment*. Visa Press Release, May, www-s2.visa.com/pd/eu_shop/presscentre/press_articles

WAP Forum (1998). *The Wireless Application Protocol Architecture Specification*. April, www.wapforum.org

WIPO (2000). Primer on Electronic Commerce and Intellectual Property Issues. May 2000, http://ecommerce.wipo.int

World Bank (2000). *Electronic Finance: Reshaping the Financial Landscape Around the World*. Financial Sector Discussion Paper No. 4. September, 26pp.

Wrona, K., and G., Zavagli (1999). *Adaptation of the SET Protocol to Mobile Networks and to the Wireless Application Protocol*. Proceedings of European Wireless'99. Munich, Germany, Oct. 1999, pp. 193-198.

Chapter 8

E-LOGISTICS: DELIVERING THE GOODS IN E-COMMERCE

A. Introduction

Logistics has been defined as "that part of the supply chain process that plans, implements, and controls the efficient, effective flow and storage of goods, services, and related information from the point of origin to the point of consumption, in order to meet customers' requirements".[1]

It is a broad subject that covers the following functions: production scheduling, order processing, transportation, demand management, warehousing, packaging, information technology, supply chain management, customer services, inventory control, import and export processing, documentation and insurance, payments, customs processing, inspection, returns processing, and implementation of related government regulations such as product and labeling standards, health and environmental protection.

It is clear, therefore, that a comprehensive treatment of the subject would require space beyond the scope of this report. Consequently, this chapter focuses on key issues in logistics that currently affect trading activities, particularly as a result of the Internet and the growth of electronic commerce.[2]

Logistics involves the management of information for the control of interrelated functions in the supply chain. Physical processes are employed to move goods, and information is used by the decisionmaker to control and optimize the physical processes. The central role of logistics in trading activities has been widely recognized. Similarly, the role of trade facilitation as support for logistics functions and trade processing in general has received much attention. In this connection, various initiatives have been taken by a number of organizations, such as UNCTAD, the United Nations Economic Commission for Europe, the World Customs Organization (WCO) and the World Trade Organization (WTO). These are described in section F.

Against this background, this chapter examines the interrelationships between the growth of electronic commerce and the requirements for logistics services, and the role played by technology in enabling service providers to meet the additional demands for logistics services that are imposed by electronic commerce. It outlines the role of order fulfilment in e-commerce (e-fulfilment),[3] the different types of logistics services (e-logistics)[4] and institutions that are emerging to address the critical problems of e-fulfilment and the role of technology and trade facilitation in enhancing logistics functions. It also examines the development of e-logistics in developing countries.[5] The discussion suggests that logistics services could be greatly enhanced through improvements in trade facilitation.

B. The implications of e-commerce for order fulfilment and logistics

The order fulfilment and logistics requirements for handling e-commerce are much greater than those in traditional trade. Traditional trade is associated with fragmented supply chains. Information tends to flow between individual pairs of parties in the supply chain without end-to-end visibility across the chain from producer to consumer. By contrast, e-commerce has given rise to greater integration of information and transactions between participants in the supply chain, leading to the creation of distribution networks in which all the participants can share information.

Apart from differences in information flows, traditional trade is dominated by the movement of large shipments in bulk consignments, often delivered to central distribution points for further distribution to retail stores. The shipments are identified by container or box or pallet or other unit of measurement by which they can be tracked or traced. Also, the demand for shipments tends to be stable and concentrated around a few large buyers and is therefore fairly

predictable, and the order cycles tend to be relatively long.

In e-commerce, on the other hand, particularly in B2C trade, the number of buyers placing orders directly with producers or distributors tends to be much larger.[6] Consequently, the total volume of small shipments is much larger, and their origins and destinations are more widely dispersed, while their movements are more frequent and require direct delivery to the final consumer. Order cycles are relatively shorter and the demand for shipments is quite unpredictable and unstable because it arises from orders placed by larger numbers of buyers and a large number of sellers. This gives rise to increased scope for stock-outs and other factors that may cause sellers to fail to fulfil.

Returns tend to be higher in e-commerce than in traditional trade, requiring additional services to deal with them. The high incidence of returns arises from consumers receiving goods that are different from what they expected or ordered and is also due to the failure of the vendor to determine in advance the final landed price of the purchased goods. Online buyers tend to have higher expectations about their purchases. Given that goods can be searched and ordered quickly online, they expect that the information about the status of goods in the supply chain and their transportation and delivery can also be supplied quickly. Customer services thus tend to be responsive, flexible and individualized.

The main characteristics of logistics that are emerging or are expected to emerge as a result of e-commerce are summarized in box 13.

C. How e-fulfilment is handled

Companies that sell merchandise online use a variety of methods and channels to fulfil customers' orders. Three principal channels are used, namely the company handling the fulfilment itself, outsourcing the fulfilment function to third-party logistics service providers and use of drop-shipping.[7] Some companies use various combinations of these methods.

In-house fulfilment services have the advantage of giving the company full control of the fulfilment process and also over costs. They also enable a company to maintain direct relations with its customers and develop collaborative relations with them. However, in-house e-fulfilment involves considerable costs in terms of physical infrastructure and operations. Observers have suggested that where traditional brick-and-mortar companies have used their own distribution systems that had been designed to handle bulk

Box 13
Major characteristics of e-commerce that impose new requirements on logistics services

- Larger number of small parcels or packages due to a larger number of buyers making direct orders and a larger number of sellers than in traditional trade;
- Large numbers of on-line customers, mostly unknown to the sellers;
- Demand for shipments is much more unpredictable and unstable since it originates from more numerous customers;
- Origins and destinations of shipments are more widely dispersed, given that more buyers place direct orders with producers and distributors and more sellers access buyers globally;
- Accountability for shipments extends through the entire supply chain, compared with traditional logistics in which accountability is limited to single links of the supply chain;
- Customers have high expectations about quality of services and demand fast delivery of shipments;
- Higher incidence of cargoes returned to the supplier than in traditional trade;
- Greater demand for and availability of information covering transactions over entire supply chain, thus allowing on-line shipment tracking and other supply chain management functions;
- Greater focus on one-to-one marketing, which creates demand for customized delivery and post-transaction customer services;
- Greater complexity in fulfilling international orders than in traditional trade, thus preventing some retailers and service providers from being involved in international e-commerce;
- The emergence of demand for on-line processing of shipments, including cargo booking, bills of lading/airway bills, freight payment, rate quotation, landed price calculations and tariff management;
- Substantial increase in the volume of small shipments, leading to growth of demand for warehousing, transport and other logistics infrastructure that can handle larger volumes of small shipments;
- Greater scope for customer self-service.

orders, these have proved to be unsuitable for handling small shipments in e-commerce. For example, where a company originally shipped a product only by truckloads to distributors, migration to e-commerce would mean receiving orders from single consumers as well and thus entail the need to create packaging and delivery systems for less-than-truckload shipments. The problem relates not only to a mismatch of physical facilities but also to information transfer. In many cases, orders initiated online have had to be fulfilled using data fed manually into the supply chain and logistics systems, and this has caused considerable inefficiencies and delays.

The second method of e-fulfilment is to outsource the services to third-party logistics service providers. As will be shown later, many companies have established capability to provide logistics services to other companies. Outsourcing is considered to be particularly advantageous for pure-play dot.com companies and start-up companies that do not have experience, capital or the necessary physical infrastructure. It is also a useful method for well-established companies that wish to concentrate on their core businesses.

The third method - drop-shipping - is a fulfilment method whereby the retailer advertises products and, having received orders from customers, places orders for the same products with companies that undertake drop-shipping services. These may be manufacturers or distributors. The retailer tells the drop-shipper where to deliver the goods. He receives payment from the customer and his profit is the difference between what the customer pays for the goods and what the retailer pays to the drop-shipper as his part of the payment. The main advantage of this method for the retailer is that he does not need to make investments in merchandise inventory. Also, it protects the retailer from losses that may arise from goods that cannot be sold. Warehousing, packing and other shipping costs are also met by the drop-shipper. In addition, the method also allows a retailer to deal in a wide variety of goods since no inventory is involved. The retailer may arrange with the drop-shipper to place the retailer's logo on the packing list so that the customer knows where the product was purchased and repeat orders are thus ensured for the retailer.

Drop-shipping may present problems, however, with regard to returned merchandise, especially if a customer orders products that are drop-shipped from several sources, in which case the retailer becomes involved in handling returns and thus in activities in which, according to the method, he should not become involved. Another risk may arise from the fact that not all drop-shippers that fulfil the orders are equipped to deal with retail customer services. Moreover, the system may be unattractive to a customer who orders several products that are eventually shipped to him or her in multiple packages from different drop-shippers at different times. Not only the customer would incur high shipping costs because of the multiplicity of packages, but also the effort to track the shipments would also be greater than if the goods were to be shipped from the same source.

Some retailers employ other strategies, in addition to the three main methods outlined above. For example, some handle some logistics functions themselves but establish partnerships with service providers to deliver other services. For instance, the company could handle warehousing and inventory but make an arrangement with a transportation service provider with which it establishes an alliance to handle transportation, distribution or delivery.

Table 26
Main methods used by e-retailing companies to fulfil orders
(percentages)

Method of fulfillment	Pure-play e-tailers	Multi-channel e-tailers
From company facility	44.5	71.8
Drop-shipped from manufacturers or distributors	30.6	5.1
Outsourced to dedicated fulfillment sources	8.3	17.9
From facility operated by alliance or joint venture partner	8.3	2.6
Electronic fulfillment (e.g. software, information)	5.6	0.0
Other	2.7	2.6

Source: PricewaterhouseCoopers (2001).

Table 27
Methods used by e-retailing companies to handle different kinds of logistics functions
(percentages)

	Inventory warehousing	Picking/ packing	Shipping	Returns	Replenishment
Pure-play e-tailers					
Company handles	47.2	41.6	36.1	63.9	52.8
Outsourced to third party	41.7	44.4	47.2	22.2	25.0
Combination of company and third-party	8.4	11.2	13.9	13.7	16.7
Other methods	2.7	2.8	2.8	0.0	5.5
Multi-channel e-tailers					
Company handles	71.8	69.2	66.7	79.5	76.9
Outsourced to third party	20.5	20.5	23.1	12.8	12.8
Combination of company and third-party	5.1	7.7	7.7	5.2	7.7
Other methods	2.6	2.6	2.5	2.5	2.6

Source: PricewaterhouseCoopers (2001).

Surveys show that there are important differences between various types of online retailers regarding the extent to which they employ the different methods of order fulfilment.[8] They show, for example, that Internet-only or pure-play e-retailers tend to fulfil a large portion of their orders through outsourcing to third-party logistics providers and using drop-shipping. On the other hand, e-tailers that use multiple channels such as physical stores, catalogues and online (multi-channel e-tailers) tend to fulfil a large part of their orders using their own facilities. Table 26 illustrates the main approaches that e-tailers use to fulfil online orders. Table 27 gives a breakdown of logistics services and how different types of e-tailers handle them. These figures show a significant variation in order fulfilment models. In the final analysis, the choice of a model is a strategic decision that an enterprise has to make on the basis of consideration of cost and customer requirements.

D. Capabilities of software applications that support e-logistics

In section B, it was shown that e-commerce gives rise to new features in logistics and transport services that are more demanding than those imposed in traditional trade. These include the need to transact with a large number of disparate customers, the emergence of new business models and practices, an increased demand for higher service levels and a growing demand for collaboration between users and service providers along the supply chain. A major implication of these features is that traditional methods of handling information such as manual methods using e-mails, faxes and the telephone are not sufficient to meet the additional demands. It has therefore become imperative for companies to develop and apply more advanced web-based and other technologies that can automate transactions and also allow the exchange of data and information between different system applications.

Against this background, there has been an upsurge in the development of computer software applications capable of supporting a variety of logistics and transport services over the Internet.[9] These not only reduce the volume of paperwork, but also improve the overall productivity of logistics services and create considerable opportunities for firms to optimize functions over the supply chain. The importance of software applications for e-logistics is demonstrated by the considerable increases in sales of such software. It is estimated that in 2000 worldwide sales of software, hardware and services used in electronic logistics reached $277 billion, and they are expected to reach $1 trillion by 2005. In the United States alone e-logistics software sales are expected to increase from $8 billion in 2001 to $45 in 2004.[10] While these figures appear to be on the high side, they nevertheless provide a useful indication of the importance being attached to the issue of logistics in e-commerce.

This section briefly describes selected applications developed for various types of logistics functions[11].

1. Online order management

Order management applications enable users to perform online order entry, and provide real-time information on all customers and on products ordered in order to enable the seller to set priorities for order fulfilment. Some applications allow customers to specify their needs and requirements in order to allow for the delivery of customized products. The system interactively offers products that match the customer's requirements, and allows him or her to choose on a self-service basis. Some applications automate the allocation to buyers of products that are in short supply according to set criteria. Others make it possible for customers and suppliers to obtain visibility into the status of orders. This enables sellers to commit delivery dates and customers to know when to expect deliveries. Some applications are designed to enable order fulfilment in B2B, many-to-many transactions. They enable order capture from many sources and execute multiple source orders.

2. Shipment tracking

Users can track individual shipments or parcels while they are in transit, and the status of shipments is monitored as it changes at different points along the transport chain. Some applications monitor shipments and can alert the shipper if the shipment is moving behind schedule. Tracking capability requires the seller or shipper to link its website to the carrier's application systems. It enables all parties in the supply chain to share information and to better plan inventory, sales or production. Shipment tracking applications can also be used by a shipper to re-route shipments.

3. Equipment and vessels tracking

The movement and locations of transport equipment such as containers and vessels, trucks and cargo-carrying aircraft can be tracked and fed into shipment tracking. It also enables terminal, port and other facility operators to plan their operations based on real-time information about the location of the vessels, equipment, and so forth.

4. Transportation management and planning

Users can carry out transportation transactions on the Internet, such as freight rate management, freight bill payment and carrier selection. Carriers can optimize route determination and adjust transportation schedules on the basis of incoming orders. Some provide automatic assignment of manifests as shipments are being processed. Manifests are automatically printed on paper and users can transmit them automatically to carriers' billing systems. Others enable shippers to select carriers automatically on the basis of freight cost, transit times and other best-carrier criteria that are specified by the shipper. On the basis of the attributes of a shipment, some applications compute total freight cost, including discounts, additions and surcharges, assign a bill of lading number and remember to assign the same bill of lading number to shipments to be consolidated for delivery to the same consignee.

5. Landed cost calculation applications

These applications are mainly designed for international e-commerce transactions. They permit automatic calculation of the landed cost of a product when received by the consignee. The calculation takes into account information on trade regulations, customs tariffs, government taxes, insurance and transportation costs. To support the calculations, some applications also incorporate large databases on such information as most-favored-nation (MFN) tariffs and tariffs negotiated under bilateral or multilateral trade agreements and preferential agreements such as the Generalized System of Preferences (GSP). Some applications allow shippers to describe their products in plain language, and the software automatically matches the description to Harmonized System Tariff Schedule (HS) codes. Others enable exporters and importers to compare different landed prices automatically for different Incoterms, for example costs, insurance and freight (CIF) and free on board (FOB).

6. Online customer service management

Customer service (or customer relationship management) systems provide capabilities for communication and interaction between sellers, service providers and customers. Customers can access interactively customer service specialists directly and request help online. Responses can be given at virtual help desks. Sellers can contact customers to ask them if they need help. Vendors and service providers can post answers to frequently asked questions (FAQs) and thus provide a form of self-service to customers. Online discussion groups or chat rooms provide useful information to sellers and buyers. Some applications maintain the history of sold items by tracking the serial numbers of the items, contracts and warranty

details, and records of after-sales services and agreements.

7. Collaborative logistics management systems

These allow supply chain participants to collaborate in various ways, for example to plan jointly their transport requirements and plans, and to share information on transport capacity availability and thus optimize their vessel scheduling. Participants can also tender for transport or other services. They can also offer customers, producers and suppliers complete visibility into demand data and fulfilment schedules. If exceptions occur that cannot be executed, the trading partners are notified automatically to allow them to quickly resolve the situation.

8. Customs clearance

Customs clearance and compliance applications permit online preparation of import/export documents and provide direct connection to customs services. They also generate automatically customs documents and distribute them to suppliers, buyers, shippers, carriers, freight forwarders and customs brokers. In addition, import data can be filed electronically in advance of the arrival of shipments, thus saving money by reducing the time that goods are held in Customs. Some applications can verify automatically whether imports and exports comply with different countries' trade laws, regulations and procedures, including embargo, boycotts and restricted products.

9. Returns management

A consumer wanting to return a product visits the customer service section of the retailer from whom the purchase was made. The customer selects options for returned products. The program guides the customer through a series of prompts and questions such as the reasons for wanting to return the product. The program may offer some troubleshooting tips if the product is being returned because it is defective. If the customer's decision to return the product is final, he or she is prompted to print a mailing label to effect the return.

10. Integrated all-in-one supply chain management

As opposed to stand-alone solutions designed for single functions, integrated applications attempt to handle multiple supply chain functions starting from the moment an order is placed until delivery to the final customer. A number of logistics companies, in partnership with technology companies, have attempted to develop such applications, although it would appear that integrated systems are not widespread.

11. Summary observations

A large number of software applications are being developed to handle different types of logistics functions. Some of them focus on one or a few functions. Some are designed for B2B transactions, while others are designed for B2C transactions or both. The tendency for software companies to develop differentiated systems, customized for different markets or users, may cause incompatibility between applications.

There is widespread agreement that the integration of software applications systems is essential in order to enable companies to optimize their supply chain functions. For example, automating warehousing and transportation or distribution systems using different systems that cannot exchange data may not bring about much improvement in inventory control. A study by Cap Gemini Ernst & Young found that 80 per cent of users of logistics services indicated that the integration of transportation and distribution systems was important for their overall business strategy[12].

Because of the critical need for the efficient transfer of instructions between different logistics systems, various types of solutions have been sought. The development of XML (Extensible Mark-up Language) is an example of possible solutions to the problem. XML creates formatted messages with metatags that describe the data being transmitted. The receiving system is therefore able to understand how to handle the message. Some logistics service providers have pioneered the creation of XML-based products that can support the integration of supply chain systems[13].

E. E-logistics service providers and outsourcing

There are two broad categories of logistics service providers, namely in-house providers and third-party logistics service providers (3PLs). An in-house logis-

tics provider is a division or department within a company, usually asset-based, that provides such functions as transport, forwarding, warehousing, information technology or other types of logistics functions. A 3PL is an independent, stand-alone entity that is not part of a parent company for which it is supplying logistics functions. Its customers are outside the firm.

A 3PL can be asset-based, in that it owns a fleet of vessels or warehouses, or it can be non-asset-based. Asset-based 3PLs include major integrators such as DHL, FederalExpress and UPS, which play the role of carriers, forwarders and distributors. A distinct category of 3PLs is fulfilment houses and drop-shippers. The latter were described in section B. A fulfilment house stores the e-merchants' merchandise and takes responsibility for getting it to customers. The merchandise and the business are owned by the e-retailer while the fulfilment house provides warehousing, packing, shipping and delivery services. In certain cases its functions may extend to covering credit card processing, packing and order tracking. Fulfilment houses differ from integrators in that in the former case the merchant need not maintain in-house inventory while in the latter case the merchant would require to maintain inventory and carry out online fulfilment processes himself.

In recent years many companies have tended to use the services of more than one 3PL and it has become necessary to nominate a logistics service provider to coordinate the services of the other 3PLs, giving rise to the concept of fourth-party logistics service provider (4PL), also referred to as a lead logistics provider (LLP). A 4PL may also arise where a service provider supplies several services to a company and subcontracts some of them to other 3PLs.

Another group of logistics service providers that can be distinguished from the others are logistics or transport exchanges. These are B2B online market places or trading communities that facilitate trade in freight transportation services between buyers and sellers of such services. Members include shippers (manufacturers, distributors, retailers, 3PLs, freight forwarders and brokers) on the one hand, and carriers or transportation companies on the other. They have evolved from original carrier-shipper matching services into online communities for supply chain collaboration. They also include exchanges established by shippers in partnerships with other companies that function as their logistics service providers. These exchanges undertake such online functions as matching offers of carriers with requirements of shippers through auctions and automatic exchanges, providing price information, freight scheduling and tracking, managing contracts and freight payments, customs compliance and producing user-defined reports.

Another category of 3PLs is providers of logistics management applications. These companies do not provide direct logistics services, but they provide systems that support such functions as described in section D. In certain cases they operate in partnerships with other 3PLs such as integrators or carriers and in other cases they function as application service providers (ASPs). They may do so by hosting web-based logistics/transportation exchanges or providing solutions to buyers and sellers of logistics/transportation services for their in-house logistics management.

1. Outsourcing of 3PLs

Outsourcing of logistics services was mentioned briefly in section C. It is one of the critical issues in current discussion of e-logistics services. Logistics services are witnessing a considerable expansion of 3PLs, primarily because companies, including e-merchants, prefer to outsource logistics functions. It is predicted that in the United States outsourcing of e-logistics will increase from $12 billion in 2000 to over $71 billion in 2004[14].

The remarkable growth of logistics outsourcing has been attributed to a number of factors[15]. Many companies have installed various types of applications to optimize their in-house logistics functions, and these applications are tending to become increasingly sophisticated and complex. Some companies are unable to cope with the changes and have responded by outsourcing the provision of the applications to specialized technology companies. In other cases, companies have simply not yet installed any logistics applications and outsourcing has been a convenient short cut.

A second factor is companies' desire to concentrate their resources and competencies on their core businesses. A third factor is the avoidance of sunk costs and risks, since outsourcing eliminates the need to incur costs on training logistics staff and acquiring warehouses, equipment and hardware. Fourth, for a start-up company or a company that is expanding quickly, outsourcing allows it to expand the volume

of its business quickly with minimum investments, simply by relying on third-party facilities and services. Fifth, by providing services to several firms, 3PLs are in a position to develop large databases and other information that an outsourcing firm can access at lower cost than if it were to collect the same data itself.

Despite the promising benefits of outsourcing, companies still need to carry out a proper assessment of the scope and timing of outsourcing as well as the choice of 3PLs to which outsource. A company must compare the costs and advantages of providing logistics functions in-house with those of outsourcing.

F. E-logistics, e-fulfilment and trade facilitation

Section D outlined the capabilities of software applications in supporting e-logistics functions and e-fulfilment. In addition to the role played by technology, it is widely recognized that trade facilitation has a critical influence on the ability of traders to fulfil orders or deliver goods in e-commerce, especially in international transactions.[16] Furthermore, it could be suggested that even when suitable applications are employed to automate such functions as order management, warehousing, inventory and transport management, most of the benefits could fail to materialize if trade facilitation is inefficient.

Trade facilitation has been defined as the simplification and harmonization of international trade procedures that include activities, practices and formalities related to the collection, presentation, communication and processing of data required for the movement of goods in international trade.[17] It includes such functions as export and import formalities, customs clearance, payments and insurance. There has been widespread concern that in many countries trade facilitation is characterized by a host of inefficiencies that cause delays and high costs. It has been estimated, for example, that the global average of the cost of complying with procedures in international trade amounts to 7 to 10 per cent of the overall value of international trade.[18] Other estimates indicate that potential savings from more efficient information processing in international trade documentation in 1997 would have been of the order of $100 billion, or 30 per cent of the total overhead costs of international trade.[19]

The main problem areas include the following:[20]

1. The existence of a considerable number of documentation requirements, which include government documents, commercial documents and those relating to transportation. A particular international transaction may involve as many as 60 documents,[21] and most of the information they contain is the same. In addition, there is a lack of harmonization of documentation systems between countries and also between the private sector and government. All this contributes to high costs and to delays in processing trade and logistics functions.
2. Variations in the customs valuation of exports and imports, with customs valuation in many countries characterized by such problems as double invoicing and undervaluation, which make of the true value difficult.
3. Although the Harmonized System (HS) has made a considerable contribution in the classification and coding of commodities, some observers are of the opinion that the six-digit codes used in the HS are too broad and that new codes should be introduced gradually in order to provide more trade information. In this regard, the national tariffs of many countries are specified in greater detail beyond the six digits, which means that there is no harmony between the HS classification and the additional levels used in the individual countries.
4. Lack of harmonization of customs procedures and the existence of outdated trade procedures such as exchange controls, long retention of goods in customs custody and regulations that require paper documents.
5. Lack of transparency in many regulations, leading to an inability to predict costs and delivery times.
6. The existence of multiple transport liability regimes, including the Hague Rules, the Hague-Visby Rules, the Hamburg Rules and the United States Carriage of Goods by Sea Act (COGSA), leading to confusion as to which rules to apply in which trade.
7. Customs administrations that are poorly equipped as regards physical infrastructure and human resources, and also lack of cooperation between customs administrations of different countries. Many customs administrations are also prone to

corruption, which leads to delays, high costs and a distortion in trade information.

8. Limited use of automation and information technology in trade facilitation functions, leading to delays, high costs and inefficiencies.

There have been many initiatives and proposals aimed at improving trade facilitation. The following are a few illustrative examples.[22] At the international level, the World Symposium on Trade Efficiency, held in 1994, provided an impetus for efforts to improve trade processing. Linked to the Symposium, the UNCTAD trade efficiency initiative is an example of a programme aimed at addressing problems of logistics in a wider context by promoting the application of information and communication technologies (ICTs) to trade. This is a broad-based initiative focused on simplifying and harmonizing trade procedures worldwide by allowing traders, especially small and medium-sized enterprises (SMEs), access to advanced ICTs.[23] A practical application of this initiative is the ASYCUDA programme, which is widely used by developing countries. This is a computerized customs management system that handles various trade procedures such as manifests, customs declarations and accounting, and utilizes international codes developed by the WCO and the United Nations.[24]

Another development is the revision of the Kyoto Convention, now known as the International Convention on the Simplification and Harmonization of Customs Procedures (as amended), which has been agreed by the WCO. It will come into force when it has been ratified by 40 WCO members.[25] It is expected that the adoption and implementation of the revised Convention by a large number of countries will go a long way to minimizing existing trade facilitation obstacles.

The WTO has included trade facilitation on its agenda. The key issues concerned were articulated at the Trade Facilitation Symposium organized by the WTO in 1998. The symposium covered a wide range of issues, including documentation requirements, official procedures, automation and use of information technology, transparency, predictability and consistency, and modernization of border-crossing administration. A number of areas related to trade facilitation are covered by WTO agreements and the symposium proposed improvements in certain of the rules as well as the incorporation of additional rules on trade facilitation.

As a follow-up to the UNCTAD trade efficiency initiative, the G7 have adopted the G7 Initiative, which is a scheme intended to use export declaration data to process import consignments. It is based on the premise that export declaration data could be used to clear consignments for imports. This would facilitate the movement of goods across borders and would be a step towards the ideal of seamless international trade transactions in which trade participants would supply their information only once and export data and information would equal imports. This ideal could only be realized, however, if all government customs requirements could be simplified and harmonized and the transmission of trade information based on internationally agreed standards.[26] The G7 Initiative is to be applied in international trade transactions between the G7 countries.

A project closely linked to the G7 Initiative is the International Trade Prototype (ITP) project developed jointly by the United Kingdom and the United States customs administrations. The development of the ITP was based on several goals and principles, including the automation and exchange of standardized information that would be agreed by the two countries. Furthermore, it attempted to streamline government reporting requirements in trade transactions and to develop harmonized and simplified messages and procedures that reduce the need for redundant entry or transmission of data. A key element of the ITP is similar to the G7 Initiative, namely developing a process in which data provided for export declaration to the export customs administration are forwarded to the import customs administration and used to process import entry and clearance in the country of destination. The ITP project and the G7 Initiative were merged in 2000.

G. E-logistics in developing countries

The growth of e-logistics is highly correlated with the growth of e-commerce. Consequently, e-logistics and e-fulfilment activities have developed to a much greater degree in developed countries than in developing ones. There is nevertheless scope for the development and growth of these activities in developing countries as well. This section outlines areas in which such countries can exploit available or potential opportunities. These include access to global e-logistics services, participation in Internet-based transportation/logistics exchanges and applying available

technologies to B2B transactions in various transportation/logistics services in the developing countries themselves.

1. Access to global e-logistics services

In section II it was pointed out that in e-commerce there is a large volume of small shipments and the deliveries are global. The transportation and distribution of such shipments, both for B2C and B2B transactions, tend to be dominated by global express delivery companies such as DHL, Federal Express and UPS. These companies provide services on a global scale, covering practically all parts of the world, including developing countries. Consequently, shippers are able to use such companies to send shipments to any destination with the frequency and speed that buyers require. A number of service providers offer merchants free online downloads of software from their websites in order to allow them to benefit from tracking, tracing and other logistics functionality and also to integrate their back-end systems with those of the logistics service provider. Also, some developing countries have established firms that provide e-logistics services that shippers can use.

A number of developing country e-commerce sellers are making use of the services of the global logistics service providers to sell in global markets.[27] However, the main constraint relating to these services is the high shipping costs charged. Sellers are able to rely on such service providers if they deal in high-value merchandise.

2. Participation in Internet-based logistics and transportation exchanges

As outlined in section V, logistics/transportation exchanges provide a forum in which service providers and users can conduct transactions.[28] Being Internet-based, in principle any service provider or user should be able to browse the net in order to offer or buy a service and fulfil online the required contractual transactions. The extent to which service providers and users make use of these exchanges, even in the developed countries, has not been well documented. Furthermore, except for the charter of whole vessels, the offers and bids made on the exchanges are in relation to specific trade routes, which may not cover many developing countries. Therefore, overall, the true potential of the exchanges for developing countries has yet to be established.

3. Application of logistics technologies in B2B transactions in the developing countries

Section IV described a variety of technology applications that are being developed or used in providing e-logistics services. Such technologies are made accessible to users in different ways, such as outright purchase from technology developers or vendors, commercial partnerships between technology companies and users, application service providers hosting and servicing the users' websites, or through 3PLs.

Information about the costs of developing or purchasing various types of e-logistics software and applications is not readily available. It suffices to note, however, the growing tendency, even in the developed countries, for logistics companies to rely on 3PLs and partnerships with technology companies as an indication of the high cost and skills requirements involved in the purchase and maintenance of the applications. Outright purchase or in-house ownership would therefore not appear to be a feasible option for logistics companies in developing countries except perhaps for basic applications.

The second option, namely commercial partnerships between logistics service providers and technology companies, is likely to succeed where the user of the application generates sufficient revenues to compensate for the costs incurred by the technology company. A similar condition would apply in the case of an ASP or 3PL arrangement. In principle, any service provider in a developing country that has the requisite volume of services should be in a position to attract partnership with a technology company or be able to engage the services of 3PLs.

Access to technology, however, need not be through direct business affiliation between logistics service providers and technology companies. Instead, a logistics service provider in a developing country could establish a partnership with a service provider in a developed country that already possesses or has access to the required technology. For example, a number of developing country airlines have established alliances with major airlines of developed countries and through such alliances they benefit from a wide range of the latest technologies in the industry.

In addition to accessing technology through commercial partnerships, developing countries may benefit from technical cooperation programmes with

multilateral organizations or bilateral donors. Examples of such programmes include the Advance Cargo Information System (ACIS) and the Automated System for Customs Data (ASYCUDA), both of which incorporate elements of e-logistics systems. ACIS is a logistics information system that provides capability to track cargo and equipment of various transportation modes such as rail, road and lake and at interfaces such as ports and inland clearance depots. It is administered by UNCTAD and is being implemented in a number of developing countries.[29] ASYCUDA, on the other hand, is a programme designed to modernize customs, including the automation of customs processes and procedures. It uses information technology to accelerate customs clearance by simplifying documentation. This programme is also administered by UNCTAD and the system has been introduced into a large number of countries.[30] It is an open system that links to traders and carriers, allowing them to perform their customs operations directly.

H. Conclusions and recommendations

Logistics is a broad subject encompassing many activities, and this chapter has dealt with only certain key logistics issues of the day. Electronic commerce is imposing additional requirements on logistics services, but the growth of e-logistics has lagged behind the rapid growth of e-commerce. Logistics service providers have attempted to accommodate the increasing demands by trying to adapt their existing systems and by using 3PLs.

E-logistics services are being provided by in-house departments and 3PLs. There has been a remarkable growth of 3PLs as companies have tried to outsource many of their e-logistics services. While outsourcing is based on a number of sound economic reasons, companies still need to make a proper evaluation of its feasibility for their particular case.

Technology and software applications play a central role in supporting e-logistics services in handling the complex and demanding business models that are emerging. Logistics and transport service providers, supported by technology companies, are making concerted efforts to automate logistics functions in order to cope with the ever-increasing demands of e-commerce.

The development of differing applications to meet the requirements of specific users and functions is a source of incompatibility between applications, even within the same company. There is a critical demand for the integration of systems to ensure that instructions can be efficiently exchanged between different types of logistics applications.

Another impediment to efficient e-logistics is poor trade facilitation. Costly and slow movements of goods in international trade transactions are caused by excessive and unnecessary documentation requirements and official procedures, the lack of adequate automation and of use of information technology, the lack of transparency and predictability in trade processing, and the existence of inefficient and uncoordinated cross-border administration services, especially customs. A large number of international and regional organizations as well as commercial institutions are implementing a variety of measures to improve trade facilitation.

To achieve more efficient e-logistics and e-fulfilment, it is desirable to have a trading environment in which there is perfect information about goods as regards their description, origins and destinations, and costs for different origins and destinations. Sellers and buyers should be able to monitor and track goods at every point along the way from the supplier to the consumer. All stakeholders should be able to check on the Internet the availability and status of orders. All this can be achieved if trade information is simplified, automated and fully harmonized in all countries, and all restrictive government export/import regulations and practices are eliminated. It also requires sophisticated supply chain management systems for compiling and enabling global end-to-end monitoring of trade information.

To achieve these broad objectives and also to take into account the special problems of developing countries, it is recommended that Governments, the international community and the private sector cooperate in promoting the following specific measures:

1. Taking advantage of the great potential provided by Internet technology in order to capture, transfer and monitor trade information over global networks of supply chains in an open fashion;
2. Automating customs declaration systems in order to develop customs-to-customs information exchange and thereby provide a basis for the

elimination of unnecessary export/import requirements, which can instead be replaced by fully integrated international transactions;

3. Harmonizing and improving the classification of commodity tariffs, and facilitating the identification of individual consignments;

4. Providing investment resources especially for customs administrations in order to upgrade their efficiency;

5. Harmonizing and simplifying trade facilitation regulations and procedures, and in particular encouraging greater harmonization of customs procedures through the wide adoption and implementation of the revised Kyoto Convention on the Simplification and Harmonization of Customs Procedures;

6. Promoting cooperation between authorities of exporting and importing countries in order to provide verification and compatibility in trade information. In this context, the International Trade Prototype (ITP) project developed by the United Kingdom and the United States customs administrations could provide a model to be developed at the international level. The international community should give support to further development of the project;

7. Encouraging greater transparency in trade processing activities and taking measures to reduce corruption and other forms of malpractice in customs administration;

8. Promoting partnerships between developing country logistics service providers and developed country logistics service providers that are applying e-logistics systems;

9. Providing technical cooperation programmes to developing countries for the promotion of services that support e-logistics, for example in customs, transportation services, cargo terminals and related services.

Notes

1 Definition adopted by the Council of Logistics Management, http://www.clm.org/mission/logistics.asp.

2 Other dimensions of logistics may be covered in future issues of this report.

3 E-fulfilment can broadly be defined as everything that takes place, in electronic commerce transactions, from the time an order is taken to the time the product is received by the customer.

4 E-logistics is the application of logistics processes to the fulfilment of electronic commerce transactions. It applied to business-to-business (B2B) e-commerce as well as business-to-consumer (B2C) e-commerce. E-logistics differs from conventional or tradtional logistics in that it attempts to satisfy the expectations and requirements of merchants and customers engaged in e-commerce as outlined in table 26. Also, in e-logistics there is more collaboration and sharing of data and information across the supply chain between providers and users of logistics services.

5 Some of the elements discussed in this chapter were reflected in UNCTAD (2000).

6 In B2B e-commerce, while the buyers may be large, some shipments may be small packages. The majority of shipments, however, tend to be larger, palletized, less-than-truckload shipments.

7 For an extended discussion of alternative methods of e-fulfilment, see, for example, PricewaterhouseCoopers (2001).

8 See PricewaterhouseCoopers (2001).

9 It is worth noting that the demand for automated logistics applications existed even in traditional trade. However, e-commerce has undoubtedly spurred the development of new and more powerful applications.

10 See Coleman (2001).

11 For an extended description of the various applications outlined here, see, for example, Bayles (2001), Buxbaum (2001),Tariffc.com, Xporta.com, mycustoms.com, borderfree.com, ClearCross.com, Nextlinc.com, From2.com, Vastera.com, UPS.com, DHL.com, AirborneExpress.com, FederalExpress.com,EmeryWorld.com, Yantra.com and Optum.com.

12 See Cap Gemini Ernst & Young (2000).

13 For a discussion of XML, see UNCTAD (2000) and Bayles (2001).

14 See Buxbaum (2001).

15 For an extended discussion, see Amami and Marelli (1996).

16 While e-commerce relates to both domestic and international transactions, the main issues of trade facilitation concern cross-border trade.

17 See World Trade Organization (2000).

18 See United Kingdom Department of Trade and Industry (2000).

19 Crowhurst (2000)

20 For an extensive discussion of the problems of trade facilitation, see World Trade Organization (1998a, 1998b)

21 See World Trade Organization (1998b).

22 For a description of trade facilitation activities undertaken by various organizations, see World Trade Organization (1997, 1998c) and SITPRO (1998/9).

23 See Columbus Ministerial Declaration on Trade Efficiency (1994).

24 See World Trade Organization (1997, 1998c).

25 See International Convention on the Simplification and Harmonization of Customs Procedures (as amended), http://www.wcoomd.org/ie/Eng/Conventions/Conventions.html.

26 See United States Department of the Treasury (1999).

27 Some of the case studies of e-commerce in LDCs presented in chapter x of this report provide examples of such sellers.

28 The buying and selling of transportation/logistics services is to be distinguished from online buying and selling of goods that are shipped and delivered using the transportation/logistics services.

29 See ACIS, wysiwyg://21/http://www.untad.org/en/techcop/tra0105.htm.

30 See ASYCUDA, http://www.asycuda.org/aboutas.htm.

References and bibliography

Amami, M. and Marelli, M. (1996). *Business Logistics Outsourcing and Inter-organizational Electronic Networks*.

Armstrong and Associates, Inc. (2000). *Who's Who in Logistics: Guide to 3PLs and Global Logistics Services*, ninth edition, Stoughton, WI, U.S.A. Armstrong and Associates, Inc.

Bayles, D. (2001). *E-commerce Logistics and Fulfilment: Delivering the Goods*, Upper Saddle River, NJ, U.S.A.,Prentice Hall PRT.

Buxbaum, P. (2001*) Digital Logistics: Value Creation in the Freight Transport Industry*, First Conferences Ltd., Eyefortransport, www.eyefortransport.com/lasvegas2000/.

Cap Gemini Ernst & Young (2000). *Third Party Logistics Services: Views from the Customers, University of Tennesee, United States.*

Coke, J. (2000). "Who does the best job of e-fulfilment", *Logistics Online, Logistics Management and Distribution Report*, 11 January, www.manufacturing.net/magazine/logistic/archives/2000/1…/1m1100efulfilment.ht.

Coleman, M. (2001). "Software gets its hands dirty", *Investors' Business Daily*, 5 January.

Columbus Ministerial Declaration on Trade Efficiency (1994), http://sunsite.wits.ac.za/untpdc/tei/columbus.html.

Crowhurst, R. (2000). "Trade facilitation: Reducing the economic frictions that get in the way of trading across borders", SITPRONews, July.

Damas, P. (2001). "Building e-logistics networks", *American Shipper*, April, pp. 15-20.

Kapsinow, S. (1999). "Using fulfilment services for e-commerce", *Ecommerce Guide*, 15 April, http://www.internet.com.

McCullough, S. et al. (1999). *Mastering Logistics*, Cambridge, MA. U.S.A. Forrester Research, Inc.

Poirier, C. (1999). *Advanced Supply Chain Management: How to Build a Sustained Competitive Advantage,* San Francisco, Berret-Koehler Publishers, Inc.

PricewaterhouseCoopers (2001). *E*-fulfilment*: A long last mile*, Columbus, OH, U.S.A., January.

Shelton, B. (1999). "Building customer loyalty on the web", *Ecomworld*, 1 March.

SITPRO (1998/9). *SITPRO Annual Report 1998/9, The Trade Facilitation Year*, http://www.sitpro.org.uk/annual/ar1998-9/pg6a.html.

United Kingdom Department of Trade and Industry (2000*). World Trade and International Trade Rules*, http://www.dti.gov.uk/worldtrade/facilitation.htm.

UNCTAD (2000) Building Confidence: Electronic Commerce and Development. United Nations Publication, Sales No. E.00II.D.16.

United States Department of the Treasury (1999). *U.S. Customs Service, Announcement of a General Test Regarding the International Trade Prototype*, http://www.customs.ustraes.gov/news/fed-reg/notices/fr071999.htm.

World Trade Organization (1997). *WTO Council for Trade in Goods, Trade Facilitation: Background Note by the Secretariat*, C/CW/80, 2 June.

World Trade Organization (1998a). *WTO Trade Facilitation Symposium: Report by the Secretariat*, March.

World Trade Organization (1998b). *Checklist of issues raised during the WTO Trade Facilitation Symposium*, G/C/W/113, 20 April.

World Trade Organization (1998c). *WTO Council for Trade in Goods, Trade Facilitation: Update of Background Note G/C/W/80,* Addendum, 2 December.

World Trade Organization (2000)