INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

COMMERCIAL TRANSACTIONS

ON

THE INTERNET

by

Anne-Hortense Joulie

Institute of Comparative law
McGill University, Montreal
Quebec, Canada

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements of the degree of Master of laws (LL.M)

September 1996

To my parents

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere thanks to my supervisor, Professor David Johnston, for his guidance and support.

I also would like to thank Graciella Barrasso and Pierre Delastre for having patiently and diligently proof-read this thesis.

Thanks are also due to John Kirkpartrick for his precious help to obtain for me the documentation for this thesis.

ABSTRACT

This study explores selected issues in the legal environment created by domestic and international electronic contracting practices on the Internet within the United States and international jurisdictions: questions regarding the formation of the contract through the Internet, the enforceability of such a contract (contractual writing requirements, legally binding signatures), the contents of the contract, the ways to prove the electronic contract, the applicable law and the competent court, and finally, the best ways to settle disputes arising from electronic contracts are considered.

We examine to what extent contract law, and in particular article 2 of the Uniform Commercial Code (UCC), provides a satisfactory legal ground for the Internet, and how the various model trading partner agreements or the United Nations Commission on International Trade Law's Draft Model Statutory Provisions (UNCITRAL DMSP) deal with legal contract issues. We attempt to show that contracts in Cyberspace do not require any substantial reform but only some changes and adaptations to existing law, since when the policy considerations that underlie an existing rule still make sense as applied to Cyberspace, a completely new rule is not worth having. When parallel can be drawn from the way the law deals with old technologies such as the telephone, the telex or the telegraph, only adaptations to the new technology are often needed. Adaptations regarding the formation, the validity, the proof, of the contract and the allocation of risk in the transmission of the electronic message, are therefore to be implemented. On the other hand, it appears sometimes that old policies do not fit anymore to the new technology which creates, by virtue of its specificities, completely new issues and needs new rules or new concepts to be elaborated. This is the case for the paper-

based requirements, the methods of authentication of the electronic records, the laws and jurisdictions' conflicts when applied to electronic transactions.

But as long as those adaptations are not yet implemented, we advocate that the parties can, and should, efficiently address the existing legal uncertainties in a trading partner agreement in order to provide for certainty and stability. We give appropriate recommendations to businesses willing to use the Internet to conduct their commercial transactions on preferred contract law practices.

RESUME

Cette étude explore, au regard des droits américain et international, certains aspects des problèmes juridiques soulevés par les contrats signés par le biais du réseau Internet, tant au plan national qu'international. Sont ainsi étudiés la validité, la formation et les conditions de forme du contrat, le contenu du contrat et sa preuve, la loi applicable ainsi que le réglement des litiges survenus à l'occasion d'un contrat "électronique".

Nous examinons dans quelle mesure le droit actuel des contrats, en particulier l'article 2 du Code de Commerce Uniforme américain, fournit un fondement légal adapté à Internet et comment les différents modèles d'accords entre partenaires commerciaux, ou le modèle de loi UNCITRAL relatif aux contrats "électroniques", traitent ces questions.

Nous tentons de montrer que la législation actuelle ne nécessite pas de réforme fondamentale mais seulement des adaptations ou changements ponctuels. Lorsqu' une politique juridique qui soutend actuellement une règle de droit reste justifiée lorsqu' appliquée à Internet, une nouvelle règle totalement différente n'est pas nécessaire. Lorsque les parallèles sont possibles avec la législation applicable aux "anciennes" technologies telles que le téléphone, le télex ou le télégraphe, des adaptations sont suffisantes: cela concerne la validité, la formation, la preuve du contrat et l'allocation des risques dans la transmission. En revanche, lorsqu' Internet crée des problèmes totalement nouveaux, il est alors nécessaire d'élaborer de nouvelles règles basées sur de nouveaux concepts. Ainsi en est-il pour les conditions de forme du contrat, pour les méthodes d'authentification des messages électroniques, pour les conflits de lois et de juridictions.

En attendant, pour plus de stabilité contractuelle, nous conseillons aux parties contractantes de traiter préalablement ces questions non encore résolues dans un accord de partenariat commercial et donnons pour cela des recommendations.

TABLE OF CONTENTS

* *

*

INTRODUCTION

Businesses are increasingly using electronic messages, networked computers and information systems for conducting business that was once transacted solely on paper.

Electronic commerce is indeed rapid and accurate and can reduce the cost of doing business. The main advantages in the use of electronic communication technology to conduct business are the increased speed with which transactions can be conducted, the ability of commercial entities to transact business with the same ease as if they were across the street from one another, even when separated by thousands of miles of land or ocean, the elimination of repetitive computer input, the reduced inventory needs, the faster response to business demand, the reduced need for paper documents, the avoidance of transcription errors in commercial exchange of data and significant overall cost reductions. According to a report of the Commission of the European Communities, the cost of useless paper documentation in business transactions is estimated at five billion ECU's, with a 50% error rate in the resulting commercial documents, adding a further 15% to the cost of the final product[1]. Thus, it is not suprising that international trade is increasingly conducted by electronic means, in particular through the Internet, in all stages of the transaction, from negotiation through contract formation, performance (e.g., shipment), insurance and payment.

---

[1]Commission of the European Communities, "The Legal Position of the Member States with Respect to Electronic Data Interchange: Final Report", September 1989.

The Internet[2] can be defined as the international network of interconnected computer networks. It is borderless and covers the global community of computer networks. Internet is the first communication medium that allows remote users to readily access information and equipment across the world. Just as one uses the mailbox at the corner (now called the "snail mail" by Internet users), one can now send a letter or file nearly instantaneously to another user thousands of miles away by way of electronic mail[3]. Distance is no longer a significant barrier. Business can be conducted as quickly and easily halfway around the world as it once was up and down Main Street. According to Matthew R. Burnstein, Internet has made the "Global Village" a reality[4]...

The Internet enables businesses to contract for sale of goods electronically, process purchase orders, invoice for the transaction, and issue shipping notices in a one-step process. Countless goods and services are thus

---

[2]The terms "Internet", "Cyberspace", "information superhighway", "National Information Infrastructure" are more or less similar .The term "cyberspace" was first used by science fiction writer William Gibson in his book *Neuromancer*, the original cyberpunk novel (New-York, Ace Science Fiction Books, 1984). Gibson defined the term as "the mass consensual hallucination in which humans all over the planet meet, converse, and exchange information". The term "information superhighway" was first used in 1988 by Mitch Kapor (who founded Lotus Development Corporation in 1982) to describe a national network used for transporting information in multiple forms, including sounds, pictures, words, and numbers. The National Information Infrastructure (NII) is a superset of the planned National Research and Education Network (NREN), which is part of the United States federal government's High Performance Computing initiative. *Cf.* Erik J. Heels,"Let's make a few things perfectly clear: Cyberspace, the Internet, and that Superhighway" (1995) Student lawyer 15.

[3]The Internet was first designed by the United States Defence Departement, and initially constructed in the 1970's in response to the Cold War and threat of nuclear war. It was intended as a communication network which could withstand a nuclear attack, providing alternate routes for the government to send commands to its defence forces that would bypass communications links destroyed by a nuclear bomb. It soon spread to include links with university researchers under government contract. *Cf.* David E. Wires, "The security of information on the Internet: professional responsability, privilege and how safe is safe?", The Canadian Institute, Toronto, May 14, 1996.

[4]Matthew R. Burnstein, "Conflicts on the Net: Choice of Law in Transnational Cyberspace" (1996) 29 Vanderbilt J. of Transnational Law 75, p.81.

sold over the Internet, and the numbers continue to escalate (*cf* for example TRADENET for the port industry, MEDINET for the health care industry, BUILDNET for the construction industry, BOXMART for leasing, purchasing and selling large cargo containers, FAST for computer parts sales, GLOBEX for commodities futures and futures-options, TELCOT for the sale and purchase of cotton, COMMERCENET[5] for the purchase of goods and services, for bank services, and so on...)[6]. A British company even aims to begin "a formal electronic stock exchange on the Internet"[7].

As of July 1995, the Internet links an estimated thirty millions' users in 146 countries, and the number of users continues to grow at an astonishing 20% per month[8]. In addition to individuals, large and small corporations, law firms and legal departments, and specialty boutiques are discovering the power of the Internet. At present, 60% of Electronic Data Interchange (EDI)[9] users are in the manufacturing business, 13.7% are in wholesale trade, 8.1% are in transport and utilities, 7.7% are retailers and all others comprise

---

[5]CommerceNet is backed by companies such as Hewlett-Packard, Apple, Sun Microsysytem, Lockheed, and Bank of America. It allows users to purchase goods and services and do banking over the Internet. CommerceNet plans to use encryption and digital signatures' technology to protect network users from fraud and theft. *Cf.* Jared Sandberg, "Group of Major Companies Is Expected To Offer Goods, Services on the Internet", WALL ST. J., April 8 1994, at B3.

[6]For just a sampling of the shopping available on the World Wide Web, *See* http://www.yahoo.com and search for "Shopping". Sites include The Internet Shopping Network, the Internet Shopping Page, and the All-Internet Shopping Directory.

[7]Richard L. Hudson, "British Start-Up to Trade Stocks on the Internet" Wall St. J., Feb. 3, 1995 at A7A.

[8]April Streeter, "Don't get burned by the Internet", LAN Times, Feb 13, 1995.

[9]In its strict meaning, "EDI" is the technology and method by which business data may be communicated electronically between computers in standardized formats (such as purchase orders, invoices, shipping notices, and remittance advices) in substitution for conventional paper documents. Technically stated, EDI is the transmission, in a standard syntax, of unambiguous information between computers of independant organizations. But, in its broad sense, "EDI" has become the term commonly used to describe the use of computers for the movement of businesss information by telecommunications, irrespective of whether narrower technical definitions of EDI were also used: *Cf.* Report of the Working Group on Electronic Data Interchange (EDI) on the work of its twenty-fifth session, New-York 4-15 January 1993, A/CN.9/373 at 20.

10.4%[10]. As the popularity of the Internet grows, the quantity and sophistication of the commerce transacted through it will grow as well. Retail and wholesale storefronts are sprouting *en masse*, and methods for making payments are being implemented. EDI will then be the required method of conducting business domestically and internationally in the near future. It's rapidly becoming a competitive necessity.

Nowadays On-line catalogues and order forms are readily found on the Internet. Offers and acceptances occur in e-mail and contracts are formed, performed, and broken in Cyberspace. However the law currently governing commercial transactions was largely developed for a time when business was conducted with paper documents sent by mail. At the beginning of electronic transactions, businesses negotiated "electronic trading partners" agreements in written form, which posed fewer problems. Parties initially executed a written, paper agreement establishing protocols for electronic authentication and digital signatures. But now, on-line contracting is moving toward a system where users simply log on, point, and click, and a contract is formed. Cyberspace thus raises challenging new legal issues. Disputes arise regarding the formation, the enforceability, and the performance of contractual obligations.

Let's take examples. In a music forum, CDs are available for sale. The subscriber is first asked to choose the type of music -classical, jazz, modern, etc. Then a selection is shown by composer in alphabetical order with prices. A choice can be made which then asks for the quantities and explains that the price previously quoted does not include VAT or sales tax, postage or other

[10]Robert W. McKeon, "Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena" (1994) 12 J. of Computer & Inf. Law 511.

incidentals. Next an option is given to 'order' or 'cancel'. If the order option is taken then delivery details are requested. Credit card information follows where a special password may be set up for security reasons. Again the option to cancel is given. Otherwise the order goes through, and the CD is mailed to the subscriber or in the case of software or books, could be downloaded to the subscriber's computer. This transaction gives rise to many legal questions. Is there a binding contract? What happens if the CD is paid for but the goods are not delivered, or that goods are delivered but not in conformity with what was agreed upon?

Another example, culled from the "misc.legal" UseNet newsgroup, gives us an idea of the questions that can arise when shopping via the Internet:

> #69979
> From: [author's name omitted]
> Subject: Internet deals gone awry: MAIL FRAUD or SMALL CLAIMS COURT
> Date: Mon, 13 Feb., 1995 15:07:29 GMT
> When Internet deals go bad, what can be done to fight back? Recently, I have made a "deal" with someone in another state. I though I was getting a motherboard populated with 16MB of SIMMs, but after giving the Federal Express COD delivery person a money order for about $600, I opened the box to find a broken board with no memory. I called the Post Office and tried to cancel the Money Order: no such luck. I called Federal Express too and tried to stop the delivery of the money order: no such luck.
> What can I do? (Legally, that is...)
> Sue him in Small Claims court...in his state? [I]n my state?
> Report it as Mail Fraud (but it was FedEx, not U.S. Postal Service...)
> or am I flat-out screwed [sic]?
> Has any legal precedent been set yet in this area?
> Have any cases like this been fought and won? Lost?
> How do you fight brick-in-the-mail Internet Fraud?
> [author's name omitted]

The reliability and integrity of such a way to purchase goods depend upon the adaptability of existing laws.

In traditional paper-based commerce although legislation does not usually explicitly demand the use of paper, the terminology will often create that result. Legislation can speak in terms of "the document", as well as the need to have things "in writing" and "signed". Likewise, formalities pertaining to manually written documents, signatures or notices are often required as forms of proof in disputes involving the validity or enforceability of commercial contracts. In the absence of such documents and authentication as proof of validity, a party's legal remedies are substantially impaired. A similar need exists with commerce on the Internet as everything is carried out through computers. In the course of such commerce, disputes will occur requiring authentication and documentation of information movements to prove dispute issues.

The use of electronic technology can therefore create legal uncertainty with a party not being sure that its electronic message complies with the necessary legislative requirements. Yet, if current requirements for paper-based documents, notice and signature are maintained, the potential of electronic commerce will not be reached, and advances in accuracy, speed, and efficiency resulting from electronic business will be lost.

In addition, the universal acceptance of networks for transacting business requires security measures to ensure the privacy needed for commercial transactions in a global competitive environment. Security measures that provide assurance that the authenticity and integrity of a communication have not been compromised will tend to support the enforceability of agreements by the legal system. The security issues that must be dealt with are: (i) requirements for authentication of the source of a transaction, (ii) assurance that the message content is unaltered, (iii)

prevention of disclosure of the transaction to unauthorized persons, (iv) verification of receipt of the transaction by the intended trading partner.

Today, the laws are changing slowly and contract law will likely adapt to our growing dependence on Cyberspace transactions. Governments and businesses are currently trying both to adapt the existing paper-based requirements to accommodate technological change as well as develop new, alternative rules where existing rules cannot be adapted to accommodate technological change[11].

An important proposed expansion of Article 2 of the Uniform Commercial Code (hereinafter U.C.C.) is currently being undertaken by the National Conference of Commissioners on Uniform State Laws. It covers software, data and information contracts and validates certain electronic transactions, such as shrink wrap, on-screen, mass market licenses and other standard electronic agreements, provided the contract and performance occur electronically and the licensees have the opportunity to review the license terms[12].

Furthermore, as the Internet is by nature international, most of the transactions carried out on the Internet -and it is one of the main advantages

---

[11]Sports and business through the use of electronic commerce have been compared in the following manner:

> "Transacting business through the use of electronic data interchange is like playing a new sport which has no specific rules governing the play. While we can analogize the rules governing other sports (in this case, paper-based transactions), those rules (which traditionally have come from legislation, court decisions, and regulation) may or may not work adequatly. These pre-existing are not electronic data interchange specific, and applying the paper-based rules to electronic transactions may lead to inappropriate results."

Amelia Boss, *The Proliferation of model interchange Agreements,* in EDI Worldwide, Proceedings of the Third International Congress of EDI Users, Brussels 1991.

[12]Robert A. Feldman, "Emerging Issue in Computer Law" (1995) 12 Computer Lawyer 1.

of the Internet- will be international. No longer are parties to a commercial transaction bound by artificial national boundaries with their accompanying sets of domestic rules. It is then important that the different countries, both domestically and internationally, agree on the electronic policies' issues so as to harmonize the rules regarding electronic commerce and not to prevent but to facilitate international electronic transactions. The international trading community has recognized this need. Significant attention has already been paid to the developments of legal definitions that accommodate electronic documents, writings, signatures and notices[13]. The sources of this attention have been governments as well as businesses and professional groups. Among them, a working group of the United Nations Commission on International Trade Law (UNCITRAL) is currently working on a "Model Statutory Provisions" (hereinafter UNCITRAL DMSP), which deals with various legal aspects of electronic transactions such as the formation of contracts by electronic means, the legal value of electronic documents as to the current legal requirements to be an "original", a "writing", a "signed" document, the legal value of computer records, the evidentiary value of electronic messages. It aims at removing many of the obstacles which exist to the full scale implementation of electronic trading.

But as long as there does not exist a clear framework in domestic or international legislative, judicial and administrative recognition, validation, and regulation of electronic commerce, and in the absence of industry-wide customs or standards to guide conduct, parties got used to address these legal uncertainties by entering into agreements governing their electronic

[13]Judith Y. Gliniecki & Ceda G. Ogada, "The Legal Acceptance of Electronic Documents, Writings, Signatures, and Notices in International Transportation Conventions: A Challenge in the Age of Global Electronic Commerce" (1992) 13 Northwestern J. of Int. Law & Business 117.

trading[14]. Many organizations nationally and internationally have been developing model or standard interchange agreements which parties to electronic commerce can use to structure their transactions. In effect, these organizations have been evolving a legal structure for electronic commerce, one that may be adopted privately by contracting parties, but also a legal structure that may serve as a roadmap for other lawmaking institutions faced with developing a framework for electronic commerce, such as the UNCITRAL Working Group which used them to draft its Uniform Rules.

The idea of a model interchange agreement was first raised at the international level by the Nordic Legal Community in the early 1980's[15]. That initial idea resulted in the adoption by the International Chamber of Commerce (ICC) in 1987 of the Uniform Rules for Conduct for International Trade Data by Teletransmission (UNCID)[16]. The UNCID Rules are a small set of non-mandatory rules which EDI users, suppliers of network services, and others implementing electronic communications technologies may incorporate into any communications agreement.

Since the publication of the UNCID Rules, numerous model interchange agreements have been developed -by EDI user groups representing specific industries (such as Odette, representing the European automotive industry[17], or the International Maritime Committee, representing the maritime industry[18]), by electronic data interchange industry groups (such as electronic

---

[14]Called "interchange agreement" or "electronic trading partner agreement".

[15]Amelia H. Boss, "Electronic Data Interchange Agreements: Private Contracting Toward a Global Environment" (1992) 13 Northwestern J. of Int. Law & Business 31, p. 38.

[16]International Chamber of Commerce, *Uniform Rules of Conduct for International Trade Data by Teletransmission* (UNCID) (ICC Publication No. 452, 1988).

[17]*Guidelines for Interchange Agreements*, prepared by the Organization for the Data Exchange through Teletransmission in Europe (Odette) (1990).

[18]CMI Rules for Electronic Bills of Lading, adopted by the Comite Maritime International (International Maritime Committee or CMI) in June 1990, published in Letterof Credit Update 27-31 (April 1991).

data interchange associations in the United Kingdom[19], Australia[20], Canada[21], New Zealand[22] and South Africa[23]), by attorney groups (such as the American Bar Association[24]), by governmental agencies[25], and by multinational organizations (such as the Commission of the European Communities through its TEDIS program[26], the Customs Cooperation Council[27], or the CMEA[28]). These groups cover many areas of trade, from sale and services agreements, to customs and transport.

Mainly, these Model Agreements deal with business issues such as technical requirements, acknowledgment of receipt, security measures, etc., and with legal issues such as contract formation, validity and enforceability of the contract, evidentiary value of messages, liability for failure or error in communication, terms and conditions of the underlying contract, dispute resolution... The parties who are in a continuous business relationship are thus given the opportunity to adhere to these Model Agreements, and incorporate those rules by reference into their business dealings. Just as

---

[19]EDI Association Standard Electronic Data Interchange Agreement, prepared by the EDI Association of the United Kingdom (2d ed. August 1990).

[20]Model Electronic Data Interchange Agreement and Commentary, prepared by the Legal Sub-Committee advising the EDI Council of Australia (version 1, October 1990).

[21]Model Form of Electronic Data Interchange Trading Partner Agreement and Commentary, prepared by the Legal and Audit Issues Committee of the EDI Council of Canada (Canada 1990).

[22]Standard EDI Agreement, prepared by the New Zealand Electronic Data Interchange Association (New Zealand, October 1990).

[23]Model Interchange Agreement, prepared by the Organization for the Simplification of International Trade Procedures in South Africa (March 1991).

[24]Model Electronic Data Interchange Trading Partner Agreement and Commentary, prepared by the American Bar Association (June 1990), published along with The Commercial Use of electronic Data Interchange - A Report and Model Trading Partner Agreement, in (1990) 45 Bus. Law. 1645.

[25]Standard Interchange Agreement, prepared by the Ministry of Communication of the Province of Quebec (Canada, September 1990).

[26]TEDIS Programme European Model EDI Agreement, prepared by the Commission of the European Communities, DG XIII - D (May 1991).

[27]Guideline Concerning Customs-Trader Interchange Agreements and EDI User Manuals, Customs Cooperation Council document 35.910 (March 22 1990).

[28]Model Agreement on Transfer of data in International Trade, agreed upon by the Republic of Finland and CMEA Member States (1991).

commercial practices evolved "Incoterms" which permitted choice of those shipping, risk of loss and cost terms which applied to their transactions, the suggestion has been made that "Editerms" could be developed for electronic commerce[29].

Within this thesis, I attempt to show that contracts in Cyberspace do not require any substantial reform but only some changes and adaptations to existing law. Since the policy considerations that underlie traditional rules still make sense as applied to Cyberspace, a completely new rule is not worth having. Parallels can be drawn from the way the law dealt with old technologies such as the telephone, the telex or the telegraph, where adaptations to the new technology developed. Adaptations are therefore needed to make it clear that: (i) a contract is not void and unenforceable by the mere fact that it has been concluded only through electronic means; (ii) it is deemed to be formed when the offeree receives the acceptance, and where the offeree's main place of business is; (iii) the hearsay and the best evidence rules do not preclude the record of an electronic message to be admissible in court provided the retention procedure vouches for enough trustworthiness; (iv) the risk of errors in the transmision of the messages is on the sender unless the addressee had the duty to confirm the message and did not do so, or knew or had reasons to know that an error occured. However, sometimes old policies don't fit to the new technology which creates new issues in some respects. In that case, the law should take into account this phenomenon by recognizing that: (i) the terms "writing" and "signature" must be replaced by the term "record" and methods of authentication that exist in the electronic

---

[29]Pascal Brousse, "Toward a More Suitable Interchange Contract", International Chamber of Commerce, Commission on International Commercial Practices, Working Party on EDI, Doc. 460-10/ Int. 42, Jannuary 1992; Carol Xueref & Pascal Brousse, "EDI: 'Editerms' would help to cope with EDI legal issues" (1992) 1 Computer & Telecoms Law Review 3.

environment such as the "digital signature"; (ii) new laws and jurisdictions' conflicts are needed which do not depend on locations.
But as long as those adaptations are not yet implemented, I advocate that the parties can, and should, efficiently address the existing legal uncertainties in a trading partner agreement in order to provide for certainty and stability.

In the first two sections, I study the validity and the enforceability of a contract formed via Internet; then I discuss how it is possible to prove the contract thus formed and what is its content; finally I deal with the issues of applicable law and dispute settlement.

My primary jurisdiction is contract law of the United States, that is to say mainly the Uniform Commercial Code. The U.C.C. is a code pertaining to business law. It has been adopted individually by almost all of the States. It is continuously being revised by a permanent committee, the Permanent Editorial Board of the U.C.C. As recently as 1991, this committee expressly pointed out that Article 2, concerning contract law, needed to be revised in order to take into account the new technology of computers: "The technology and use of [electronic transactions] have evolved without any revision in any article of the U.C.C. (...) When [electronic transactions] are used, obvious questions are how does one satisfy §2-201's requirements of a 'signed writing' or how does one give 'written notice' or furnish 'conspicuous' terms on a computer? Similar problems involve the point at which a contract is formed through [electronic transactions] and the incorporation of 'additional and

different' terms. Whatever the correct answers, revisions of Articles 1 and 2 will be required[30].

The corresponding case law is also taken into account as it is part of the contract law.

Two main models are considered throughout this thesis.

First is the American Bar Association Model Electronic Data Interchange Trading Partner Agreement (hereinafter ABA Model Agreement). This model has been prepared by the Electronic Messaging Services Task Force, a subcommittee on Electronic Commercial Practices of the UCC Committee, Section of Business law, of the ABA. It is a model for an electronic trading partner agreement. Along with its section-by-section Commentary, it aims at furnishing a tool for counsel whose clients are integrating electronic means into their contracting procedures.

Second is the UNCITRAL Draft Model Statutory Provisions on the Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Data Communication (hereinafter UNCITRAL DMSP). It was prepared by the Working Group on Electronic Data Interchange (EDI). It is not a model of a trading partner agreement but it is drafted as a uniform statute dealing with issues pertaining to electronic transactions. This UNCITRAL DMSP is worth stressing since it has been prepared by all the member states of the United Nations Commission and it purports to be a model for national legislators when reviewing national laws for the electronic context[31].

---

[30]The Permanent Editorial Board of the Uniform Commercial Code, "PEB Study Group: Uniform Commercial Code, Article 2 Executive Summary"(1991) 46 The Business Lawyer 1869, p. 1874.

[31]The Working Group on Electronic Data Interchange was composed of the following states: Austria, Bulgaria, Cameroon, Canada, China, Costa Rica, Denmark, Egypt, France, Germany, Hungary, India, Islamic Republic of Iran, Italy, Japan, Kenya, Mexico, Morocco, Nigeria, Russian Federation, Saudi Arabia, Singapore, Spain, Sudan, Thailande, United Kingdom of Great Britain and Northern Ireland, United States of America and Uruguay; and the following

Within a common electronic network, there exist two major relationships: those between the service supplier and the users; and agreements between the users themselves. Only the latter will be dealt with in this study.

observers: Australia, Bolivia, Brazil, Côte d'Ivoire, Finland, Indonesia, Israel, Federated States of Micronesia, Pakistan, Philippines, Romania, Sweden, Switzerland and Venezuela.

SECTION 1- THE FORMATION OF THE CONTRACT THROUGH ELECTRONIC MEANS

While many electronic transactions are not intended to obligate the sender contractually[32], numerous other electronic messages are intended to establish a binding obligation on the sender in order to result in an enforceable agreement.

Within this section, the questions posed are:

(1) Is an electronic message capable of revealing the "assent" of the parties to enter the agreement?

(2) Is it then possible to transmit an offer and an acceptance through Internet in order to create a valid contract, and under what conditions will they be legally binding?

(3) Who bears the liability or the risk of an error or a failure in the transmission of the message?

1. The manifestation of mutual assent through electronic means: the offer and the acceptance

According to the common law of contracts, an offer message has to meet an acceptance, which agrees to the offer entirely, for a contract to

---

[32]Most of the EDI initiatives in the Canadian oil and gas industry, for example, are primarily focused on exchanging information regarding production, revenue accounting and billing, so that recipients may quickly and easily utilize that information for their own purposes: these data exchanges under these programs do not create legally binding contracts. *Cf.* Brian D. Grayton, "Canadian Legal Issues Arising from Electronic Data Interchange" (1993) 27 University of British Columbia Law Review 257, p.272.

emerge. The offer and the acceptance must contain the assent of the parties to be juridically bound.

Within this part, we will study if the manifestation of assent can lawfully be transmitted through computers and networks; and then under which conditions are electronic offer and acceptance legally effective in order to bind the parties.

1.1. The manifestation of binding assent by electronic message

Contract law is founded on actors manifesting an intent to commit themselves (through offers or acceptances). A contract is a binding promise, or set of promises: a condition to the binding of a party to a typical contract is that the party must have manifested his voluntary assent to it. But as soon as a party has expressed its intent to commit itself, the party is bound and the other party is thus entitled to rely upon it (except for the possibility of revoking the offer or the acceptance, dealt with later).

In the electronic environment, can an electronic message manifest the "assent" of a party, and is the party consequently bound by its message (offer or acceptance)?

Electronic contracting contemplates transmission of an electronic impulse signifying an order and, in some cases, an electronic transmission indicating either receipt or acceptance of the particular order. But, with EDI for example, the exchange may occur without any human actor making a decision to place an order or to accept the order that has been placed: in trading partner relationships, a system can be implemented by which a computer can decide to issue an order based on the buyer's inventory records,

and another computer can accept the order based on parameters for acceptability programmed into it. In a purely automatic electronic exchange, the question is whether the electronic message can establish an offer and an acceptance given the absence of documentation and of human decision.

1.1.1. Under the common law

U.C.C. Article 2[33], shuns formalistic rules for ascertaining assent, and permits assent to be discovered wherever it may be. U.C.C. §2-204(1) states, "A contract for sale of goods may be made in any manner to show agreement, including conduct by both parties which recognizes the existence of such a contract". Thus Article 2 is very open to finding that contracts have arisen between parties and flexible in the way it looks for contracts, but it still demands some manifestation of assent to the basic terms by both parties.

According to Raymond T. Nimmer, Reporter for the Committee to revise Article 2B of the Uniform Commercial Code, even if it is the computer that issues the specifics of the message, the actions taken by the system stem from programming created on behalf of the buyer or from specific instructions entered by the buyer's staff[34]. Thus, the assent to the message (the offer or the acceptance) will be presumed and it will be binding.

For Benjamin Wright, an eminent authority on electronic contracts, the law is flexible in the manifestations of assent it recognizes. In the world of electronic business messages, the sender of a message manifests its assent

[33]Article Two of the U.C.C. governs sales-of-goods contracts in all states but Louisiana.
[34]Raymond T. Nimmer, "Electronic Contracting: Legal Issues" (1996) 14 Journal of Computer & Information Law 211, p.215.

merely by sending a message. This very act of sending a message can signify assent. Even the programming of a computer to automatically issue messages should suffice[35]. Therefore, the transmission of an appropriate electronic message can constitute either offer and acceptance under the common law or communication showing agreement under U.C.C. Article 2.

The proposed revision of U.C.C. Article 2, which aims at covering the new issues created by computer technology as a new means for contracting, provides that:

> Section 2-208 "Electronic transactions: formation":
>
> "(b) A contract is created (...) *even if no individual representing either party was aware of or reviewed the initial response, the formation, or the action* that signifies acceptance of the contract. Electronic records exchanged in an electronic transaction *are effective* when received in a form and at a location capable of processing the record or the intangible even if no individual is aware of the receipt[36]." *(Emphasis added).*

This makes it clear that the effectiveness of the electronic message does not depend on the existence of a human decision-maker reviewing any of the relevant materials. The assent to any electronic message is presumed and the mere fact of sending it binds the sender.

1.1.2. Under the ABA Model Agreement

For the ABA Model Agreement also, the assent can be transmitted through the computer, but the mere fact of sending a message electronically

---

[35]Benjamin Wright, *EDI, E-Mail and Internet: Technology, Proof and Liability, The Law of Electronic Commerce*, 2nd ed., Boston, Little, Brown & Co., 1995, §5.4.
[36]Raymond T. Nimmer, *supra note 34*, p. 225.

has no legal significance: the message will only be binding if the receiver sends an acknowledgment of receipt in return.

The acknowledgment of receipt is the condition for a message to have any legal effect. The Model Agreement constructs an environment in which receipt, and not transmission, determines the legal effect of any message transmitted by EDI, and in which verification of the transmission is a mandatory element of conducting business with EDI.

First, the Model Agreement rejects the principle that transmitting a message has any legal significance. Section 2.1 of the Model Agreement provides that no document shall give rise to any obligation until "properly received". This requires that the transmitted document be accessible (and not actually examined[37]) at the receiving party's computer. But the fact that proper receipt of a document has occurred does not automatically bestow it with legal significance.

Indeed the Model Agreement further imposes an affirmative obligation upon the receiving party of any document, upon proper receipt, to promptly and properly transmit in return a message verifying receipt of the original document (the "functional acknowledgment")[38]. In the absence of receiving verification, the originating party is on notice that communication may not have effectively occurred.

---

[37]In a paper-based environment, this is similar to when a letter is delivered, but the envelope remains unopened.

[38]Electronic Messaging Services Task Force, "The Commercial Use of Electronic Data Interchange - A Report" (1990) 45 The Business Lawyer 1647, p. 1668.

1.1.3. Under the UNCITRAL Draft Model Statutory Provisions

The UNCITRAL Draft Model Statutory Provisions, also, provides for an article that deals with the conditions under which the sender of a message is bound by the content of the message and therefore under which the receiver is entitled to rely on. The article reads as follows[39]:

> Article 10. [Effectiveness] [Obligations binding on the originator] of a data [record]
>
> (1) As between the originator and the addressee, an originator is [deemed] [presumed] to have approved the [content] [communication] of a data [record] if it was [issued] [transmitted] by the originator or by another person who had the authority to act on behalf of the originator in respect of that data [record].
>
> [(2) As between the originator and the addressee, a data [record] is [deemed] [presumed] to be that of the originator if the addressee properly applied a procedure previously agreed with the originator for verifying that the data [record] was the data [record] of the latter.]
>
> [(3) An originator who is not [deemed] [presumed] to have approved the data [record] by virtue of paragraph (1) or (2) of this article is [deemed] [presumed] to have done so by virtue of this paragraph if:
>
> (a) the data [record] as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to the authentication procedure of the originator; or
>
> (b) the addressee verified the authentication by a method which was reasonable in the circumstances.][40]

In sum, the sender will be bound by its message (i) if it is issued itself or through a person under its authority, or (ii) if the receiver has checked the

---

[39]Square brackets indicate that the Working Group has not decided yet on the exact wording.

[40]UNCITRAL Documents A/CN.9/WG.IV/WP62 of 20 July 1994 (for Articles 1-10) and A/CN.9/WG.IV/WP.60 of 24th January 1994 (for Articles 11-15) available under the name of "EDI-TXT" in the Library 0 of the CompuServe Legal Forum.

origin of the message in accordance with a method previously agreed on or commercially reasonable.

The UNCITRAL DMSP, however, does not necessarily require that an acknowledgment of receipt be sent back by the receiver for the message to be legally binding. But, if so agreed by the parties, then the UNCITRAL DMSP states the legal consequences of the failure to acknowledge the message:

> Article 11. Acknowledgment of receipt
>
> (...)
> (2) If, on or before transmitting a data message, or by means of that data message, the [sender] [originator] has requested an acknowledgment of receipt [and stated that the data message is to be of no effect until an acknowledgment is received], the addressee may not rely on the message, for any purpose for which it might otherwise seek to rely on it, until an acknowledgment has been received by the [sender] [originator].
>
> (3) If the [sender] [originator] does not receive the acknowledgment of receipt within the time limit [agreed upon, requested or within reasonable time], it may, upon giving prompt notification to the addressee to that effect, treat the data message as though it had never been received[41].

In sum, in this situation, the legal effect of a message is subject to a prompt acknowledgment of receipt, in the absence of which, the message is deemed not to have ever been received and the receiver is not entitled to act upon it.

'41 *Id.*

According to article 2-208 of the proposed revision of Article 2[42], the mere fact that the offer and the acceptance occurred by way of electronic means does not preclude the contract from being valid and enforceable at law. So does, for example the UNCITRAL DMSP make clear: Article 12, as regards to the formation of contracts, states that:

> (1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data [records] [messages]. Where a contract is formed by means of data [records] [messages], it shall not be denied validity or enforceability on the sole ground that the contract was concluded by such means[43].

However, offer and acceptance is an area where electronic transactions pose some unique problems. First, because electronic communications enable the automation of the decision-making process leading to the formation of a contract, such automation might increase the possibility that, due to the lack of a direct control by the owners of the computers, a message would be automatically sent and a contract formed, that did not reflect the actual intent of one or more parties at the time when the contract was formed. The consequences of an error in the generation of a message might be greater in this situation than with traditional means of communication, since the mistaken contract would be automatically executed.

Second, because of the lack of certainty as to the role, and the legal consequences, played by the acknowledgment of receipt, it might be said that when a supplier sends a functional acknowledgment confirming receipt of a purchase order in complete and proper form, it becomes bound to ship the

---

[42] *Cf. supra section 1.1.*

[43] Model Electronic Data Interchange Agreement and Commentary, *supra note 20.*

ordered goods at the stated price. This may depend on whether the supplier's catalogue is considered to be an offer to sell goods or an invitation to treat. Even if, as is often the case, it is regarded as merely an invitation to treat, to which the manufacturer has responded by sending in an offer to purchase, can it be said that the functional acknowledgment has no legal effect and that the supplier is not bound until it sends a formal acceptance or purchase acknowledgment?

Under which conditions will an electronic offer or acceptance be legally effective in order to create a binding contract?

1.2.1. The offer via computer

1.2.1.1. Under the common law

According to the common law of contracts, an offer consists of an expression of a willingness to enter a contract when that expression occurs in a form sufficiently concrete to establish that agreement.

This doesn't mean, however, that the offer be in writing. The issue as to whether an electronic contract is sufficient to constitute a legal "writing" (which will be discussed later) is to be set apart, for, subject to considerations concerning the Statute of Frauds, no requirement exists in law that a contract offer be in writing: conduct may establish a contract[44]. There is even no requirement that there be a conscious, immediate intent to make a binding commitment.

---

[44]U.C.C. §2-207(3).

As we have just seen, electronic messages are capable of asserting the intent of the sender to be bound by the content of its message. Therefore an electronic message that purports to be an offer can constitute a valid offer. To the extent that the purported offer contains the minimum elements required to be a valid legal offer[45], the electronic message will be valid as such and will thus be binding.

1.2.1.2. Under the ABA Model Agreement

The ABA Model Agreement treats offers like other documents: according to Section 2.3, an offer does not give rise to any obligation until properly received. Irrespective of whether the receiving party wishes to accept the offer, the receiving party must transmit a functional acknowledgment[46] for the offer to be effective.

1.2.1.3. Under the UNCITRAL Draft Model Statutory Provisions

Likewise, the UNCITRAL DMSP doesn't deal specifically with the offer but provides that, as for any type of message, it will be effective and thus the offer will be binding, by the mere sending of the offer as long as it actually came from the sender, or upon acknowledgment of receipt if necessary.

---

[45]According to U.C.C. §2-204(3), a contract may come into being even if some of its terms are indefinite, provided "there is a reasonable basis for giving an appropriate remedy".

[46]Report of the Electronic Messaging Services Task Force, *supra note 38*, p. 1674

1.2.2. The acceptance via computer

1.2.2.1. Under the common law

As to the acceptance, common law presumes that an effective acceptance must be communicated with knowledge of the offer and an intent to accept that offer. As a matter of law, however, intent is measured by objective manifestations, rather than subjective intention. This means that the person responding to an offer is held to intend "what appeared from his expression to be his intention" unless circumstances indicate clearly to the contrary. Thus, in ordinary contract law, the defense of "I didn't mean what I said" may not carry weight. Likewise, the defense of "I didn't mean what my computer said" may not be relevant where all the characteristics of the electronic response induced the other party (or his computer) to conclude that a contract has been reached.

Consequently, the fact that a completely automatic acceptance occurs does not indicate that there has been no adequate acceptance of the electronic offer since in contract creation one deals with the apparent intention of the party establishing the electronic acceptance device or system itself. Assuming the facts fit, a company that creates an entirely automated system to electronically confirm offers creates the objective indicia of an intention to be bound by the responses issued within the parameters that it programmed into the automated system (objective indicia control).

On the other hand, there must be some indication that the automated system was intended to signify acceptance, rather than merely to confirm receipt. Modern communications systems make possible immediate and

routine confirmation of the receipt of an offer and even of the terms of the offer. This confirmation can be an important safeguard against garbled messages and other system-based problems. Merely issuing a confirmation of receipt of the offer cannot create a contract, whether confirmation occurs automatically or by action of a human actor.

This has been held in *Corinthian Pharmaceutical Systems v. Lederle Labs*[47] which examined whether a purely electronic message constituted a manifestation of assent to a contract. Corinthian is an electronic contract case, although it does not involve EDI, or e-mail. The technology involved was interactive telephone. Lederle Laboratories, a pharmaceutical manufacturer, had installed a computer order entry system (Telgo) that let customers place orders remotely using touchstone telephones. Customers could, from their offices, dial directly into Telgo and place orders by punching keys on their telephones.

On May 19, 1986, Corinthian Pharmaceutical, a drug wholesaler, learned that on May 20 the price Lederle charged for DTP vaccine would rise from $51 to $171 per vial. Corinthian immediately dialed into Telgo and placed an order for 1000 vials. Telgo automatically responded to Corinthian by giving it a tracking number for the order.

Some days later, however, Lederle refused to fill the order, so Corinthian sued, claiming breach of contract. The court held that there was no contract. The order placed by Corinthian was an offer to buy, but there was no acceptance from Lederle. In other words, Lederle had not manifested its assent to the contract to sell 1000 vials. Corinthian argued that the tracking number from Telgo was an acceptance, but the court rejected this argument, saying

---

[47]724 F. Supp. 605 (S.D. Ind. 1989).

that the number was just an administrative message, not a clear acceptance[48]. The court reinforced its conclusion by observing that in previous terms and conditions communicated from Lederle to Corinthian, Lederle had made clear that no order was effective until accepted by Lederle. Significantly, the court implied that if Telgo did indicate acceptance, a contract would have been born. It would have been a contract in which assent would have been manifested only electronically (offer by Corinthian through the telephone; acceptance by Lederle through the electronic tracking number).

In some cases, of course, the differentiation between confirmation of an offer and acceptance of that offer will present close factual issues. The distinction does not and should not turn on whether the response was triggered automatically. The capability to create an automated acceptance system rests fully within the range of conduct that, under general contract law, constitutes a form of acceptance sufficient to create a contract. Yet, some methodology should be created for stabilizing the distinction in practice between electronic confirmation that an offer was received and electronic acceptance of that offer[49]. The party who accepts the offer must expressly say so and distinguish it from its usual acknowledgments of receipt.

The *Corinthian* case can probably be relied upon as confirming that an electronic acknowledgment message will not amount to an acceptance so as to create a binding agreement between the parties. Since the purpose of the functional acknowledgment is to confirm that the incoming message was in recognizable form and capable of being translated and processed by the

---

[48]The order tracking number was analogous to an EDI functional acknowledgment. It was evidence of receipt of a message, but it did not respond to the substance of that message.
[49]Raymond T. Nimmer, *supra note 34*, p. 216.

recipient's system, it seems reasonable that the courts would regard it as not representing a sufficient indication of acceptance. However, a trading partner agreement would typically set out in advance by means of an "EDI protocol" precisely at what point in a series of transmissions a binding agreement would be created.

In line with the *Corinthian* case, the proposed revision of U.C.C. Article 2-208 pertaining to "Electronic transactions: formation", expressly stipulates that:

> "(a) In an electronic transaction, if an electronic message initiated by one party evokes an electronic message or other electronic response by the other, a contract is created when:
> (...)
> (2) the initiating party receives a message *signifying* or *acknowledging acceptance* of the *offer contained in its message"*

By this way, Article 2-208 tends to assure that symmetrical knowledge exists between the parties.

Concerning the medium of acceptance required, general contract law provides that acceptance must be made in the manner specifically required by the offeror, but that if no specification of the method for acceptance is made in the originating offer, acceptance may be in "any manner and by any medium reasonable in the circumstances[50]".

Determining what constitutes a reasonable response involves considerations of the "speed and reliability of the medium, a prior course of

---

[50]U.C.C. 2-206(1)(a) official Comment 1; Restatement (Second) of Contracts §65 comment b (1981). Comments to both indicate that the law is flexible and receptive to new media, which presumably include electronic media. The Restatement indicates more generally that acceptance can be in any manner customary at the time and place.

dealing between the parties and the usage of trade." A seller who makes computer-based systems available to the general buying public or to specific trading partners with which it deals may respond through an electronic acceptance of the offer. Clearly, this is the case where the electronic offer or the trading partner agreement requires that response. It is also the case if the agreement and the electronic message are silent on how to communicate acceptance. This can arise through a course of dealing between trading partners, or through a more grounded analysis which emphasizes that the seller's acts in making available an ordering system of a given type and the buyer's use of that system indicates willingness to use such methodology in response.

Still, concluding that electronic acceptance would be reasonable does not mean that other methods of acceptance are unreasonable. Some courts have held that acceptance of a telegraphed offer by a mailed acceptance was reasonable in the absence of specifications in the offer insisting on a more rapid form of acceptance This may however not be the case in a rapid exchange or a just-in-time delivery system which implicitly requires prompt response. Indeed, the U.C.C. provides that an offer to buy goods "for prompt or current shipment shall be construed as inviting acceptance either by prompt promise to ship or by the prompt or current shipment of...goods[51]" The emphasis in both options is on prompt action. Of course, if the trading agreement expressly requires electronic acceptance, or if the electronic offer expressly requires such acceptance, the responding seller must reply in that manner.

---

[51]U.C.C. §2-206(1)(b).

Not all computerized orders, however, make provision for an electronic acceptance. The range of alternatives for accepting an offer corresponds roughly to the range of alternatives available in manual or paper-based systems. The most common alternative means of acceptance is the shipment of the goods ordered. Delivery of product against the offer may be acceptance and constitutes a reasonable approach in transactions entailing immediate delivery requirements. The Restatement (Second) of Contracts indicates that if an offer invites acceptance by performance, the contract requires no notice of acceptance to the offeror (buyer)[52]. However, an offeror not notified of acceptance within a reasonable time may treat the offer as having lapsed by acting before delivery of the goods[53].

1.2.2.2. Under the ABA Model Agreement

Concerning acceptance, the ABA Model Agreement, in accordance to its principles, requires that, for each type of document, the parties are to specify whether acceptance is required and if so, the corresponding acceptance document that will evidence such acceptance[54].

In no event, however, does the Model Agreement eliminate the need for acceptance of an offer. In the absence of an acceptance document being specified for a document from which an offer is made, no obligation may arise before the document has been properly received. Then, if no acceptance document is required, the conduct of the receiving party, if it acts to accept or

---

[52]Restatemnt (Second) of Contracts §54.
[53]U.C.C. 2-206.
[54]Report of the Electronic Messaging Services Task Force, *supra note 38*, p. 1674.

otherwise justifiably relies upon the original document, may be sufficient to create a binding obligation[55].

As for the medium of acceptance, the ABA Model Agreement requires that acceptance be given in the same manner[56], *i.e.*, by EDI communication, as the offer. Although the Code permits acceptance to be transmitted in any reasonable manner, the drafters of the Model Agreement determined that the mutual course of conduct by trading partners to communicate through electronic means was sufficient, as a whole, to justify limiting the manner in which acceptance may occur without any resulting detriment to the interests of the offeree. Indeed, mandating a medium of acceptance that is the same as used by the offeror is comfortably within the concept of reasonableness. According to the Restatement (Second) of Contracts §65 (1981)[57] "medium of acceptance is reasonable if it is the one used by the offeree". A comment thereto confirms that "reasonableness is a function of the speed and reliability of the medium, a prior course of dealing between the parties and the usage of trade". The Model Agreement, however, does not contemplate that electronic means may be used to communicate acceptance with respect to an offer that was communicated by other means[58].

---

[55]*See* U.C.C. §§2-204(1), 2-206(1); Restatement (second) of Contracts § 90 (1981). In addition, if the parties establish a course of performance involving the transmission of a purchase order, for which no acceprtance document is provided but the contract is nevertheless routinely performed, the absence of an acceptance document will not interfere whit the existence of a valid contract. *See* U.C.C. § 2-208.

[56]ABA Model Agreement Section 2.3

[57]The Restatements are methodical and systematic compilations of case law elaborated in specific fields of the law, such as the law of torts, the law of contracts, the law of property , the conflicts of laws, etc. They are prepared by the American Institute, a private oganization composed of practitioners, judges, and law professors, in order to attempt to make the law uniform and to simplify it. However, it is not imperative or binding.

[58]Report of the Electronic Messaging Services Task Force, *supra note 38*, p. 1677.

At the twenty-fifth session of the Working Group on Electronic Data Interchange[59], it was generally agreed that a possible rule should make it clear that a functional acknowledgment, the purpose of which was merely to indicate that a message had been received, was not intended to carry any legal effect as to the possible formation of contract by means of electronic communications. In no instance, unless expressly agreed by the parties, should an acknowledgment of receipt be confused with any decision on the part of the receiving party to agree with the content of the message.

But, apart from the evidential consequences as to the receiving and the accuracy of the sent message attached to the acknowledgment by the rules, the Working Group decided not to deal with the legal consequences of the acknowledgment of receipt as to formation of the contract. This should rather be dealt with by the parties themselves. But, if they fail to do it, the presumption should be that the acknowledgment does not constitute acceptance of the offer the acknowledgment purports to recognize.
Article 11 pertaining to acknowledgment of receipt, §4 reads[60]:

> (4) An acknowledgment of receipt, when received by the [sender] [originator], is [conclusive] [presumptive] evidence that the related data message has been received and, where confirmation of syntax has been required, that the data message was syntactically correct. *Whether a functional acknowledgment has other legal effects is outside the purview of these Rules*[61].

---

[59]Report of the Working Group on Electronic Data Interchange (EDI) on the work of its twenty-fifth session, New-York 4-15 January 1993, A/CN.9/373, at 90.
[60]Model Electronic Data Interchange Agreement and Commentary, *supra note 20.*
[61]*emphasis added.*

1.3. The correspondence between the offer and the acceptance

For a contract to emerge, the acceptance has to agree to the offer entirely. The mutual assent has to be perfectly symmetrical, so that both parties have clearly agreed to all terms. Article 2, however, recognizes a contract where it is unclear that the parties have assented to all terms: U.C.C. §2-204 (3) states that "Even though one or more terms are left open a contract for sale does not fail for indefiniteness if the parties have intended to make a contract and there is a reasonably certain basis for giving an appropriate remedy".

A difficulty in electronic communications is not only in showing assent to be bound, but also in assenting on the same thing. One must avoid ambiguity on what is assented to. For example, in an interactive, "real-time" mode, the actor engages in a series of queries and responses, as between a customer and an automatic teller machine. A buyer might, for instance, first indicate ten widgets, and then change it to five. To clarify assent, the system might ask, "You have selected five widgets for a total of $500. Is this order correct? Enter Yes or No. The buyer would then have to enter the word "Yes" to show assent. To prove that assent did occur, the system should retain a secure record that permits reconstruction of the information displayed to the buyer and his response. It might not be enough for a system to tell an unsophisticated consumer that a transaction is subject to particular terms that are available somewhere (perhaps in a database) but which have not specifically been displayed to the consumer. As a logical matter, this should be enough, but as a practical matter the consumer might claim he just did not see, understand, or assent to the terms. To foreclose such a claim, Benjamin Wright advocates the system be designed not to execute a transaction until

terms have been displayed to the consumer or the consumer has actively indicated that he is aware of the most important terms and is aware that he can be given access to all the terms upon request all the terms upon request[62].

Conclusion Part 1

It is therefore agreed that electronic messages are capable of showing the "assent" of the parties. Unless the parties have agreed that an acknowledgment of receipt is required to give legal effect to the message, the sending party will be committed by the mere dispatching of its message (offer or acceptance) since its assent to be bound will be presumed (as long as the message actually comes from the sender).

Considering that the law is tolerant of the manner in which the offer and the acceptance are transmitted as soon as they sufficiently reveal the agreement, it is therefore possible to make an offer and to accept it through electronic messages. The contract formed by this way is valid at law.

However, to remove any doubts as to their intent to be bound by electronic transmissions, parties who are in a long-lasting trade relationship and who have the possibility to draft a trading partner agreement, are advised to include their desire to trade electronically and be legally bound by the consequences, like the ABA Model Agreement does, for instance[63].

---

[62]Benjamin Wright, *supra note 35*, §5.4.

[63]*See*, for an exemple, the recitals of the ABA Model Agreement, which states: "[The parties] desire to facilitate purchasa and sale transactions ... by electronically transmitting and receiving data in agreed formats in substitution for conventional paper-based documents and to assure that such transactions are not legally invalid or unenforceable as a result of the use of available electronic technologies for the mutual benefit of the parties". More specifically, §3.3.1 provides: "This Agreement has been executed by the parties to evidence their mutual

Furthermore, given that the technology exists and is quick and efficient (the computer technology has developed devices by which the sender of a message can be notified almost immediatley that its message has been recieved, and received without defects), parties are advised to require acknowledgment or verification of message receipt for a message to be deemed received and to have any legal effect. Yet, this acknowledgment must not be confused with an acceptance. The parties should agree on what will be deemed an appropriate acceptance leading to the formation of an electronic contract. In order to avoid misunderstandings, the offeree, when accepting an offer, should be clear enough by distinguishing it from a mere acknowledgment of receipt.

But the law itself should be adapted to this new way of contracting and should make it clear, following the example of article 12 of the DMSP, that a contract is not void merely because it has been formed via electronic messages. What is more, taking into account that computer technology allows for prompt and reliable verification of receipt, it should require any message to be confirmed by an acknowledgment of receipt in order to have legal consequences.

2. The time and place of formation of the electronic contract

Since parties to a transaction on the Internet are often far from each other, or, even better, since a party may move if it uses a portable computer, the questions regarding the time or the place of the formation of the contract are particular in the electronic context. It is of importance since it can have many legal consequences such as the applicable law, requirements such as

---

intent to create binding purchase and sale obligations pursuant to the electronic transmission and receipt of documents...".

taxation or registration, the competent jurisdiction, the possibility of revoking the offer or the acceptance, etc.

Within this part, the questions posed are: when is a contract created via electronic messages deemed to be definitively formed and when is it still possible to retract an offer or an acceptance; and where is the contract deemed to be formed.

2.1. The time of formation of the electronic contract and the revocation issue

2.1.1. The time of formation of the contract

2.1.1.1. Under the common law

The drafters of Article 2 of the Code specifically did not address the question of when a contract is effectively formed[64]. Consequently, in accordance with Section U.C.C. § 1-103, common law principles of contract formation continue to apply.

The Restatement (Second) of Contracts provides an effective structure for analyzing the treatment of the role of the communication medium in the contract formation process[65].

---

[64] *Cf.* U.C.C. §§2-204 et 2-206: the Code is silent on rules pertaining to the timing of contract formation[, except to the extend it provides that a contract may be formed even though the time of its making is uncertain (U.C.C. § 2-204(2)).

[65] *See* Restatement (Second) of Contracts §§ 63-65 (1981).

The Restatement distinguishes between two situations. In the first, the parties are in each other's presence and are able to communicate without any substantial lapse of time (the person-to-person framework). In the second, the parties are not in each other's presence and the means of communication used to transmit offers and acceptances result in a delay between the dispatch and receipt of those communications. In the latter situation, the common law provides the "mailbox rule", pursuant to which the dispatch of a message is effective without regard to whether a message ever reaches the other party. One key element of the theory behind this rule is that an offeror is free to specify the manner by which the offer can be accepted; by expressly or implicitly permitting acceptance to be made by mail, the offeror has chosen to bear the risk that the acceptance might be lost. The rule also covers messages transmitted by telegraph[66]: comment "e" to Restatement (Second) of Contracts §63 says the rule should also apply to messages in any public service instrumentality similar to mail or telegraph. However, the rule does not apply, when the parties are in the presence of each other, where the communication between parties is instantaneous. The "receipt rule" pursuant to which the message is effective when it actually reaches the recipient, applies in this situation. The rationales are that in this situation, (i) the offeree can accept with no risk that the offeror has already issued a revocation, and (ii) if communication fails, one or both parties will know immediately[67]. Consequently, Section 64 of the Restatement specifically acknowledges the use of technology in communication in the form of "telephone or other medium of substantially instantaneous two-way communication", such as conventional telex, and sets forth the principle that

---

[66]Restatement (Second) of Contract §63 comment a (1981).
[67]Restatement (Second) of Contract §63 comment a (1981).

communications using those technologies are governed by the same principles that apply when the parties are in presence of each other.

Which rule applies to computer communication such as the Internet? The answer will depend on whether the system is considered to be of the same nature as the mail or the telegraph or is deemed to be instantaneous as in the person-to-person framework. It seems however that there is no unanimity as to the answer among the authorities.

According to Raymond T. Nimmer, electronic contracting systems could fit into either the remote communication or the person-to-person framework.

One argument for applying the person-to-person rules to an EDI system stresses that the receipt and potential response to the receipt of an offer or an acceptance can be virtually instantaneous, especially in cases involving completely automated systems in which the two computers are essentially analogized to two human beings. The analogy fails, however, where the rationale of the "in person rule" typically does not exist. That rationale emphasizes that both parties will be aware of the break in connection and be able to respond to and remedy it.

On the one hand, this may not be the case within an electronic system. For example, in a system where acceptances are deposited in a recipient computer file for later action by a human order filler, a break in communication may never be detected by the intended recipient whose files never contain the acceptance. In such systems, the analogy to a telephone conversation does not hold because awareness of the communication being sent does not reach a human being until (or unless) the material is in the recipient computer and

displayed or printed out for action. Thus the "mail box rule" can not be relevant in such an electronic environment.

On the other hand, however, computer systems, including EDI, can be designed to circumvent the problem that neither party will be aware of the failed communication, at least indirectly. The design element entails automatic verification of receipt of the message. If such capability is designed into a system, that fact justifies applying the person-to-person rules. Where receipt verification is a part of the ordinary system, the sender will be first aware of receipt or non receipt virtually instantaneously. Depending on the verification form, the sender will also be able to ascertain whether the information was garbled or intact. In such a case, the sender may immediately correct ambiguities or failure. Therefore, courts should apply the person-to-person rules that acceptances, in order to be effective, must be received[68].

For Benjamin Wright, EDI and other electronic transactions (especially the Internet) are not perfectly instantaneous. In his opinion, messages, including acknowledgments, may take as much as a few hours to traverse stores and forward systems. In a turbulent business climate such as the international foreign exchange market, half an hour is a long duration. Therefore, the mailbox rule should be adopted there[69], even if there exist systems to be sure of the reception of the electronic message.

The proposed revision of U.C.C. Article 2, however, opted for the person-to-person framework and the application of the receipt rule. The proposed Article 2-208(a) states that the acceptance must be received: "a

---

[68]Raymond T. Nimmer, *supra note 34*, p. 223.
[69]Benjamin Wright, *supra note 35*, at §15.6.

contract is created when (1) the response is *received* by the initiating party (...) (2) the initiating party *receives* a message...".

And Article 2-208 (c) specifies that: "In determining when an electronic message sent to another party is received by that party, the following rules apply: (1) If the recipient of the record has designated an information system for the purpose of receiving such records, receipt occurs when the records enter the designated information system..."

2.1.1.2. Under the ABA Model Agreement:

The ABA Model Agreement, for its part, which deals only with EDI communications *stricto sensus,* holds clearly that an acceptance is effective only when received[70]. The grounds are that EDI has the capability to permit prompt, reliable verification that a message has been received, and that it has been received intact and without communication errors. This verification can occur immediately, and several EDI industry standards require such verification to be sent in a commercially prompt manner. If there are ambiguities or misunderstandings perceived by either party, the problems can be corrected by additional, immediate communication. If there is a failure in the communication, EDI permits one or both parties to know or have reason to know of the failure by virtue of the capability of the technology to provide timely verifications.

As a result, the Model Agreement incorporates rules that parallel those provided by common law for other types of technology which facilitate instantaneous communication.

---

[70]Report of the Electronic Messaging Services Task Force, *supra note 38*, p. 1667.

2.1.1.3. Under the UNCITRAL Draft Model Statutory Provisions:

The Working Group has included a provision in the UNCITRAL DMSP to provide a direct answer to the question of when an electronic contract should be deemed concluded. It was said to be needed "in order to provide certainty on one of the most crucial questions" of electronic contracting.

As to the time when a contract was deemed to be concluded, several possible points of time were discussed: When the acceptance of a contract offer enters the computer system of the receiver; when the acceptance is made available to the information systems, when the acceptance reaches the information system; when the acceptance enters and is recorded by the computer system of the receiver; when the acceptance is made available to the receiver's information system interpreting and processing the message; when the acceptance is recorded on the computer system directly controlled by the receiver in such a way that it could be retrieved; or when the acceptance reaches the receiver.

As an example of such a provision, the Working Group noted that article 9.2 of the "TEDIS European Model EDI Agreement" prepared by the Commission of the European Communities (May 1991), reads as follows:

> "Unless otherwise agreed, a contract made by EDI will be considered to be concluded at the time and place where the EDI message constituting the acceptance of an offer is made available to the information system of the receiver."

Furthermore, they noted that receipt rule is in line with articles 15(1) and 23 of the United Nations Sales Convention, with the draft UNIDROIT Principles, and with national legislations in a number of States.

However, the concept of "availability" of the message containing the acceptance of a contract was criticized as being unclear. Another criticism was that the concept appeared to be different from the rule applicable in general contract law, most notably the rule in article 18(2) of the United Sale Convention, according to which an acceptance of an offer became effective at the moment the indication of assent reached the offeror. It was pointed out that some of the situations dealt with by the uniform rules would also be covered by the United Nations Sales Convention and different rules on formation of contracts could create uncertainty.

The following receipt rule was finally decided upon:

> Article 12. Formation of contracts
>
> [(2) A contract concluded by means of data [records] [messages] is formed at the time when (...) the data [record] [message] constituting acceptance of an offer is received by its addressee or deemed to be received under article 13.]
>
> Article 13.Time (...) of receipt of a data [record] [message]
>
> (a) [subject to subparagraph (b) of this article,] at the time when the data [record] [message] enters the information system of, or designated by, the addressee in such a way that it can be retrieved by the addressee or when the data [record] [message] would have entered the information system and been capable of being retrieved if the information system of the addressee had been functioning properly.
>
> [(b) if the data [record] [message] is in such a form that it requires translation, decoding or other processing in order to become intelligible by the addressee, at the time when such processing is completed or at

the time when such processing could reasonably expect to be completed.][71]

In conclusion, the preferred solution seems to be the receipt rule. This rule is indeed more suitable to the computer technology since it takes into account its possibility to check that a message has been properly received and its potential to be reliable.

2.1.2. The time of effectiveness of a revocation message

According to the basic common law of contracts, an offer may be revoked at any time prior to its effective acceptance. It also can be revoked, in the case of the receipt rule, before it actually reaches the offeree. Yet, with regard to revocation, which of the rules -mailbox rule or receipt rule- does apply?

Indeed, concerning the time when the revocation message is deemed to be effective, the primary common law distinction separates cases of timing with regard to the offer (or acceptance) from cases dealing with a rejection (or revocation). In the United States, most states hold that a rejection is effective only when received by the other party[72]. In some cases, of course, a lapse of time terminates the offeree's power to accept without any specific revocation of the offer, either because the time lapse exceeded the terms of the offer or because of an unreasonable delay. For example, under the U.C.C., where the initiation of performance is a reasonable mode of acceptance, a party who has not been notified of the acceptance "within a reasonable time may treat the

[71]Model Electronic Data Interchange Agreement and Commentary, *supra note 20.*
[72]Restatement of Contracts §68. This general common law rule has been changed by statutes in some jurisdictions, indicating that revocation of an offer is effective when sent.

offer as having lapsed before acceptance[73]". In the case of express revocation of an offer, a response is received "when the writing comes into the possession of the person addressed, or of some person authorized by him to receive it for him, or when it is deposited in some place which he has authorized as the place for these or similar communications to be deposited for him[74]". The common law thus takes a different solution compared to offer and acceptance for revocation since it adopts the receipt rule. This disparity has been criticized by several commentators[75].

In the electronic context, however, neither the proposed revision of U.C.C. Article 2, nor the UNCITRAL DMSP, nor the ABA Model Agreement, seem to make a distinction regarding the effectiveness of a message purporting to revoke an offer or an acceptance. None of them deal specifically with the matter.

The proposed revision of U.C.C. Article 2 states clearly that "Electronic records exchanged in an electronic transaction are effective when received[76]". It doesn't distinguish between the messages according to their contents. "Electronic records exchanged in an electronic transaction" seems to be broad enough to encompass revocation messages.

The ABA Model Agreement is also clear in that its receipt theory applies to all electronic documents, whatever their content. As previously seen, the Model Agreement is built on an environment in which receipt

---

[73]U.C.C. §2-206(2).

[74]Restatement (Second) of Contracts §68; U.C.C. § 1-201(26).

[75]*See e.g.*, Mac Neil, "Time of Acceptance: Too Many Problems for a Single Rule" (1964) 112 U. Pa. L. Rev. 947; Sharp, "Reflexions on Contract" (1965) 33 U. Chi. L. Rev. 211.

[76]Article 2-208 of the proposed revision of Article 2.

determines the legal effect of any message transmitted by EDI (subject it be verified and properly acknowledged, but, if the receiving party fails to acknowledge, a breach of the agreement occurs, for which the receiving party may be liable in damages).

In sum, the receipt rule is the general rule for every electronic message, whatever they purport to do. This solution favors the simplicity and hence the certainty and predictability of the law. Furthermore, the hardship on the offeror at common law resulting from the fact that an acceptance, once dispatched, may render useless an offeror's attempts to revoke, is alleviated. If the revocation is received before the acceptance is received, there is no contract.

2.2. The place of formation of the contract

The place of a contract may be of relevance for certain legal purposes. For example, it might be relevant for taxation or registration requirements, and it might constitute a factor for establishing court jurisdiction or for determining the law applicable to the contract or its required form.

The determination of the place of formation of a contract may raise particular difficulties in situations involving the use of electronic communications. The transmission of electronic messages might be initiated in different places, such as a place of business of the sender, or the place where the sender held its computers, or any place from where the sender might operate, for example, by means of a portable computer. During the transmission process, particularly when third party service providers are

involved, electronic messages might travel through places that are irrelevant to the underlying commercial contract.

2.2.1 Under the UNCITRAL Draft Model Statutory Provisions

According to the Working Group, only the place where the message has been placed at the disposal of the recipient is sufficiently predictable to provide legal certainty as to the place of formation of a contract. However, devising the rule might be difficult in view of the possible involvement of several commercial parties and several third-party service providers, each of which might operate computers from different places. Exceptions need then to be made to the receipt rule for those cases where the place of receipt is not objectively determinable by the parties at the moment when the contract was formed and for those cases where the place of receipt might have no relevance to the underlying transaction. The place of formation of a contract may be determined by reference to an objective event so as to avoid being linked inappropriately to, for example, the place where computers were located. In view of the possible unpredictability regarding the place of operation of the computer facilities of the recipient, the place of business of the recipient may be a more relevant and more predictable place for the formation of a contract[77].

In view of these considerations, the drafters of the UNCITRAL DMSP choose the place of business of the recipient as being the more relevant place for the purpose of determining the place of formation of a contract:

---

[77]Report of the UNCITRAL Working Group on EDI, *supra note 58*, nº 108.

Article 12. Formation of contracts

[(2) A contract concluded by means of data [records] [messages] is formed at the (...) place where the data [record] [message] constituting acceptance of an offer is received by its addressee or deemed to be received under article 13.]

Article 13.(...) place of receipt of a data [record] [message]

(1) Unless otherwise agreed between the [sender] [originator] and the addressee of a data [record] [message] and [unless otherwise provided by other applicable law], a data [record] [message] is deemed to be received by its addressee.

(2) Unless otherwise agreed between the [sender] [originator] and the addressee of a data [record] [message] and [unless otherwise provided by other applicable law], a data [record] [message] is deemed to be received by its addressee *at the place where the addressee has its place of business;* where the addressee has more that one place of business, the data [record] [message] is deemed to be received at the place of business with the closest relationship to the content of the data [record] [message][78].

2.2.2. Under the ABA Model Agreement

The ABA Model Agreement, for its part, is silent on the place of formation of the contract when formed with EDI.

Conclusion part 2

Insofar as the applicable rules of contract formation are uncertain in their application in the electronic environment, it is presumably proper for this area to be addressed in an electronic trading partner agreement. The parties should provide that no legal obligation shall arise until receipt (receipt rule), and should define the place of formation of the contract according to

[78]Model Electronic Data Interchange Agreement and Commentary, *supra note 20.*

the place where the offeror has its main place of business - since this one doesn't move.

Taking into account the potential capability of electronic communications to assure clear and unequivocal mutual understanding (thanks to the possibility to provide quick, efficient and reliable verifications of messages) which permits them to be classify as a means of "instantaneous" communication, the law should consequently adopt the receipt rule for electronic messages, whatever their content, as particularly suitable for electronic transactions. In addition, the law should decide that the place of formation of the contract is the place of business of the addressee, for this one is well known and certain.

3. The allocation of risk and liability for failure or error in the transmission of a message

Unlike paper documents, electronic communications can theoretically be altered during transmission without leaving a trace. In communicating by electronic means, the parties may face various risks, such as failure in communication, alteration of the content of a message, delayed communication, communication of data to the wrong addressee, repudiation of the original message, temporary or permanent unavailability of electronic services...

Which party should bear the risk or liability of a failure or mistake in the transmission of a message?
One question concerns the liability for damages of a party who caused a failure or mistake in communication; another question is which party is to

bear the risk of loss resulting from a failure or error in communication where nobody is liable for the loss.

3.1. Under the common law

3.1.1 Liability for damages caused by a faulty transmission

According to the general law of contract on mistake, the sender of an offer or of an acceptance can avoid the consequences of a mistake if the receiving party had reason to know of the error[79] or if that party did not rely to its detriment on the mistaken message.
In an electronic transfer, this indicates that between buyer and seller, the sender of the mistaken message takes responsibility for its mistake if the other person relied on the message without any reason to suspect that it was a mistake. Thus, shipment of a million widgets in a transaction environment where no more than one hundred were ever ordered before may not require the mistaken buyer to pay for the excess shipment, but shipment of one hundred when the intended offer was only ten may bind the sender of the mistaken order.

The major competing loss allocation principles come from U.C.C. Article 4A which is designed to provide allocation principles applicable to funds transfers in an electronic milieu. These rules parallel common law principles, in that they absolve the party making a mistake from liability where there is no reliance (i.e., no acceptance of the payment order), but otherwise place loss on the person making an error in transmission. The

[79]Restatement (Second) of Contracts §153(b) (1981).

Article 4A rules, however, reallocate loss in cases where a security system was in place that could have discerned the error, but one party failed to comply with the system.

Indeed, it may be noted that the issue of liability is often closely linked to the observance of commercially reasonable procedures for verification and security of communication.

3.1.2. Risk of loss resulting from a failure in the transmission

It is also conceivable in electronic contracting that an intermediary can inadvertently alter a message during transmission or format conversion. Analogous problems have previously arisen where messages were communicated via telegraph companies or language translators.
Under §20(2) of the Restatement (Second) of Contracts, if at the time of the exchange one party knows of the interpretation the second places on the messages, and the second does not know of any different meaning, then the second's interpretation controls. In *Germain Fruit Co. v Western Union Telegraph Co.*[80], a seller sent a telegram offering oranges at "two sixty" (i.e., $2.60) per box. The telegraph company dropped the "two". The buyer ordered oranges based on the telegram, and the seller delivered. The buyer, claiming it understood the telegram to offer $1.60, refused to pay more. The court found the buyer had no reason to know the price was $2.60 (the well-known market value). The court said the seller could recover $2.60 per box from the buyer.

---

[80]137 Cal. 598, 70 P. 658 (1902).

Yet, when neither party is aware of the intermediary's mistake, there is a split among the authorities as to what the result should be: there exist two streams of United States case authorities. Under one group of cases, the offeror bears any loss caused by the mistake. The rationales are: (i) the offeror chose the medium of communication[81], and (ii) the intermediary is the offeror's agent[82]. But the opposing cases say that it is not fair simply to say that the offeror bears the loss. Rather, these authorities hold that the exchange did not form a contract (and the consequences should be based on that conclusion). The reasoning is that because the intermediary is not really an agent and the parties achieved no mutual assent, no contract could have been formed. The fundamental rationale for this approach to the problem comes from the fact that neither the sender nor recipient may have been at fault in creating the problem, but that some loss occurred and must be allocated to one or the other. In such case, the proper choice is to place the loss on the sender unless the recipient was in fact at fault in not recognizing that an error existed[83].

In a computer-based system, as between the primary parties, however, there does not appear to be a current common law principle requiring the adoption and compliance with a security system to detect errors or fraud. Arguably, however, the failure to electronically discern an obvious mistake in a transmitted message may cause a court to conclude that the recipient "had no reason to know" of the mistake, and that its reliance on verbatim electronic terms was not reasonable or protected. More generally, engaging in

---

[81] Ayer v. Western Union tel. Co., 79 Me. 493, 10 A 495 (1887). This rationale however collapses where the offeree is the first to use the intermediary, for example by transmitting an inquiry to the offeror.

[82] Des Arc Oil Mill v. Western Union Tel. Co., 132 ark. 335, 201 S.W. 273 (1918). The intermediary however is usually not a true agent but rather a public instrumentality.

[83] Raymond T. Nimmer, *supra note 34*, p. 239.

transactions requires, as a matter of prudent business conduct, the creation of an effective means to discover and prevent errors and fraud in the transactions.

3.2. Under the ABA Model Agreement

The ABA Model Agreement establishes a general obligation to confirm any document received. However, in the event a transmitted document is unintellegible or garbled, an acknowledgement may not be possible. To fairly divide the risks and the burdens of electronic commerce, the ABA Model Agreement provides for the following rules: If the originating party has transmitted the document, but the receiving party has failed to provide notice of the garbled transmission, the originating party's records of the content of the document shall control[84]. If nevertheless total gibberish is transmitted so that the receiving party can't identify the originating party, no responsability to respond is imposed. The provision also applies only when no acceptance document has been specified. If an acceptance document is specified with respect to a document that is garbled or unintelligible, there would be no obligation arising from such document even if it was received. According to the corresponding comment of Section 2.4, the term "unintelligible or garbled" is not intended to include documents which, when formatted for human review, are capable of being read but which contain information which the received party knows, or has reason to know, may be incorrect. Therefore, Section 2.4 is intended to apply only to unintellegible messages, incapable of having effective meaning , but which may be effectively traced to the originating party.

[84] ABA Model Agreement §2.4.

3.3. Under the UNCITRAL Draft Model Statutory Provisions

In a general way, articles 6, 7 and 8 of the UNCID rules cite the duty to observe commercially reasonable procedures for verification and security of communication.

The Working Group of the UNCITRAL DMSP suggested that the uniform rule might state the obligations of the recipient with regard to the detections of errors, the obligations flowing from the detection of an error and the consequences of the recipient's compliance, or failure to comply, with its obligations. If the recipient knew or should have known that the message was garbled or somehow impossible to process, it should be under an obligation to notify the sender. In cases where the sender did not receive such notification due to the negligence of the recipient who failed to comply with applicable security procedures or to give the required notice, the uniform rules might state the sender should be able to rely on the message as sent. In cases where the recipient notifies the sender of an error, the message might be given no effect[85].

Finally, the current version reads as follows:

> (5) Where an originator is [deemed] [presumed] to have approved the content of a data [record] under this article, it is [deemed] [presumed] to have approved the content of a data [record] as received by the addressee. However, where a data [record] contains an error, or duplicates in error a previous [record], the originator is not [deemed] [presumed] to have approved the content of the data [record] by virtue of this article in so far as the data [record] was erroneous, if the addressee knew of the error or the error would have been apparent, had the addressee exercised reasonable care or used any agreed procedure of verification.]

[85]Report of the UNCITRAL Working Group on EDI, *supra note 58*, nº 123.

[(5) bis Paragraph (5) of this article applies to an error or discrepancy in an amendment or a revocation message as it applies to an error or discrepancy in a data [record]][86].

Conclusion Part 3

A solution for the parties is to deal themselves with the manner in which the responsability of errors should be shared and what type of security or other procedure should be settled as a means to detect and prevent mistakes. Then either party's failure to conform to the procedure shifts loss to that party in compliance with the procedure that would have prevented the risk from occurring.

This is for example the result created in U.C.C. Article 4A. One part of this process, of course, involves retaining sufficient records to establish what source produced the alleged error. In addition, the risk of error issue also requires defining what responsibility the parties have for errors caused by electronic service providers hired as intermediaries for transmitting messages. The preferable approach by contract parallels the majority view in common law. If an error induces detrimental reliance, the party who chose and used the service provider bears the loss caused by its error. If both parties selected and use the service provider, the risk of error remains in the sender in cases where detrimental reliance, the party who chose and used the service provider bears the loss caused by its error. If both parties selected and use the service provider, the risk of error remains in the sender in cases where detrimental reliance occurred and the recipient had no reason to know an error occurred.

---

[86]Model Electronic Data Interchange Agreement and Commentary, *supra note 20*.

Conclusion Section 1

To the extent that applicable rules of contract formation are uncertain in their application in an electronic environment, or to the extent that these applicable rules may not yield the optimal result in an electronic environment, it is always preferable for the parties to anticipate the problems and to provide the answers as they intend in a trading partner agreement. This agreement would deal with the question of knowing when a message is deemed received, when a message is effective, giving rise to legal consequences, when and where the contract is formed. The parties may wish, for that purpose, to simply make reference to a Model Agreement, such as the ABA Model Agreement, which deals with all of those issues.

Furthermore, considering the uncertainties regarding the allocations of risk and liability in case of errors or failure in electronic communications, it is preferable for the parties to make provision for it in a trading partner agreement. If the agreement imposes an obligation on the sender to assure the completeness or accuracy of the data transmitted, the sender would then be liable in case of a failure in communication by virtue of a breach of the interchange agreement; if the agreement imposes on the receiver of the message an obligation to verify any message received and to notify the sender of any unintelligible or garbled message, the breach of this obligation would then put the risk of errors in transmission on the recipient. As for the problem of allocation of risk in the event of errors that are not the fault of either party, the rule could be that the sender is liable for errors in messages which it transmits, unless the recipient knew or should have known of the error.

In a general way, we advise the parties to require acknowledgment or verification of message receipt in their interchange agreement. Indeed, the requirement of verification solves several issues at the same time: (1) the question of the efficacy of an original message in the event of non-acknowledgment and the obligations on each party if no anowledgment is sent; (2) the issue as when a message is deemed received; and (3) the question of the allocation of the risk of errors.

However, if legal rules governing contract formation by electronic means were clarified, the need for such provisions would be eliminated. The law should thus provide for provisions that expressly deal with the contract formation by electronic means. It should make it clear that:

(1) a contract can legally be formed through electronic messages;

(2) the contract is formed when the offeree receives the offeree's electronic message purporting to accept the offer;

(3) it is then deemed to be formed when the offeree actually receives the acceptance and at the place of its main place of business;

(4) the risk of the transmission -failure or error in the transmission of the message- is on the sender unless the addressee knew or should have known the error or failure occurred.

SECTION 2- THE ENFORCEABILITY OF THE CONTRACT: FORM REQUIREMENTS

The main concern of the parties when they contemplate an electronic transaction is its validity and its enforceability. One of the most obvious issues relating to paperless transactions is whether they comply with statutory requirements for documents in writing. The difficulties arise primarily in satisfying Statute of Frauds limits on the enforceability of contracts. So far, there appear to be have been no reported decisions in the Commonwealth or in the United States that directly consider the enforceability of electronic contracts.

One of the primary goals of electronic messaging is the elimination of paper transactions, which ultimately means the elimination of conventional writing.

However, U.C.C. Section 2-201 Statute of Frauds requires that, in any contract for the sale of goods for $500 or more, there must be: (i) a writing, (ii) containing a quantity term, (iii) sufficient to indicate that a contract has been made, (iv) and signed by the party against whom enforcement is sought. In an electronic environment, these restrictions create problem as to the existence of a "writing" and as to the requirement of a "signature" by the party against whom enforcement is sought.

Judicial interpretation has made it clear that the effect of this Section is not to render unwritten agreements void or illegal but unenforceable. However, in the context of electronic transactions, the objective will most likely be to enforce agreements between trading partners. Interestingly, as

long ago as 1677, it was held that a writing need not be in any particular form to satisfy the Statute, although at that time electronic transactions were surely never contemplated[87]. None of the cases that have considered the sufficiency of a "writing" have had to look at anything other that some form of paper document. Instead, the cases have been more concerned with the content of documents and whether they are sufficient under the Statute.

The issues concerning electronic contracts can be grouped into three questions:

- Is a particular contract within one of the classes governed by the Statute of Frauds?
- If it is, does a given sequence of electronic transmissions constitute compliance?
- If not, what are the implications?

In many cases, however, U.C.C. Section 2-201 need not to be complied with. Its practical effect is limited by exceptions contained within its terms, and by non statutory exceptions created by the courts.

The exceptions set forth in U.C.C. Section 2-201 itself, are: (i) between merchants, in the event a party sends a signed confirmatory writing to the other party, sufficient to satisfy §2-201, such writing is acceptable against the receiving party if that party has "reasons to know its contents" and does not object to those contents within 10 days of receipt; (ii) where the seller significantly relies on a contract to manufacture special goods for the buyer; (iii) where a party admits in its pleadings, testimony or otherwise in court

---

[87]Brian D. Grayton, "Canadian Legal Issues Arising from Electronic Data Interchange" (1993) 27 University of British Columbia Law Review 257, p. 264.

that a contract for sale was made; and (iv) where payment has been made and accepted or where goods have been received and accepted.

The non statutory exceptions most often recognized by the courts result from the application of the estoppel doctrine. A plaintiff trying to prevail over a defendant assertion of the Statute of Frauds must demonstrate that (i) a promise to perform was made by the defendant, (ii) the plaintiff reasonably relied on the promise, and (iii) some type of unconscionable injury or unjust enrichment must result from a refusal to enforce the underlying contract[88]. The Restatement also specifically allows the assertion of estoppel to circumvent the requirements of the Statute of Frauds[89].

Furthermore, in the international context, many conventions, and in particular the Convention on the International Sale of Goods[90], have excluded the concept of a Statute of Frauds from many international goods of sales[91].

Finally, the Statute of Frauds mainly applies to sale of goods for $500 or more and to consumer transactions.

In addition to the U.C.C., most States have some form of Statute of Frauds governing contracts that cannot be fully performed within one year. [92]

---

[88]*See* International Prods & Technologies, Inc.v. Iomega Corp., 1995 WL 138866 (E.D. Pa. 1989); Lige Dickson Co., v. Union Oil Co., 635 P. 2d 103 (Wash. 1981).

[89]Restatement (Second) of Contracts §139 (1981).

[90]Convention on the International Sale of Goods, article 11: *cf.* Nicoll Christopher, "EDI Evidence and the Vienna Convention" (1995) 95 The Journal of Business Law 21.

[91]Braustein , "Remedy, Reason, and the Statute of Frauds: A Critical Economic Analysis" (1989) 1989 Utah Law Review 383.

[92]*See* the federal Statute of Frauds, 31 U.S.C.A. §15019 (1986); the Controlled Substances Act, 21 U.S.C.A. §802 et seq. requires a specific written form for sale of a dangerous pharmaceutical; the Fair Labour Standards Act, 29 U.S.C.A §§212(a) et 215(a)(1) (1973) reqauires written assurances of compliances with wage-hours laws of sellers and resellers.

1. The writing requirement

1.1. Under the common law

Conventionally, writing means reducing words to paper. Yet the term "writing" is abstractly understood to embrace more than just "ink on wood fibers"[93]. According to the U.C.C. Section 1-201(46) "'written' or 'writing' includes printing, typewriting, or any other intentional reduction to tangible form". Evidently, the word "includes" allows for other means of producing a tangible document. In approving a pencil as a proper instrument for writing, the court in *Clason v. Bailey*[94] held a writing must be visible to the eyes and suggested it must be durable. Hence the significant feature of the definition of a "writing" deals with the reduction to tangible form. Thus, at least as to the writing element, the sufficiency of the electronic message depends on the manner in which one finds it stored or produced.

A parallel can be drawn with other technologies. The introduction of the telegram and the telex, both involving the communication of a series of electrical impulses, did not present an insurmountable difficulty to the courts in concluding that a sufficient writing existed. In *Selma Sav. Bank v. Webster County Bank*[95], the court accepted a telegram, the content of which had been orally provided to Western Union by telephone, as a writing effective as an acceptance of a negotiable instrument, having recognized that, in fact, the initiating party had not actually transmitted or provided a physical piece of paper. The court quoted *Howley v. Whipple*[96], as follows:

---

[93]Benjamin Wright, *supra note 35*, at §16.4.
[94]14 Johns. 484 (N.Y. 1817). Also U.C.C. §2-201 official Comment 1 recognizes pencil.
[95]182 Ky. 604, 206 s.W. 870 (1918).
[96]48 N.H. 487 (1869).

> "When a contract is made by telegraph, it makes no difference whether the operator writes the offer or the acceptance in the presence of his principal and by his express direction, with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire of thousand miles long (...) nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office".

At least one court has also accepted a tape recording as an adequate "writing", where both parties knew the tape was being made to record their discussion[97]. In recent decisions under decisions under the Statute of Frauds, where the writing in question consisted of a telecopy, the courts have accepted the telecopy as a "writing" without questioning that result[98].

Systems that routinely yield printed output similarly satisfy the writing concept, whether that output occurs at the receiving point or in a functional acknowledgment returned after receipt[99]. If the transmission came from a written document, that writing may be adequate[100],

The comparability of electronic communications to these other technologies is of interest. Nevertheless, courts and authors do not agree as to the conclusions to be drawn.

In Raymond T. Nimmer's opinion, in purely electronic transmissions that do not begin or result in printed or other tangible manifestations required for the Statute of Frauds, the enforceable status of the transactions remains unclear. This status will depend on how the computer systems retain records of the transmitted offer (or acceptance) and whether a court will accept

---

[97]Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212, 11 U.C.C. Rep. Serv. 443 (D. Col. 1972).

[98]International Prods. & Technologies, Inc. v. Iomega Corp, 1989 U.S. Dist. LEXIS 13589 (E.D. Pa. 1989); Bazak Int'l Corp. v. Mast Indus. Inc., 73 N.Y. 2d 113, 535 N.E. 2d 633.

[99]Sumitomo Marine & Fire Ins. Co., Ltd. v. Cologne Reinsurance Co. of Am., 552 N.E.2d 139 (N.Y. 1990).

[100]Raymond T. Nimmer, *supra note 34*, p. 227.

the idea that electronic records reduce the message to "tangible form." There is no unanimity among the courts. Some United States federal courts, in dealing with criminal law prosecution, conclude that modern electronic technology requires treating electronically stored information as tangible in all respects, while other courts expressly reject that ruling. In a civil court setting, electronic storage in discernible form should be sufficient. Where the messages at both ends of the contracting chain yield information fully integrated into the database of the relevant computer and not discernible as a discrete offer or acceptance, however, the tangibility requirement is not met. The idea of the statute is to provide a discernible record of the transaction, and fully integrating data into a broad database loses that capacity[101].

Robert W. McKeon, for its part, draws a parallel with the Copyright Act of 1976. A tangible medium, for the purpose of the Copyright Act of 1976, includes any means of expression from which copyright material can be perceived, reproduced or otherwise communicated, either directly or with the aid of a machine or device[102]. The tangible medium must be able to contain a "fixed" work for longer than just a transitory period[103]. Therefore, an electronic message stored (or "fixed") on the hard disk drive of a computer (or other means) should be a sufficient "tangible form" to qualify as a writing under the U.C.C., especially when the U.C.C.'s principle of liberal construction is applied[104].

---

[101] *Id.*

[102] 17 U.S.C. §102(a) (1988).

[103] 17 U.S.C. §101 (1988).

[104] Robert W. McKeon, "Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena" (1994) 12 Journal of Computer & Information Law 511, p.531.

A significant case involving non-traditional writings is *People v. Avila*[105]. In Avila, the court found a lawyer, who falsified the driving records of his clients, guilty of forgery. The driving records were recorded on computer disks, and culpability under the statute required the falsification of a written instrument (defined as "any paper, document or other instrument containing written or printed matter or the equivalent thereof..."). The court held that computer disks satisfy the definition of a written instrument, and the lawyer's conviction was affirmed.

1.2. Under the ABA Model Agreement

According to the ABA Report, telegrams, telexes, telecopies, which all involve the transmission of a message by a series of electronic impulses are similar to electronic messages. They do differ in that their transmissions always result in a writing whereas, whether an electronic transaction results in a printout depends upon whether the receiver wants one. But the relevant point, from the Statute of Frauds perspective, is that electronic messages have the capacity to produce a writing on request. Telegrams, telexes and telecopies have all been accepted as offering circumstantial guaranties of trustworthiness equivalent to those that a writing provides. Thus, a similar result with respect to electronic messages should not be unexpected. Indeed, the records of electronic transactions show potential for reliability and accuracy that is equivalent to the records maintained with regard to the use of the other technologies. The records are retained on a form of media (magnetic tapes or disks) which are identical to the type of media used to record oral conversations, a form which has been accepted as a "writing" in other

[105]770 P.2d. 1330 (Colo. App. 1988).

instances. This message, however stored, constitutes objective, corroborating evidence which demonstrates the possible existence of a contract. Thus, the evidentiary purpose of the writing requirements is met[106]. Therefore, assuming use of reliable record retention procedures, electronic transactions should be, according to the ABA Report, equivalent to a Statute-of-Frauds writing.

The Report seems to argue that a record is a condition to an electronic message satisfying the Statute of Frauds' writing requirement. However, as Benjamin Wright notes, it is then curious that §3.3.2 of the ABA Model Agreement defines "writing" as electronic messages that have only been properly transmitted rather than transmitted and recorded. Under the ABA Model Agreement the writing "requirement is intended to be satisfied by the transmitted [message] itself, regardless of the medium by which the record of the transmission is established and maintained." The ABA Report does not recognize this inconsistency[107].

1.3. Under the UNCITRAL Draft Model Statutory Provisions

The UNCITRAL Working Group for Electronic Data Interchange, for its part, when dealing with the definition of an "electronic writing", considered two possible approaches: one possibility would have consisted in extending the definition of a "writing" to encompass electronic messages; the other one would have been to adopt a "functional equivalent" approach[108]. This latter consists of identifying the essential functions that are traditionally

---

[106]Electronic Messaging Services Task Force, "The Commercial Use of Electronic data interchange- A Report" (1990) 45 The Business Lawyer 1647, p. 1686.
[107]Benjamin Wright, *supra note 35*, at §16.4.5.1.
[108]Report of the UNCITRAL Working Group on EDI, *supra note 58*, nºs 50 req.

fulfilled by writing, with a view to establishing the conditions under which electronic messages would be deemed to fulfill those functions and thereby receive the same legal recognition as paper documents.

The view was expressed, however, that it might be inappropriate to adopt for general use a definition of "writing" that might overly stretch the common understanding as to what "writing" consisted of, because such an extended definition might lead to the undesirable result of validating the dematerialization of instruments for which States might wish to maintain the paper-based form. Thus they preferred the "functional approach".

The following functions of a writing were listed: (1) to provide that a document would be legible by all; (2) to provide that a document would remain unaltered over time and provide a permanent record of a transaction; (3) to allow for the reproduction of a document so that each party would hold a copy of the same data; (4) to allow for the authentication of data by means of a signature; and (5) to provide that a document would be in a form acceptable to public authorities and courts In addition, the following functions were suggested as characteristics of writing: (6) to finalize the intent of the author of the writing and provide a record of that intent; (7) to allow for the easy storage of data in a tangible form; (8) to ensure that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves; (9) to help the parties be aware of the consequences of their entering into a contract; (10) to facilitate control and subsequent audit for accounting, tax or regulatory purposes; and (11) to bring legal rights and obligations into existence in those cases where a writing was required for validity purposes. Finally, the UNCITRAL article reads as follows:

Article 6. [Functional equivalent] [Requirement] of "writing"

(1) Where a rule of law requires information to be presented in writing, or provides for certain consequences if it is not, that requirement shall be satisfied in relation to a data [record] containing the requisite information if:

(a) the information can be [reproduced] [displayed] in [visible and intelligible] [legible, interpretable] [durable] form; and

(b) the information is preserved as a record[109].

Thus, both the ABA Model Agreement and the UNCITRAL DMSP assert that the record of an electronic message can constitute a valid Statute-of-Frauds writing as long as the record retention procedure shows reliability and accuracy.

2. The signature requirement

In addition to the necessity for "written" documents, the Statute of Frauds also required that they be "signed" by the party against whom enforcement is sought. To what extent can a message which is solely in electronic form can be deemed to contain a "signature"?

2.1. Under the common law

U.C.C. Section 1-201(39) defines "signed" as including any "symbol executed or adopted by a party with present intention to authenticate a writing".

---

[109]Model Electronic Data Interchange Agreement and Commentary, *supra note 20.*

Therefore, in determining whether a contract was signed by the party against whom enforcement is sought, as required by the U.C.C. Statute of Frauds, the writing must show the requisite intent: the party must have had the "present intention to authenticate a writing".

Meanwhile, a comment to Section 2-201, states that a writing must be "'signed'...which includes any authentication which identifies the party to be charged[110]." Thus, the purpose of a signature is twofold: (i) authentication, and (ii) identification of the parties.

Both parts are necessary. Authentication indicates that a document, is what it purports to be - a contract for the sale of goods. Identification of the parties goes to the issue of liability for the terms of the contract set forth in the document.

Whether a particular "signature" was intended to authenticate a document is a question of fact[111]. A comment to Section 1-201 of the U.C.C. explains:

> "The inclusion of authentication in the definition of 'signed' is to make clear that as the term is used in this Act a complete signature is not necessary. Authentication may be printed, stamped, or written; it may be by initials or by thumbprint. It may be on any part of the document and in appropriate cases may be found in a billhead or letterhead. No catalog of possible authentications can be complete and the court must use common sense and commercial experience in passing upon this matter. The question always is whether the symbol was executed or adopted with present intention to authenticate the writing[112]."

---

[110] U.C.C. §2-210 Official Comment 1.

[111] *See*, e.g.,Vess Beverages, Inc. v. Paddington Corp., 886 F.2d 208, 213 (8th Cir. 1989).

[112] U.C.C. §1-201 Official Comment 39.

Moreover, the authorities have tended to disregard irregularities in form and to be very liberal in determining what constitutes a Statute of Frauds signature.

The established rule is that a signature is whatever symbol, mark or device one chooses to use as a representative of himself[113] There is no requirement that the signature be in any particular form[114]. By custom and usage, any mark which has a token of knowledge, approval, acceptance, or obligation has come generally to mean the person's name as if he wrote it himself[115]. What kind of instrument a party uses to make his signature is immaterial. The signature may be handwritten, printed, stamped, typewritten, engraved, photographed, or even cut from one instrument and attached to another[116]. A person signs a writing by attaching his name to the writing in some manner with the intention of signing it.

The essence of signature is the intent to use it (whatever it happens to be) to adopt or approve a writing. The courts have proved to be pragmatic. *Kohlmeyer & Co. v. Brown*[117] involved a confirmation statement, for a sale of securities, written on a fill-in-the-blank form that contained the printed name and logo of the seller but no separate signature. The court held the printed name constituted the seller's signature because that was the intent evident from the form's use. *Interstate United Corp. v. White*[118] examined whether a seller had signed a contract for the sale of business assets. The seller had affixed no discrete symbol that might be construed as a signature. The

---

[113]Joseph Denunzio Fruit Co. v. Crane, 79F. Supp. 117, 128 n.16 (S.D. Cal. 1948).
[114]Hessenthaler v. farzin, 564 A.2dn990, 993 (Pa. Super. Ct. 1989).
[115]*Crane*, 79 F. Supp. at 128 n.16.
[116]*Id.*
[117]126 Ga. App. 700, 192 S.E.2d 400 (1972).
[118]388 F.2d 5 (10th Cir. 1967).

court held, however, that the seller's conduct, rather than any written symbol, amounted to authentication. The conduct was the seller's preparation of a final draft of the contract and supporting papers, its requiring that the buyer obtain a certain consent to fulfill the contract, and its sending of certain letters to suppliers.

Still, the intent to sign or authenticate must be clear. A name in a recital on a document is not necessarily sufficient[119]. According to Benjamin Wright, one way to help to make intent clear in electronic messages would be to use words that show intent. Thus, the intent to sign an electronic mail message with plain text characters is more clear if the message says "Signed: John Doe" or "My name appearing at the end of this message is my signature."

The Restatement (Second) of Contracts adopts a similar approach. Section 134 states that a signature may be any symbol made or adopted with an intention, actual or apparent, to authenticate the writing as that of the signer[120]. The signature needs not to be put at the foot of the memorandum, but must be made or adopted with the declared or apparent intent of authenticating the memorandum as that of the signer[121].

Courts have consistently held that a sufficient signature may exist in telexed or telegraphed documents[122].

In *Joseph Denunzio Fruit Co. v. Crane*[123], a federal district court held that a teletyped message satisfied the California Statute of Frauds. The court explained that both parties had teletype machines, so as one machine was operated, the message would simultaneously be typed by the other machine.

---

[119]Lee v. Vaughn *Seed* Store, 101 Ark. 68, 141 S.W. 496 (1911).

[120]Restatement (Second) of Contracts §134 (1981).

[121]*Id.* at Comment b.

[122]*Crane*, 79F. Supp. 117, 129 (S.D. Cal. 1948); *Farzin*, 564 A.2dn990, 994 (Pa. Super. Ct. 1989).

[123]79F. Supp. 117 (S.D. Cal. 1948).

In addition, "each party was readily identifiable and known to the other by the symbols or code letters used." In addressing what constitutes a "signature" for purposes of the Statute of Frauds, the court stated that it "must take a realistic view of modern business practices, and can probably take judicial notice of the extensive use to which the teletype machine is being used today among business firms, particularly brokers, in the expeditious transmission of typewritten messages."

In *Hessenthaler v. Farzin*[124], the Pennsylvania Superior Court held that a mailgram was a "signed" writing as contemplated by the Statute of Frauds. The court recognized similarities between the paperless methods of communication:

> "Although the issue [of whether a mailgram satisfies the Statute of Frauds] is one of first impression in Pennsylvania, these types of questions are likely to arise with greater frequency in the future, as businesses and individuals increasingly rely on similar methods of negotiation such as electronic mail, telexes and facsimile machines in conducting their business affairs".

The court stressed that neither the statute nor case law requires a signature to be in any particular form. In fact, given the many types of signatures that courts have found to be valid, insisting on a traditional form of signature would be too rigid. A more realistic approach in determining whether a party intended to authenticate through a particular mark is to consider the reliability of the writing or memorandum. The court held that the mailgram, which stated: "We, Dr.Mehdi and Marie Farzin, accept the offer of $520,000 for our property at 6175 and 6185 Hocker Drive, Harrisburg, Pennsylvania," had such precise detail that there was little question of its reliability. The court noted that the sellers carefully identified themselves at the beginning of the mailgram, clearly expressed their intent to accept the offer, and carefully

---

[124]564 A.2dn990, 990 (Pa. Super. Ct. 1989).

described the property and consideration involved. For purposes of the Statute of Frauds, the court held that the mailgram was a "signed" writing because it sufficiently revealed the seller's intention to adopt the writing as their own.

The court's analysis focused on the reliability of the document as a whole as meeting the signature requirement of authenticity rather than on one, specific symbol.

2.2. Under the ABA Model Agreement

According to the ABA Report[125], with electronic transactions, the act of initiating the transmission of a message is comparable to transmission by telegrams, telexes, and telecopies. In all instances, a message is composed (either manually or by computer application) and the message is entered for transmission. The transmitted messages similarly contain information identifying the source of the message either in the content of the message itself or in circumstances surrounding its transmissions[126]. In most cases, it will be reasonable to conclude that the initiating party used an identifying symbol affixed to or contained in the message with the requisite present intention to authenticate the writing in accordance with the Code.

However, a court is instructed to "use common sense and commercial experience in passing upon these matters": whether the imprint or electronic "envelope" identification is acceptable will require a finding on a case-by-case basis of the requisite intent.

---

[125]Report of the Electronic Messaging Services Task Force, *supra note 38*, p. 1687.

[126]Most commercial telecopiers receiving transmissions will imprint the date, name of the originating party, and the phone number from which the message was transmitted upon the paper document at the receiving end. With EDI, the name of the originating party is generally contained in the electronic "envelope" in which individual messages are collected and transmitted and is often a data element of the particular message.

2.3. Under the UNCITRAL Draft Model Statutory Provisions

As for the writing problem, the UNCITRAL Working Group decided to adopt a functional approach to the problem of the signature in an electronic environment[127], rather than trying to extend the definition of the "signatures".

The functions traditionally performed by a handwritten signature on a paper-document were said to be mainly the following: (i) to indicate to the recipient of the document and to third parties the source of the document; (ii) to indicate that the authenticating party approved the content of the document in the form in which it was issued and intended to be bound by the content of the document.

But rather than defining which electronic means of authentication used in electronic communication could constitute a valid substitute for "signatures" in the electronic environment when it was required by a statute, the Working Group chose to establish the general conditions under which electronic messages would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements that currently presented barriers to electronic commerce. Indeed, there are many possible means to authenticate electronic messages and new means will certainly evolve in the future. What is more, it would then not limit the contractual freedom of the parties to agree on any method of authentication. Hence it was said more appropriate to provide authentication criteria that would be sufficiently flexible to meet the needs of practitioners.

---

[127]Report of the UNCITRAL Working Group on EDI, *supra note 58*, nºs 63 et req.

In accordance with this view, they laid down that a message should be regarded as authentic provided that it was authenticated by a method that was commercially reasonable under the circumstances. But again, the Working Group decided not to attempt to defining the "commercial reasonableness" of an authentication procedure by any reference to any specific technique for they will evolve in the future.

In determining whether a method of authentication is commercially reasonable, factors to be taken into account were said to include the following: (1) the status and relative economic size of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial transactions took place between the parties; (4) the kind and size of the transaction;(5) the status and function of signature in a given statutory and regulatory environment; (6) the capability of the communication systems; (7)the authentication procedures set forth by communication system operators; and (8) any other relevant factors.

Finally, the article pertaining the functional electronic equivalent of "signatures" when required by a statute reads as follows:

> Article 7. [Functional equivalent] [Requirement] of "signature":
>
> (1) Where a rule of law requires information to be signed, or provides for certain consequences if it is not, that requirement shall be satisfied in relation to a data [record] containing the requisite information if:
>
> [(a) a method [of authentication] identifying the originator of the data [record] and indicating the originator's approval of the information contained therein has been agreed between the originator and the addressee of the data [record] and that method has been used; or]
>
> (b) a method [of authentication] is used to identify the originator of the data [record] and to indicate the originator's approval of the information contained therein; and
>
> (c) that method was as reliable as was appropriate for the purpose for which the data [record] was [generated or communicated] [made], in the

light of all circumstances [, including any agreement between the originator and the addressee of the data [record]][128].

Therefore, both the ABA Model Agreement and the UNCITRAL DMSP argue that an electronic message can constitute a valid Statute-of-Frauds signature if the parties have used an agreed method of authentication determining which symbols affixed to or contained in the message actually identify themselves.

Conclusion Section 2

The current language of the U.C.C. is ambiguous on whether a computer communication fulfills the Section 2-201 Statute of Frauds writing and signature requirements. While no case has challenged the enforceability of such a contract, the increasing use of computer messaging suggests that disputes will inevitably arise.

Nevertheless the purpose and policy of the U.C.C., as defined in Section 1-102, is to "simplify, clarify, and modernize the law governing commercial transactions" and to "permit the continued expansion of commercial practices through custom, usage, and agreements of the parties". And the American Bar Association's Article 2 Study Committee is currently engaged in a study of the issues arising out the inadequacy of Article 2 in light of today's technology.

Pending U.C.C. revisions suggest a completely different approach to the idea of a writing or a written document. Considering that electronic records not only supplement written documents, but supplant them in many cases, and that there should be no dispute in law that the electronic equivalents are

---

[128]Model Electronic Data Interchange Agreement and Commentary, *supra note 20.*

adequate, the use of writing is therefore replaced throughout the drafts by a new term: record.

The definition of "records" states: "'Record' means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." This language draws in part from copyright law concepts about when a work of authorship is fixed in a tangible medium of expression. It does not require particular forms of authentication or methods of reproduction. This is consistent with the idea that evolved in reference to written works which are writings whether signed, sealed or otherwise authenticated.

In addition, as for the electronic Statute of Frauds the terms of proposed sales revisions state that a record can be authenticated in any form which is reasonable under the circumstances, including prior agreements of the parties. This creates the most open-ended standard possible and leaves open to judicial review any further refinement of the law of electronic signature.[129]

But for the time being, most trading partners got used to consider the issues regarding compliance with the Statute of Frauds. Some of them adopt a "waiver strategy" setting forth, in one form or another, a waiver of the applicability of the Statute of Frauds. In some instances the agreements include a covenant not to assert a defense based upon the Statute of Frauds. Any claim that the failure of the content of the electronic message to be in writing and signed by the party to be charged would constitute such a defense. Second, and sometimes not exclusive of the former, agreements use a "definition strategy", providing that the electronic communication constitutes "writing" that are to be considered "signed" by the parties. In

[129]Raymond T. Nimmer, *supra note* 34, p. 230.

many instances, the agreements specifically provide that the use of a user access code in conjunction with any transmission constitutes a "signature" for the purposes of the Statute of Frauds[130].

As for the different model agreements[131], varying approaches are adopted concerning the way they comply with writing and signing requirements. Virtually, every model agreement addresses the writing problem, although the strategies adopted are different.

Some agreements define the electronic transmission to bring it within the definition of a "writing" and to satisfy the definition of a "signature[132]. The ABA model Agreement, for example, states that any document that has been properly transmitted pursuant to the terms of the Model Agreement, is defined to be a "writing" or "in writing"[133]. In addition, it describes a "signature" as any identifications consisting of symbols or codes that are adopted by a party and electronically affixed to or contained in documents transmitted by such party[134]. Then the Model Agreement combines the "writing" and "signature" concepts and provides that any "writing" containing, or to which is affixed, a "signature" shall be deemed for all purposes (i) to be "signed" and (ii) to constitute an original when printed

---

[130]This is the result of the study conducted by the Electronic Messaging Services Task Force in thepreparation of the model Trading partner Agreement, "The Commercial Use of Electronic Data Interchange- A Report" (1990) 45 The Business Lawyer 1647, p. 1680.

[131]*See* Introduction.

[132]*See* e.g., Australia Interchange Agreement clause 3.3 and 3.4: "any message to which a signature is affixed shall be deemed to be in writing, signed, and to constitute an original", Model Electronic Data Interchange Agreement and Commentary, prepared by the legal subcommittee advising the EDI Council of Australia, version 1, October 1990; canada Interchange Agreement §6.04: "electronic document shall be deemeed to constitute a writing signed and delivered by the sender", Model Form of Electronic Data Interchange Trading Partner Agreement and Commentary, prepared by the Legal and Audit Issue Committee of the EDI Council of Canada, 1991; ABA Model Agreement §3.3.2.

[133]ABA Model Agreement §3.3.2.

[134]ABA Model Agreement §1.5.

from electronic files or records established in the normal course of business. Thus, a properly transmitted document reflecting the signature of the transmitting party should be sufficient to satisfy the formal requirements of the Statute of Frauds[135].

Other agreements state that the electronic transmission "shall have the same force and effect" as a paper transmission[136]. The South African agreement, for instance, contains a provision that each party "guarantees" the binding nature of each electronic transmission[137]. In other interchange agreements, the parties similarly recognize the validity and enforceability of electronic messages[138]. The ABA Model Agreement, for example, establishes the basis for either party to assert estoppel in order to bar reliance upon the Statute of Frauds: Section 3.3.4 contains a promise by each party not to contest the validity the validity or enforceability of "signed documents" under the provisions of the applicable law relating to whether agreements be in writing or signed by the party to be bound thereby.

A different tactic, used in combination with those described above, is for the parties to agree not to contest the validity or enforceability of an electronic

---

[135]Report of the Electronic Messaging Services Task Force, *supra note 38*, p. 1691.

[136]*See* e.g., the UK Interchange A greeement §5: the parties agree to accord electronic messages "the same status as would be applicable to a document or to information sent other that by electronic means", EDI Association Standard Electronic Data Interchange Agreement, prepared by the EDI association of the United Kingdom, 2nd ed.August 1990. *See* also TEDIS European Agreement, article 10: "messages shall have comparable value to that accorded written documents", TEDIS Programme European Model EDI Agreement, prepared by the Commission of the European Communities, DG XIII-D (May 1991).

[137]South Africa Model Agreement §12.1, Model Interchange Agreement, prepared by the Organization for the Simplification of International Trade Procedures in South Africa, March 1991.

[138]FINPRO Model Agreement §8, Model Agrrement on Transfer of Data in International Trade, agreed upon by the Republic of Finland and CMEA Members States (1991); Quebec Agreement §6.3(1), standard Interchange Agreement, prepared by the Ministry of Communication of the Province of Quebec, Canada, September 1990; TEDIS European Agreement, §10, TEDIS Programme European Model EDI Agreement, prepared by the Commission of the European Communities, DG XIII-D (May 1991); ABA Model Agreement §3.3.1.

transaction[139] nor object to the introduction of evidence of the electronic transaction[140]. Additionally, some of the model agreements acknowledge the importance of the parties conduct and performance under the agreement as demonstrating their intent to be bound by the electronic transaction[141].

The issues, however, are not yet resolved. It is thus recommended that the parties agree in advance in their interchange agreement what means of authentication they will be using, what personal identification numbers or similar authenticating codes will be sufficient to serve as "signatures". The agreement may provide that the parties not challenge the validity of electronic merely on the basis that they are in electronic form, that the parties accord electronic messages the same status as paper messages.

However, again, in order for the law to accommodate to electronic transactions the laws should state expressly that:

(1) a contract is not unenforceable by the mere fact that it exists only in electronic form under the pretext that it doesn't comply with the Statute-of-Frauds;

(2) a reliable record of an electronic message is to be considered as a "writing" (the term "record" being substituted to the term "writing" since a new logic is needed to fit to this new technology);

(3) any computer control techniques -including acknowledgments, passwords, cryptography...- that can reveal the intent of the sender is to be considered as a "signature", this latter not being needed anymore (in its strict meaning).

---

[139]TEDIS Model Agreement §9.1: the parties accept that transactions are validly formed through electronic exchange of messages and waive right yo contest validity of electronic transaction.

[140]Australia Interchange Agreement §3.4, Model Electronic Data Interchange Agreement and Commentary, prepared by the legal subcommittee advising the EDI Council of Australia, version 1, October 1990; TEDIS European Agreement article 10; ABA Model Agreement §3.3.4.

[141]ABA Model Agreement §3.3.3.

Electronic messages pose also evidentiary problems.

In the environment of electronic commerce, the documents can be created, transmitted, and received without needing to be printed out. Computers provide for efficiency in storage and retrieval, and allow the parties to negotiate the contents of a document by amending and retransmitting it without the need to re-type it entirely each time. The document, when received, is stored on disk and retrieved as and when necessary. Thus, there is no paper document which attests to the transaction that occurred. This is indeed one of the main advantages of electronic communications but it creates evidentiary problems. And widespread reliable use of these techniques of electronic commerce will occur only if they have, and are perceived to have, the same similar level of security as paper-based systems. Yet, the problem with electronically stored messages is that alteration is simple and leaves no traces.

Electronic messages pose then three evidentiary problems: (i) proving that an electronic communication actually came from the party that it purports to come from; (ii) proving the content of the transaction, namely the communications that actually occurred between the parties during the contract formation process; (iii) reducing the possibility of deliberate or inadvertent alteration of the contents of the electronic record of the transactions[142].

---

[142]"Legal issues and Information Security", Office of Technology Assessment, Congres of the United States, Washington, D.C., U.S. government office, September 1994.

How is it possible to prove that an electronic message actually occurred, and what was its content? What are the requirements an electronic record must meet in order to constitute a reliable and valid evidence admissible in court?

1. Under the common law

To be admitted as evidence, an electronic message or record must first be authenticated or identified. But when relevant and authentic messages are involved, the opposing party may still object to admission under certain rules that regulate evidence. The two that most directly affect electronic transactions are the hearsay rule and the best evidence rule.

1.1. The authentication of the electronic record

Generally, any evidence relevant to a matter at issue may be admitted at a trial. Evidence is relevant if it tends to prove that some fact of consequence is so. A component of the relevancy requirement is that any message or record offered for admission as evidence must be authentic: evidence, though necessary to prove a pertinent fact, is not relevant if it cannot be authenticated. Evidence is authentic if it is what it is claimed to be. The proponent usually bears the burden of showing in his foundation that evidence is relevant and authentic. This is done by introducing preliminary (foundation) evidence to show the relevancy and identity of the thing offered as evidence[143].

What are the techniques legally accepted for establishing authenticity?

---

[143]Benjamin Wright, *supra note* 35, at §7.1.

The proponent might show authenticity with virtually any type of preliminary evidence - the testimony of witnesses on the circumstances surrounding the message, the internal characteristics of the message itself, or a demonstration of the process producing the message[144]. The point with authenticating evidence is that it be persuasive[145].

A mere statement of origin in a communication is usually insufficient to establish authenticity. For purposes of admitting communications into evidence, courts expect more of a foundation, with the stated goal of preventing fraud. The simple presence of a signature purporting to be from a certain person, cannot by itself authenticate the document. The proponent must introduce evidence that the signature is genuine - such as a comparison to a specimen autograph or the testimony of an expert who scientifically analyzes the fingerprints on, or the paper and ink constituting, the document.

In *United States v. Sliker*[146], the judge identified two methods of authenticating evidence: comparison with other authenticated specimens[147] or distinctive characteristics[148] in conjunction with where the evidence was found[149].

Under Federal Rules of Evidence (hereinafter FRE) 901(b)(4) the authentication of evidence may come from its "appearance, contents,

---

[144]*See* Federal Rules of Evidence (FRE) 901 (The Uniform Rules of Evidence, which have been adopted in one form or another in most states, are similar to the FRE).

[145]"Authentication means that you have to prove that your evidence is genuine. How do you do that? The late Irving Younger used to say, 'Any way that makes sense.' It is an excellent summary of the law.", McElhaney, "Authentication: Proving Your Evidence Is Genuine" (1993) A.B.A. J. 96.

[146]751 F.2d 477, 499-500 (2d Cir. 1984).

[147]quoting FRE 901(b)3.

[148]quoting FRE 901(b)4.

[149]The judge noted two cases where the contents of seized documents, and the location where they were found, provided a sufficient basis for authentication, *Silker*, 751 F.2d 477, 499-500 (2d Cir. 1984).

substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." The associated Advisory Committee Note states: "Thus a document or telephone conversation may be shown to have emanated from a particular person by virtue of its disclosing knowledge of facts known peculiarly to him;...similarly, a letter may be authenticated by content and circumstances indicating it was in reply to a duly authenticated one."

For purposes of admissibility, the so-called reply doctrine supplies an authenticity presumption for some messages. If one message is shown to have been issued, then a return message that indicates it is in reply to the first can be authenticated solely from its contents. In *United States v. Weinstein*[150] a telex was authenticated as a communication from the defendant by the fact that it replied to a prior letter addressed to the defendant. Hence, the return of an acknowledgment, particularly to an independently verified address, would be relevant to confirm the origin of a message[151].

Under the FRE, one way of identifying technological evidence is to present "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result[152]."
Thus, the proponent must show origin and integrity: competent testimony identifying, describing the function of, and confirming the accuracy of a computer system that produced a message or record is sufficient to authenticate the message or record[153].

---

[150]762 F.2d 1522 (11th Cir. 1985).
[151]Benjamin Wright, *supra note 35*, at §8.3.
[152]FRE 901(b)(9).
[153]FRE 901(b)(1). Authentication can be established by "testimony that a matter is what it is claimed to be".

The witness has to testify on (i) the procedure used to create and preserve the record and (ii) the record's chain of custody after creation.

An issue in laying the foundation for an electronic message or its record is the qualification of the foundation witness. Witnesses separate into two categories: a lay witness generally testifies from first hand knowledge; an expert witness is someone with special knowledge, skill, experience, or education who can help the trier of fact understand the evidence or determine a fact.

The majority rule is that a computer-records-foundation witness need not necessarily be a computer expert or have technical knowledge of the computer's data processing methods or the source of information if the records are used and stored in the company's day-to-day business.

In federal and most state courts, the witness is not required to have technical knowledge concerning the equipment's methods for data processing and storing. In *United States v. Vela*[154], computer records were automatically admissible under the hearsay rule if they were created in the ordinary course of business and if circumstantial evidence showed that the records were reliable. In *Vela*, the Court noted that the computer records of telephone bills were sufficiently trustworthy, since they were made by a disinterested company and relied upon by the company in its day to day business. According to the Court, failure on the part of the proponent to "certify the brand or proper operating condition of the machinery involved does not betray a circumstance of preparation indicating any lack of trustworthiness."

---

[154]673 F.2d 86, 90-91 (5th Cir. 1982).

The rationale in Vela was also applied in *United States v. Linn*[155], where a computer printout indicating the time and date of a telephone call was admissible and deemed trustworthy even though the "qualified witness" had no personal knowledge of computer programming or how the printout was generated. This knowledge was not necessary since the telephone record was generated automatically and retained in the ordinary course of business.

Professor Rudolph Peritz, however, argues that courts are too slack with computer records. He asserts that courts should require proponents to show, with expert testimony under an analysis like that in FRE 901(b)(9) (evidence describing a process and showing its accuracy), that the systems producing the records yield accurate results[156]. In practice, however, courts seem to presume that if businesses rely on the records in the ordinary course of their affairs, then the means by which the business's process and record the data under their control is accurate.

And indeed a minority of state courts requires technical knowledge on the part of the witness in order to insure trustworthiness of the electronic message. This minority rule demand increased levels of technical knowledge according to the complexity of the processing and transmission methods. These more technical means for laying a foundation for authentication stem from *King v. State ex rel. Murdock Acceptance Corp.*[157] The *King* standard requires that the party seeking to authenticate evidence demonstrate the reliability of the sources of information and the methods of the equipment

---

[155]880 F.2d 209, 216 (9th Cir. 1989).

[156]*Rudolph Peritz, "Computer Data and Reliability:A Call for Authentication of Business Records under the Federal Rules of Evidence" (1986) 80 Northwestern Univ. L. R. 956.

[157]222 So. 2d 393, 398 (Miss. 1969).

involved in technical terms. In addition, the records must have been made in the ordinary course of business at or near the time of the recorded event.

Chris Reed, for his part, proposes two alternative solutions to electronic messages' authentication problems. First, the sender could attach a cryptographic "digital signature" to each message; second, a trusted recordkeeper could store a record of the content of each electronic message and certain information about its origin[158]

The digital signature is a mathematical function of the message content, or part of it, which gives the identity of the sender and authenticates the contents. To be an effective signature, it must be producible by the sender alone, and any attempt to change the content of the message must be seen to be incompatible with the signature[159].

The trusted recordkeeper is also largely advocated by Benjamin Wright for purposes of authenticating electronic messages[160]. Indeed, the proper recording of the evidence/message requires that the risk of fraud by the record holder be eliminated. One method would then be to appoint a "trusted" recordkeeper, an entity situated between the points of message creation and final message disposition, having no incentive to fabricate its records. Benjamin Wright distinguishes two kinds of such recordkeeper: the external recordkeeper, who is an independent firm, such as a third party network, that is situated between the sender and receiver enterprises, and is equally obligated to each of them; and the internal one, who is a special department within the sender or receiver enterprise[161].

---

[158]Chris Reed, "Authenticating Electronic Mail Messages - Some Evidential Problems" (1991) 4 Software L.J. 161.

[159]*Id.*

[160]Benjamin Wright, "Authenticating EDI: the Location of a Trusted Recordkeeper" (1991) Software Law Journal 173.

[161]*Id.*

1.2. The Hearsay Rule applied to electronic messages

Hearsay is an out-of-court statement, offered as evidence in court by someone other than the person who made the statement, to prove that the matter asserted in the statement is true[162]. As a rule hearsay is non-admissible evidence in a court of law[163].

As for electronic transactions, one must distinguish the electronic message records from the computer business records.

1.2.1. Application to electronic message records

Electronic contracting messages are not hearsay, since they are offered into evidence merely to prove the fact that a legally potent document was issued, not to prove the truth of what is in the document[164]. Therefore, with respect to electronic contracting, the issue is whether Y sent to X an electronic message of acceptance, and if so, whether that message is admissible evidence to prove that fact.

Michaels v. Michaels[165] is an example of a case supporting the proposition that an electronic message is not hearsay if offered only to prove that it was stated. The court sustained a telex printout's admission into evidence, over a

---

[162]According to FRE 801, "'Hearsay' is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted".

[163]FRE 802.

[164]Comment to the Federal Rules of Evidence for US Courts and Magistrates, Rule 801(C); Robert W. McKeon, *supra note 10*, p.524; Benjamin Wright, *EDI, E-Mail and Internet: Technology, Proof and Liability, The Law of Electronic Commerce*, 2nd ed., Boston, Little, Brown & Co., 1995 §9.4.

[165]767 F.2d 1185, 1201 (7th Cir. 1985).

hearsay objection, on the ground that the telex contents were not offered to prove their truth. The telex indicated the interest of one party in pursuing a business transaction. It was admitted to show how another party reacted upon learning of this interest.

1.2.2. Application to computer business record

On the other hand, as for computer business records, the solution is different.

Classic computer evidence involves business records from a self-contained computer system controlled by the evidence proponent. The recorded data were input by human operators, who had obtained information from their own observations or those of others. In the classic computer evidence case, a printout offered to prove the truth of information in the computer could suffer from four possible sources of inaccuracy[166]: (1) the person with personal knowledge may not have been the one entering data, (2) the person entering data may have made mistakes, (3) the processing and storage programs manipulated and changed the data, and (4) the printout could be a distortion of the information on the records.

Thus the only way for electronic messages to be admitted in courts for the truth of their contents, is to qualify under one of the exceptions to the hearsay rule. The applicable exception to the rule will be that one that concerns records of regularly conducted activity: the so-called "business records exception".

---

[166]Benjamin Wright, *supra note 35*, §9.3.

According to Rule FRE 803(6) this exception to the hearsay rule includes:

> "[a] memorandum, report, record or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness".

Two rationales support the exception[167]. First, records kept in the ordinary course of business are likely to be reliable. Because businesses keep records for serious purposes, they are likely to be careful, and the systematic and routine accumulation and storage of information are less prone to error than casual record making[168]. Second, it would be impractical to call as witnesses all the people who played a role in preparing a large organization's records. Few of those people would be likely to remember relevant details. It is more expedient for the court simply to rely on the record.

The Advisory Committee Comment to FRE 803(6) confirms that the term "data compilation" in that provision embraces computer records. In *Brandon v. State*[169] the court has opined that the medium on which records are stored is irrelevant to the exception: the key is whether the records were created and maintained under circumstances that bespeak reliability.

---

[167] *Id.* §9.2.1.

[168] *See* FRE 803(6), Advisory Committee Note.

[169] 272 Ind. 92, 396 N.E.2d 365 (1979).

To show reliability, the proponent must lay a foundation, but there is no unanimity on how that should be done. The precise standards vary from jurisdiction to jurisdiction. Early cases tend to require more extensive testimony on the source of computer input and the function and reliability of systems than later cases do.

In *Transport Indemnity Co. v. Seib*[170], the most famous computer evidence case according to Benjamin Wright, the court considered the admissibility under the Uniform Business Records as Evidence Act (a statutory articulation of the business records exception) of a computer record of insurance premium data. Under an insurance contract, the defendant owed the plaintiff premiums calculated from a formula using past premium payments by the defendant and claims payments by the plaintiff. The plaintiff was suing for payment, and the issue was how much was owed.

Relevant data gathered by the plaintiff's personnel had been fed into a computer, calculated, and stored on tape. At trial the plaintiff offered a printout, which showed earlier premium and claims payments, together with the sums due based on the formula. The plaintiff's director of accounting, the official who oversaw the printout's preparation, testified on how information had been entered and stored on the computer and how the record had been regularly made and used in the plaintiff's business. The witness also recomputed the amounts owed to confirm the accuracy of the sums on the printout. The court held a proper foundation had been laid for the printout's admission into evidence.

In *King v. State ex rel Murdock Acceptance Corp.*[171], another famous business records exception case, the plaintiff offered into evidence a printout of

---

[170]178 Neb. 253, 132 N.W.2d 871 (1965).

[171]222 So. 2d 393 (Miss. 1979).

electronic records showing the amount due on a promissory note. The plaintiff's officer in charge of the computer accounting system testified on the source of the records, the type of computer used, and the means by which data were controlled and fed into the computer. Without hearing testimony from the individuals who made the original entries, the court held the printouts admissible:

> "if it is shown (1) that the electronic computing equipment is recognized as standard equipment, (2) the entries are made in the regular course of business at or reasonably near the time of the happening of the event recorded, and (3) the foundation testimony satisfies the court that the sources of information, method and time of preparation were such as to indicate its trustworthiness and justify its admission.

Under this standard, the proponent arguably has a considerable burden of showing system trustworthiness. The court held the plaintiff carried its burden and allowed admission of the printouts.

Some scholars, however, notably Professor Rudolph Peritz, criticize the relaxed foundation requirements that courts have applied to computerized business records[172]. Professor Peritz endorses as the more appropriate standard §2.716, Sixth Recommendation of the Manual for Complex Litigation[173], which directs that before admitting any such record into evidence the proponent must establish that the record is reliable. To do that, the proponent must, among other things, (1) show the record is the product of standard industry computing practices and (2) have an expert testify that the computer program functions reliably and accurately.

---

[172]Rudolph Peritz, "Computer Data and Reliability: A Call for Authentication of Business Records under the Federal Rules of Evidence" (1986) 80 Northwstern Univ. L. R. 956.
[173]5th edition 1982.

In spite of that, the mainstream view seems to be that, as long as the link between an event and its transcription into business record is a process that a business regularly relies on, no special foundation is necessarily required[174].

United States v. Vela[175] illustrates the mainstream view. There, even though the computerized telephone data underwent considerable processing and reformatting before reaching the final archive, the appellate court held that the trial court was not required to hear an expert vouch for the process' reliability.

According to Benjamin Wright, the outcome in *Vela* is clearly correct. The records came from the telephone company, a disinterested and responsible party. The company had a strong, independent incentive for its telephone records to be reliable. Common experience showed these records are usually correct.

In conclusion, electronic business messages appear to raise no new hearsay problems. A legally operative electronic communication itself is not hearsay if offered in court to show that it was sent[176]. On the other hand, if the record of the electronic message does not directly reflect the message, "programmer" hearsay can be an issue, but typically the business record exception can allow admission of such a record if the circumstances of the retention indicate trustworthiness.

---

[174] *See* People v. Lugashi, 205 Cal. App. 3d 632, 252 Cal. Rptr. 434, 440 (1988): specifically considered and respectfully declined to follow Professor Peritz's position.

[175] 673 F.2d 86 (5th Cir. 1982).

[176] Bradgate, "Evidential Issues of EDI", in I. Walden, *EDI and the Law*, London, 1989, at 13-14.

According to the best evidence rule, in order to prove the content of a writing or recording where the terms are material, the original is required[177]. unless it is shown to be unavailable for some reason other than the serious fault of the proponent. So the rule rejects the admission of copies of and testimony to prove the contents of writings when those contents are at issue. The purpose is to limit error and fraud, and regulates the introduction of potentially misleading evidence in the form of extracts or summaries of writings.

The rule evokes interesting questions when applied in the electronic messaging environment, where legal communications are not necessarily embodied in any particular recording.

The best evidence rule may apply to information affixed on things other than paper, provided it is the information itself that is at issue. Indeed, the FRE version covers any "writings" and "recordings", both of which are defined to "consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation[178]."

However, a proponent is excused from presenting the original writing if he shows, as part of his foundation, that one of the many broad exceptions applies. If excused, the proponent can introduce certain secondary evidence, such as copy or testimony from an informed witness, to show the writing's contents. The FRE version includes these exceptions:

---

[177]FRE 1002.
[178]FRE 1001(1).

1. FRE 1003. A duplicate of the original is always admissible to the same extent as the original unless there is a genuine question as to the original's authenticity or it would be unfair under the circumstances to admit the duplicate.

2. FRE 1004(1). If all originals are lost or destroyed (and, if the proponent lost or destroyed them, he did not act in bad faith), then secondary evidence is permitted.

3. FRE 1004(2). Secondary evidence is permitted if the original can not be obtained through judicial procedures - such as when the original is in the hands of a third party who is beyond the court's jurisdiction[179].

4. FRE 1004(3). Secondary evidence is admissible if the original is in the opponent's hands and he, after notice, does not produce the original.

5. FRE 1004(4). Secondary evidence is permitted if the writing is not closely related to a controlling issue in the trial.

6. FRE 1005. The contents of a government record or filing (including "data compilations") may be proved by certain types of copies.

7. FRE 1006. Summaries of voluminous writings or recordings may be admissible if the writings or recordings are available to the opponent.

8. Although not part of the FRE, the federal photocopy statute is effectively another exception to the best evidence rule in the FRE. It provides:

> If any business, institution, member of a profession or calling, or any department or agency of government, in the regular course of business or activity has kept or recorded any memorandum, writing, entry, print, representation or combination thereof, of any act, transaction, occurrence, or event, and in the regular course of business has caused any or all of the same to be recorded, copied, or reproduced by any photographic, photostatic, microfilm, micro-card, miniature photographic, or other process which accurately reproduces or forms a

---

[179] *See* United States v. Taylor, 648 F.2d 565 (9th Cir. 1981), in which a photocopy of a fax printout was admitted where efforts to obtain the sender's "original" had failed.

> durable medium for so reproducing the original, the original may be destroyed in the regular course of business unless its preservation is required by law. Such reproduction, when satisfactorily identified, is as admissible in evidence as the original itself in any judicial or administrative proceeding whether the original is in existence or not and an enlargement or facsimile of such reproduction is likewise admissible in evidence if the original reproduction is in existence and available for inspection under direction of court...[180]

In addition, some authorities hold that satisfaction of the business records exception to the hearsay rule also overcomes any best evidence rule objection[181].

1.3.1. Application to computer records

The rule's federal version does specifically mention computer data. FRE 1001(3) states, "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" The relevant Advisory Committee Note states that "practicality and usage confer the status of original upon any computer printout." Presumably FRE 1001(3) means that an accurate printout is an original of the particular computer record from which the printout is made. The question is then: what is an "accurate printout"?

Many computer records might be considered duplicates of other things. FRE 1001(4) defines a "duplicate" as "a counterpart produced by ... electronic re-recording ... or by other equivalent techniques that accurately reproduces

---

[180]28 U.S.C. 1732 (1988). Many states have adopted similar photocopy statutes. *See* "The Uniform Photographic Copies of Business and Public Records as Evidence Act" (1949) 14 U.L.A. 145.

[181]*See* United States v. Miller, 500 F.2d 751, 755 (5th Cir. 1974); State v. Loehmer, 159 Ind. App. 156, 304 N.E.2d 835(1973).

the original." Again, determining whether a record is a duplicate entails a judgment on what is an "accurate" reproduction.

So far, yet, the best evidence rule has played only a small role in computer evidence cases. In the case *Transport Indemnity Co. v. Seib*[182] information from paper documents had been fed into a computer. The court held that information on a tape created by that computer was admissible under the business records exception to the hearsay rule. But it did not consider whether either the initial paper documents or the data on the tape were the original writings at issue. The court permitted the information on the tape to be admitted in the form of a printout. It implicitly assumed that the printout was identical to the information on the tape, and it did not mention the best evidence rule.

The court's approach is consistent with FRE1001(3), which deems an accurate printout to be an "original" of data in a computer.

In another case, *King v. State ex rel. Murdock Acceptance Corp.*[183], the court said it followed the best evidence rule when it admitted a printout from a computer record. The court considered the printout the best evidence available of the computer record's contents. This approach seems to grow from the idea that the best evidence rule ranks evidence in a hierarchy. It requires a court in its discretion to judge which evidence is "best," second best, and so forth, and then to favor evidence at the top of the hierarchy.

Finally, the courts seem not to be demanding regarding the way the printout is created to accept it as an original under the best evidence rule.

---

[182] 178 Neb. 253, 132 N.W.2d 871 (1965).

[183] *King, supra note 169.*

1.3.2. Application to electronic messages

Three interpretations of the application of the best evidence rule to electronic messages are possible.

Under at least federal law, the best interpretation is that the best evidence rule does not apply to purely electronic messages.

First, the rule's federal version applies to an original "writing" or "recording.'" With telegraphic communications (telegrams, telexes) the messages are embodied in paper (the order handed to the carrier and the dispatch delivered to the recipient). But a purely electronic message exists independent of any particular recording.

Second, FRE 1001(1) defines both "writings" and "recordings" as "letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation." This suggests some degree of permanent recording is necessary to invoke the rule. But for paperless electronic messages there may be no original document in the sense of letters or words being "set down" somewhere. The records of the messages are not the messages themselves.

Consequently, according to Benjamin Wright, the best evidence rule does not apply to purely electronic messages.

The same interpretation applies to oral conversations that happen to be recorded. In *United States v. Gonzales-Benitez*[184] defendants claimed, on best evidence grounds, that the trial court erred by permitting an eyewitness to testify about certain conversations that had been recorded. "They claim[ed]

[184]537 F.2d 1051 (1976).

that since the conversations were recorded on tapes, the tapes themselves, and not testimony of one of the participants, were the 'best evidence' of the conversations." The appellate court dismissed the claim.

Only if the ultimate inquiry had been to discover what sounds were embodied on the tapes in question, the tapes themselves would have been the "best evidence." However, the content of the tapes was not in itself a factual issue relevant to the case. The inquiry concerned the content of the conversations. The tape recordings would have been admissible as evidence of those conversations. But testimony by the participants was equally admissible and was sufficient to establish what was said.

Likewise, in a dispute over an electronic message, the issue will be what were the message's contents, not what were the contents of any of the recordings of the message. Therefore, the best evidence rule should not exclude any of the recordings made of the message.

Another, but less persuasive, interpretation of the best evidence rule would be to consider the electronic message as the "original" writing. If, after transmission the message is lost or destroyed (through the fault of no one), any secondary evidence of the message, such as any recording of it, will serve as secondary evidence, according to FRE 1004.

Finally, under a third interpretation, which may apply in some state courts, the best evidence rule would impose a hierarchy on the available records of an electronic message. The rule would act to obtain the best obtainable evidence, preferring the most direct record of the message. But the rule would be flexible enough to permit admission of at least one of the available records.

In Robert W. McKeon's opinion[185], this approach is probably the more meritorious if a litigant wants to prove the contents of a message, since it may be distorted if it has been often transmitted. Pursuant to the FRE, and even under the *King* case[186], printout sheets accurately reflecting data are originals under the best evidence rule. In the case of electronic messages, the best obtainable original should satisfy the best evidence rule, and the accuracy of the data would be best preserved on the originating computer's hard disk drive.

Under each of these three interpretations of the best evidence rule, however, if there are any records of an electronic message, at least one record should be admissible. It would be very difficult to rule that all of the available records must be excluded. Thus the rule should not be a significant concern for electronic message users.

2. Under the ABA Model Agreement

Under most of the model interchange agreements, there is a provision by which the parties agree that evidence of the electronic message is admissible[187].

Since the domestic rules of evidence require that the "original" of a document be introduced in court, the ABA Model Agreement provides that the electronic transmission, or its printout, constitutes an "original". Section 3.3.2. states that document will constitute an "original" when printed from

---

[185]Robert W. McKeon, *supra note 10*, p. 527.

[186]*King, supra note 169.*

[187]TEDIS European Agreement, *supra*, article 10: EDI messages have a comparable evidential value to that accorded to written documents; Quebec Standard Agreement, *supra*, §6.3(2); South Africa Model Agreement, *supra*, §18; ABA Model Agreement, *supra*, §3.3.4.

electronic files or records establish and maintained in the normal course of business. And Section 3.3.4 of the ABA Model Agreement provides that electronic documents "will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form".

It also contains a mutual agreement by the parties not to contest the admissibility of copies of signed documents under either the business record exception to the hearsay rule or the best evidence rule on the basis that the signed documents were not originated or maintained in documentary form. Still Section 3.3.4, together with Section 3.3.2 does not waive the need for a proper foundation to be established for the admissibility of the evidence. In this regard, the effectiveness and reliability of each party's security procedure, record retention policies, confidentiality obligations and their conduct under the provisions of the Agreement may be relevant in individual cases to the ultimate admissibility of any document[188].

3. Under the UNCITRAL Draft Model Statutory Provisions

The UNCITRAL Working group on EDI dealt with the admissibility of the electronic generated evidence on the one hand, and with the weight of electronic generated records on the other hand.

As for the admissibility of electronic generated evidence, they decided to introduce a provision to eliminate the different legal obstacles that exist in the different legal systems, (...) such as the common law hearsay rule. They adopted the "waiver strategy", by simply stating that electronic data will

[188]Section 3.3 Comment 7.

always be acceptable under the best evidence rule and the hearsay rule, whatever the manner in which the record has been generated and stored.

As for the weight of electronically generated records, the Working Group considered it most appropriate to leave this question to the discretion of the trier-of-fact, as is currently the case in most jurisdictions, rather than establishing detailed statutory rules for weighing the probative value of electronic messages. However they considered it useful to include in the uniform rules, factors or guidelines to be taken into account in evaluating computer-generated evidence. Since it was noted that the approaches taken in most legal systems focus on the reliability of the computer system and on the reliability of the data (cf. the application of "business record exception"), the Working Group based the weight criteria on the way the evidence has been produced, so as to ascertain the integrity and reliability of the system producing the evidence.

The provision reads as follows:

> Article 9. Admissibility and evidential value of a data [record]
>
> (1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to prevent the admission of a data [record] in evidence
>
> > (a) on the grounds that it is a data [record]; or,
> >
> > (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not an original document.
>
> (2) Information presented in the form of a data [record] shall be given due evidential weight. In assessing the evidential weight of a data [record], regard shall be had to the reliability of the manner in which the data [record] was generated, stored or communicated, to the reliability of the manner in which the information was authenticated and to any other relevant factor.

(3) Subject to any other rule of law, where subparagraph (b) of paragraph (1) of article 8[189] is satisfied in relation to information in the form of a data [record], the information shall not be accorded any less weight in any legal proceedings on the grounds that it is not presented in the form of an original record[190].

Conclusion Section 3

To conclude, the law of evidence does not rest on inflexible paper-based rules that pose a barrier to the use of electronic commercial practices. Rather, it is concerned with the underlying integrity of the information on which a judge, jury, arbitrator, or mediator can reasonably rely in reaching a just conclusion to a particular controversy. Modern rules of evidence and court decisions appear to have come to terms with the realities of business and professional practice - the ever-growing dependence on information technology systems for records production and maintenance.

Yet, for better security, it is recommended that the parties, in their interchange agreement, contract to treat electronic messages, electronically "signed", as if they were manually signed paper and to agree that they shall make no objection to the use in evidence of the computer records. Those terms should be effective (in particular, thanks to the estoppel doctrine), to the extent they are not invalidated by the Unfair Contract Terms Act 1977[191].

---

[189]Pertaining to the functional equivalent of "original".

[190]UNCITRAL Documents A/CN.9/WG.IV/WP62 of 20 July 1994 (for Articles 1-10) and A/CN.9/WG.IV/WP.60 of 24th January 1994 (for Articles 11-15) available under the name of "EDI-TXT" in the Library 0 of the CompuServe Legal Forum.

[191]By virtue of section 3 of the Act, a party seeking to rely on such a clause in an action against him for breach of contract must show the clause satisfies a test of reasonableness: the clause must be "a fair and reasonable one to have been included in the contract having regard to the circumstances which were or ought reasonably to have been known to or in the contemplation of the parties at the time the contract was made". Notice this restriction does not apply to international supply contracts.

However, they should be coupled with a specific contractual duty to maintain adequate security system and to prevent unauthorized access to the system or use of passwords or signatures.

Finally, the law, in order to fit to the new technology and the new way to conduct business routinely through computers and to remove any useless long evidence dispute, should elaborate an express rule making clear that electronic messages are not hearsay and that their records are admissible into the courts provided that the retention procedure shows enough trustworthiness. This procedure, however, should not be precisely described. It should be broad enough as to anticipate the future evolution of the technology: criteria as to what is deemed to assure enough trustworthiness should be established.

SECTION 4- THE SCOPE OF THE CONTRACT

Regardless of whether a court is prepared to accept an electronic message as evidence, once it has been established that there is a binding contract, the trade terms and conditions of that agreement will still have to be determined. Trade terms and conditions refer to the detailed terms that traditionally are printed on the backside of form purchase orders, acknowledgments, and other documents. These are not the basic terms such as quantity, price, and delivery date that are usually provided for since it is necessary for the contract to be binding, but rather "standard" terms such as products warranties, time limits for filing law suits, policy for the return of defective goods, etc.

In practice, terms and conditions are often the most important and difficult legal issues to be resolved in electronic transactions.
Indeed, electronic messages are not always technically equipped, and even intended, to transmit all the legal terms of the general conditions that are printed on the backs of purchase orders, acknowledgments and other paper documents traditionally used by trading partners and this is usually not done. One of the advantages of electronic communications is speed and efficiency that do not allow for complete negotiation over all terms and conditions.

In these circumstances, what will then be the trade terms and conditions of the electronically concluded contract?

1. Under the common law

The main problem regarding the terms and conditions is to know to what extent they could be asserted by one party against the other contracting party. The court would consider whether it could be reasonably inferred from the context that the party against whose terms and conditions were asserted had had the opportunity to be informed of their content or whether it could be assumed that the party had expressly or implicitly agreed not to oppose all or part of their application.

Three situations are conceivable: (i) the parties have provided for them electronically: here, the battle of the forms will apply; (ii) the parties have not made provision for them at all: gap-filler provisions will apply; (iii) the parties have made a provision for them in a trading partner agreement.

1.1. The parties have provide for the terms and conditions electronically

Sometimes it may be practical to communicate full text trade terms and conditions electronically.

At common law, a contract could be formed only if the offer and the acceptance were mirror images of each other. An acceptance with different terms amounted to a counteroffer, and payment by the initial offeror would create the contract based on the counteroffer's terms. Therefore the last form usually succeeded as being the contract.

But the U.C.C has expanded the notion of contract[192]. U.C.C. Section 2-207 has for the most part discarded the mirror image rule, and transforms many

[192] *See Section 1.*

common law counteroffers into acceptance. Section 2-207 allows for contract formation even though they are additional terms in the acceptance[193]. Nevertheless there is a limit as to how far a diverging acceptance may go and still form a contract. There must at least be a mirror image concerning material terms such as price, quality, quantity, and delivery. Diverging terms in an acceptance relating to warranty, arbitration and the like, usually found on the back of standard forms, will not hinder contract formation between the parties.

When trade terms and conditions are transmitted electronically, the battle of the forms advances to "electronic combat". The results of electronic combat, however, should be similar to those for the old paper battle of the forms[194].

The parties may also incorporate trade terms and conditions in their electronic messages by reference. For instance, it is possible for the parties to provide "that each of buyer's purchase order transaction sets will be deemed to incorporate the terms on the back of the buyer's form and that each of seller's purchase order acknowledgments will be deemed to incorporate seller's terms"[195]. This saves transmission costs and otherwise eases communication. In this case, according to Benjamin Wright[196], so long as the recipient has notice of the reference's meaning, there seems to be no reason this would not be just as effective as transmitting full text. In *American Multimedia, Inc. v. Dalton Packaging, Inc.*[197], the Supreme Court of United States recognized the effectiveness of an incorporation of terms by reference

---

[193]Between merchants, a contract will still be formed, but materially altering terms will not be considered part of the contract. Terms that do not materially alter the contract will become part of it. *See* U.C.C. §2-207(2)(b).

[194]Benjamin Wright, *supra note* 35, §17.4.3.

[195]United Nations Commission on International Trade Law, Report of the Secretary-General, "Electronic Data Interchange: Preliminary Study of the Legal Issues related to the Formation of Contracts by Electronics Means", New-York, 25 June-6 July 1990, §68.

[196]*Id.*

[197]143 Misc. 2d 295, 540 N.Y.S.2d 410 (Sup. Ct. 1989).

in a fax. The fax stated it was subject to certain trade terms and conditions; the terms were not transmitted in the fax itself but were well known by the parties. The court held that those terms controlled.

Yet, the extent of the application of UCC Section 2-207 to electronic transactions is questionable[198]. Electronic messages are very concise, coded messages that normally indicate the price, quantity and shipping date. Trade terms and conditions, indicating warranties, arbitration, etc... are not usually transmitted.

Thus, even under the UCC, diverging terms in an acceptance regarding the price, quantity, quality or date of shipment will not likely form a contract, but merely a counter-offer. Therefore the acceptance must mirror the offer with respect to those terms. But as for trade terms and conditions, which are not transmitted Section 2-207 can not apply.

1.2. The parties have not made provision for trade terms and conditions

In this case, a lack of agreement concerning terms and conditions to apply to the electronic contract may initiate application of the U.C.C.'s contract gap-filler provisions, by default. U.C.C. Article 2 supplies a comprehensive set of commercial terms ranging from shipment to performance and general remedies provisions, going through implied warranties of merchantability and fitness for particular purposes...[199]. In addition, according to Sections 2-205 and 2-208, course of dealing, usage of trade and course of performance may also be relevant.

---

[198]Robert W. McKeon, *supra note 10*; Benjamin Wright, *supra note 35* §17.4.

[199]*See, e.g.*, U.C.C. §§ 2-305 (open price term), 2-307 (delivery in a single lot), 2-308 (place for delivery), 2-309 (time for shipment or delivery), 2-314 (implied warranty of merchantability), 2-315 (implied warranty for particular purpose).

1.3. The parties should provide for them in a trading partner agreement

For many vendors these implied terms and warranties may not be an adequate solution. To avoid default application of the U.C.C.'s gap-fillers, one logical alternative is for the buyer and the seller to enter an electronic trading partner agreement that would define the trade terms and conditions that would better fit to their transaction.

2. Under the ABA Model Agreement

Section 3.1 of the ABA Model Agreement provides for a provision by which the parties define the trade terms and conditions that are to be applied to their own transaction. It distinguishes nevertheless three ways by how this can be done by giving three options for the parties[200]:

Option [A] requires negotiation and agreement between the parties upon the additional terms and conditions; the negotiating terms would be included in the trading partner agreement.

In option [B] the trade terms and conditions will be those printed on each party's standard form document, copies of which are to be attached to the trading partner agreement are to be identified to be incorporated by reference. This option furnishes less certainty than the first one but reflects the common industry practice and defines for each party the terms and conditions on which it wishes to conduct business. Yet in the event of any inconsistency or conflict between the respective forms of the parties, option [B] moves into the electronic environment the battle-of-the-forms method set forth in U.C.C. Section 2-207[201].

---

[200]Report of the Electronic Messaging Services Task Force, *supra note 38*, p. 1700.
[201]Section 3.1 Official Comment 7.

Finally, option [C] incorporates into each contract for the sale of goods the manner by which applicable law determines additional terms and conditions that have not been agreed upon by the parties: the trade terms and conditions will thus be the default provisions provided by law. For the sale of goods, the trade terms and conditions will therefore be U.C.C. Article 2's gap-fillers.

3. Under the UNCITRAL Draft Model Statutory Provisions

In the UNCITRAL Working Group's opinion, the principle of freedom of contract must be maintained. It is primarily a matter of the rights and obligations agreed upon by the parties. At least, if the parties have not provided for the "general conditions" (*i.e.*, trade terms and conditions) in the agreement, a technique is needed to ensure that the parties were aware of, or at least had the opportunity to familiarize themselves with, the content of the general conditions. According to the Working Group, until such time as technical obstacles to the use of standardized messages for the transmission of general conditions had been overcome, a hybrid system must be envisaged in which papers documents remained the repository of general conditions. It was thus submitted that no attempt should be made by the Working Group to solve the question of the battle of the forms that is not typical of paper-based or any other means of communication. However, it decided to include in the uniform rules a provision to the effect that, where applicable law requires special acceptance of general conditions before a contracting party becomes bound, such an acceptance must be given in the prescribed form before a contract is concluded by electronic means[202]. However, there exists finally no such provision in the last current version of the DMSP.

---

[202]Report of the UNCITRAL Working Group on EDI, *supra note 58*, n°s 109 req.

Conclusion Section 4

In sum, the trade terms and conditions will be either the ones agreed upon by the parties (which is the solution recommended by the ABA Model Agreement and the preferred solution of the UNCITRAL Working Group), or, if not, the default ones provided by the revised Article 2. This solution is not different from all kind of contracts. It is not surprising since trade terms and conditions of the contract pertain to the underlying transaction and are independent of the means the parties have used to contract.

For the time being, if the parties want to avoid the U.C.C gap-filler provisions, they should provide for the desired trade terms and provisions in an agreement, or electronically if they technically can.

One of the trickiest issues in the law of Internet is the domain of private international law. The Internet raises jurisdictional questions, such as: Where can an agreement be enforced if it is formed in Cyberspace? Whose laws apply when litigation arises from activity in a transnational Cyberspace? Which courts should have jurisdiction over the Internet? If a transmission is routed through several jurisdictions, are the laws of each jurisdiction implicated?

Choice of law is "particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty"[203].

As a matter of fact, not all disputes that involve the Internet pose problems different from those of traditional private international law. Professor Trotter Hardy notes that "Some Cyberspace issues seems wholly unremarkable: it is evident to any legal eye that they are readily governed by the same rules applicable to other forms of communications[204]." The issue will be new only if there is something about the dispute that evokes or typifies those failings of traditional choice of law regimes, i.e. some reason why old methods are not

[203]Dan L. Burk, "Patents in Cyberspace" (1993) 68 Tul. L. R. 1, at 5.

[204]I. Trotter Hardy, "The proper legal regime for "Cyberspace" (1994) 55 U.Pitt.L.Rev. 993, at 998.

helpful. The simple fact of the Internet is not a sufficient reason to avoid traditional choice of law regimes[205].

What is the applicable law in a case of an internet-related transaction?

1. Under the common law

The two possible situations are: (1) the parties may have made provision for a choice of law clause in their contract; or (2) they may not have done so: it then will be necessary for the court to determine the law that would control.

1.1. The parties have provided for the law applicable to their transaction

Because certainty in contractual obligations is of paramount importance, the practice of choosing the law by way of a choice of law clause is the best means of handling choice of law for contractual disputes.
U.C.C. §1-105(1)(1994) states: "[W]hen a transaction bears a reasonable relationship to this state and also to another state or nation the parties may agree that the law either of this state or of such other state or nation shall govern their rights and duties". "[P]redictability is served, and parties' expectations are protected, by giving effect to the parties' own choice of the applicable law (party autonomy)."[206] This party's autonomy objective is "especially prominent" when the contract is to be performed in several different jurisdictions, which will often be the case with transactions concluded through the Internet since it is truly international. Section 187 of

---

[205]Matthew R. Burnstein, *supra note 4*, p.90 req.
[206]Eugene Scloes & Peter Hay, *Conflicts of law*, 2nd ed., 1992, at 657.

the Second Restatement of Conflict of Laws recognizes and encourages the practice of law and forum selection:

> §187. Law of the State Chosen by the Parties
>
> (1) The law of the state chosen by the parties to govern their contractual rights and duties will be applied if the particular issue is one which the parties could have resolved by an explicit provision in their agreement directed to that issue.
>
> (2) The law of the state chosen by the parties to govern their contractual rights and duties will be applied, even if the particular issue is one which the parties could not have resolved by an explicit provision in their agreement directed to that issue, unless either
>
> (a) the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties' choice, or
>
> (b) application of the law of the chosen state would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue and which ... would be the state of the applicable law in the absence of an effective choice of law by the parties.

However, the language of the Second Restatement and its interpretation by the courts indicate that forum selection clauses are honored so long as the choice is reasonable[207]. Two aspects of reasonableness as that term applies to contractual choice of law on the Internet are important: (i) the requirement of "connecting factors" to the forum selected, and (ii) the lack of a gross inequality of bargaining power, such as the choice doesn't appear to be oppressive to one party[208]. Traditionally, the parties' choice of law of the place of contract formation, the place of performance, the domicile of either party, the location of the corporate headquarters, or state of incorporation of a party would satisfy Section 187's reasonableness requirement[209]. On the Internet, it is unclear where some of these locations might be, but, in Matthew R.

---

[207]George A. Zaphiriou, "Basis of the Conflict of Laws: Fairness and Effectiveness" (1988) 10 Geo. Mason U. L. R. 301, at 315; *See also* The Breman v. Zapata Offshore Co., 407 U.S. 1 (1972).
[208]Matthew R. Burnstein, *supra note 4*, p.98.
[209]Eugene Scloes & Peter Hay, *supra note 204*, at 671-672.

Burnstein's opinion, arguments can be made for choosing the law of the domicile of either party[210].

Comment f to Section 187 of the Second Restatement of Conflict of Laws states:

> "The parties to a multistate contract may have a reasonable basis for choosing a state with which the contract has no substantial relationship. For example, when contracting in countries whose legal systems are strange to them as well as relatively immature, the parties should be able to choose a law on the ground that they know it well and that it is sufficiently developed.... So parties to a contract for the transportation of goods by sea between two countries with relatively undeveloped legal systems should be permitted to submit their contract to some well-known and highly elaborated commercial law".

Forum selection clauses can bring order and stability to cyberspacial contracts by substituting the highly developed realspace legal order for the uncertain and almost haphazard regime likely to result if courts are left open to choose law in cyber-disputes.

1.2. The parties have stayed silent on the applicable law to their contract

What law is applicable then in the absence of any choice of law clause?

Without a forum selection clause, the choice of law for a contractual dispute devolves upon the law of the nation most closely connected with the relevant contractual issue. Section 188 of the Second Restatement of Conflict of Law addresses choice of law for contractual disputes, absents a clause in the contract:

---

[210]Matthew R. Burnstein, *supra note 4*, p.99.

§188. Law Governing in Absence of Effective Choice by the Parties

(1) The rights and duties of the parties with respect to an issue in contract are determined by the local law of the state which, with respect to that issue, has the most significant relation to the transaction and the parties....

(2)... [T]he contacts to be taken into account in ... determin[ing] the law applicable to an issue include:

(a) the place of contracting,
(b) the place of negotiation,
(c) the place of performance,
(d) the location of the subject matter of the contract, and
(e) the domicile, residence, nationality, place of incorporation and place of business of the parties.

Therefore, if the dispute arises over the formation of the contract, presumably the law of the nation in which the contract was made would apply. Similarly, if the dispute is performance-related, the applicable law is that where performance was to occur[211].

For contracts in cyberspace, it is then possible to refer to "the domicile, residence, nationality, place of incorporation and place and business of the parties", to the extent that they are relevant (plus the place of contracting, if we consider it to be the one defined in Section 1 Part 2).

Nevertheless, these contacts may not be enough. The problem with Section 188's method for choosing law for contractual dispute is its continual reference to the "place" and "location" of certain events. Yet Cyberspace confounds notions of place and location. They mean little or nothing when it comes to Internet contracts. As Rosaland Resnick says: "The trouble with Cyberspace is that there is no 'there' there[212]".

---

[211]George A. Zaphiriou, "Basis of the Conflict of Laws: Fairness and Effectiveness" (1988) 10 Geo. Mason U. L. R. 301, at 316.

[212]Rosaland Resnick, "Cybertort: The New Era" (July 18, 1994) Nat'l L. J. A1.

In this area of the contract law, traditional methods are therefore ineffective. The need to consider choice of law in the networked world arises because conventional choices of law approaches are location-oriented. Some propositions for new methods have been made:

Matthew R. Burnstein, in a recent article[213], considers the conflict of laws' implications of transnational Cyberspace. Stating that conventional choices of laws' approaches falter in the networked world because it is location-oriented whereas the Internet is made not by countries, states and provinces, but rather by networks, domains and hosts, the author proposes different solutions to solve the choice of law problem in such a context.
One solution, also suggestied by Anne W. Branscomb[214] and Ian Trotter Hardy[215], is to adopt a whole new approach and to use the *lex mercatoria* -the Law Merchant- as a model to solve the choice of laws' conflict in Cyberspace.

The Law Merchant was a collection of customary practices among traveling merchants in Medieval Europe and Asia that was enforceable in "all the commercial countries of the civilized world". It grew up as a response to adapt to the needs of international commerce and then existed "in some sense apart from and in addition to the ordinary rules of law that applied to non-merchant transactions"[216]. The *lex mercatoria* has been described as follows:

> "The law merchant has been for centuries and continues to be today an International body of law, founded on the shared legal understandings of an International community composed principally of commercial,

---

[213]Matthew R. Burnstein, *supra note 4*.
[214]Anne W. Branscomb, "Global Governance of Global Networks", in Anne W. Branscomb, *Toward a Law of Global Communications Networks*, ed. 1986, 21.
[215]Model Electronic Data Interchange Agreement and Commentary, *supra note 202*, at 1019.
[216]*Id.* at.1020.

> shipping, insurance, and banking enterprises of all countries.... We believe that the shared legal understandings of the international mercantile community should be seen as an autonomous body of law, binding in appropriate cases upon national courts[217]."

The Law Merchant is a body of law in itself, which enables therefore an easy resolution to the choice of law question. The laws of the various nations are displaced by a law of a collection of merchants, with their own customs and usages of trade.

The lex mercatoria is a satisfying analogy to the legal problems posed by transnational Cyberspace. Like the merchants in Medieval Europe, Cyberspace users have specific needs and, by developing their own customs to the point of becoming judicially recognized and hence legally binding, they could create a new body of law specific to Cyberspace. This would simply abrogate the need for the choice of law inquiry and the attendant balancing and weighing of interests. Just as the merchants knew the customs and usages in the *lex mercatoria*, so too should users on the Internet be charged with a knowledge of the customs and usages of the on-line world.

One of the most appealing aspects of the Law Merchant as an analogy to Internet is its ability to respond and adapt rapidly to changes in the technical and legal environments. When a forum state seeks to apply a set of rules, it would look to the Law Cyberspace, which would be the collection of customs and accepted practices, codified or not, that had grown up with Cyberspace[218].

---

[217]Harold J. Berman & Felix J. Dasser, "The 'New' Law Merchant and the 'Old': Sources, Content, and Legitimacy" *in* Thomas E. Carbonneau, *Lex Mercatoria and Arbitration*, ed. 1990, at 21-24.

[218]*Id.* at 1036-1041.

Raj Bahla, in another recent article, also thinks that there should be an independent and specific body of law for Cyberspace. In order to meet the needs of participants in global electronic markets, he advocates to "reinvigorate" the role of usages of trade[219]. Indeed, for the customs to acquire powerful legal force, usages should not be seen -contrary to the approach often adopted by courts and scholars- as merely a device to interpret disputed terms in a contract. Rather, they could be viewed as the legal foundation for existing and new trade practices, and therefore, as the source of authority for and legal obligation arising from such practices. As such, it would confer legitimacy and authority on the practices, and be a source of obligation for the participants.

Besides, Matthew R. Burnstein draws analogies with sovereignless regions which are, like Cyberspace, transnational, yet non-national: outerspace (referring to Helen Shin[220]) and Antarctica (referring to Jonathon Blum[221]). In the first case, choice of law should be made through arbitration undertaken according to the Model Law on International Commercial Arbitration promugalted by the UNCITRAL since no states may assert sovereignty in this region. In the second case, the applicable law would be the default *lex fori* since the choice of law can not be at issue where there is no alternate legal system from which to choose[222].

219Raj Bhala, "Self-Regulation in Global Electronic Markets Through Reinvigorated TradeUsages" (1995) 31 Idaho L. R. 863.

220Helen Shin, "Oh, I Have Slipped the Surly Bonds of Earth: Multinational Space Stations and Choice of Law" (1990) 78 Calif. L. R. 1375, at 1375.

221Jonathon Blum, "The Deed Freeze: Torts, Choice of Law, and the Antartic Treaty Regime" (1994) 8 Emory Int'l L. R. 667.

222*See* Beattie v. United States, 756 F.2d 91 (D.C. Cir. 1984): an Air New Zealand plane crashed in Antartica. The court held that choice of law was not an issue because there were no alternative legal system from which to choose.

Finally, Matthew R. Burnstein, taking into account that nations will likely refuse to surrender their sovereignty and their power to make law, advocates the adoption of a supranational choice of law treaty for Cyberspace. Rather than crafting a new jurisdiction's entire substantive law, the nations would only need to agree on this jurisdiction's private international law. Just as multinational accords have been reached on conflict of laws with regard to a number of subjects[223], an agreement might be forged to unify choice of law rules for cyberspacial disputes. In the end, such a treaty might provide the easiest solution to the problem of choice of law in transnational Cyberspace.

In Harry Rubin, Leigh Fraser and Monica Smith's opinions[224], another possibility is for countries to assert extra-territorial jurisdiction on Internet activity based on the compelling rational that Internet transmissions have substantial effects on them. A proliferation of extraterritorial laws, however, will likely instigate more problems than it solves. Such 'legal imperialism' is sure to generate international friction and will subject the Internet community to more inconsistent laws.

They think that the uniqueness of the Internet merits an international convention settling the jurisdictional basis of a country's ability to (i) prescribe means of Internet conduct, (ii) adjudicate Internet related disputes, and (iii) enforce Internet regulations. The Internet's defiance of sovereignty and nationality makes each country equally vulnerable. Therefore, conduct and the effects of conduct might well constitute the most appropriate axiomatic basis for an Internet jurisdiction convention.

---

223 *See generally* Eugene Scloes & Peter Hay, Model Electronic Data Interchange Agreement and Commentary, *supra note 204*, at 153 n.1.

224 *Id.*

In conclusion, if the parties have neglected to provide for a choice of law clause, traditional location-oriented methods permitting to designate a national law are not all helpful since this notion is unknown to Cyberspace.

In cases where the only contacts which can be used (domicile, nationality... of the parties) are not helpful, some authors advocate that, rather than finding a new method of conflict of laws, it would be more adapted to take in consideration the usages and customs that are emerging in this area in order to create a specific and adapted body of laws for Cyberspace, in the image of the Law Merchant.

2. Under the ABA Model Agreement

As it is the best way to achieve predictability and certainty, the ABA Model Agreement provides for a choice of law selection clause: "This Agreement shall be governed by and interpreted in accordance with the laws of the States of _____[225]".
In addition to customary factors considered in selecting applicable law, the comment to this Section advises the parties to evaluate various state laws which may be in effect relating to criminal use of computers, computer privacy, and similar issues relating to technology.

3. Under the UNCITRAL Draft Model Statutory Provisions

The UNCITRAL DMSP also gives preference to the parties complete freedom to determine the law applicable to their relationship. At its twenty-

[225]ABA Model Agreement Section 4.4.

fifth session, the Working Group nonetheless expressed the view that party's autonomy in this regard should be limited by considerations of international public order so that a choice of law clause should not be used as a means of avoiding application of fundamental legal principles. Furthermore, another suggestion was made to establish a conflict-of-law rule providing that, in the absence of a contrary agreement, one national law would be applicable to various segments of an electronic transaction and providing a method for the determination of that law. Nonetheless, neither of these suggestions has been retained in the current draft of the DMSP.

Conclusion Section 5

The difficulties in determining the appropriate forum for resolution of a dispute and the applicable domestic law in the electronic environment, militate towards precise choice of law and forum clauses in order to provide for predictability and certainty.

For lack of "Law Cyberspace" for the time being, the parties to an electronic transaction on the Internet should, once again, consider including a choice of law clause in their trading partner agreement. In determining which law to apply, they should take into account the rules applicable to electronic contracts and make sure that their electronic contract will be legal and enforceable as well as their trading partner agreement. They also should pay attention to criminal laws relating to computers, computer privacy laws, and other laws relating to computer technology.

In the absence of such a choice, the law applicable to the contract will be the local law of the State which has the most significant relation to the

transaction and to the parties. The only contacts that can be taken into account in determining this law are these that are known and certain, such as the domicile, residence, nationality, place of incorporation and place and business of the parties, to the extent that they are relevant (plus the place of contracting, if we consider it to be the one defined in Section 1 Part 2).

The issue here is to determine what would be the impact, if any, of using a computer network for contracting, on the determination of the competent jurisdiction: does the fact that electronic messages traverse communication networks in several countries subject the parties to their jurisdiction? And to which one when there are several of them?
We will also discuss the best procedure for the parties to an electronic transaction to follow: what is the best way to settle dispute in the electronic environment considering that this is still a new and emerging fields where the law is not yet clearly defined and which evolved rapidly?

1. The competent personal jurisdiction in the context of electronic contracts

The question raised by the Internet concerning dispute resolutions is to determine which court will have jurisdiction over an Internet related transaction. The advent of the electronic superhighway raises the issue of whether using a computer to transmit information to a computer in another state subjects the transmitter to the jurisdiction of the state where the information is received.

Computers have added a new dimension to the area of personal jurisdiction law. "The test of whether business was transacted within [a forum state to determine personal jurisdiction] must be applied in the context, not of communication and transportation criteria of yesteryears, but of modern day commercial and personal accelerated relationships. The long

arm statutes are comrades of the computer"[226]. Indeed, jurisdiction is invariably based on the location of the person, events, object, or action or on the effects of the action. By definition, a jurisdiction has physical boundaries. Yet, Cyberspace does not. Traditional notions of jurisdiction are outdated in a world divided not into nations, states, and provinces but networks, domains and hosts. Cyberspace confounds the conventional law of territorial jurisdiction and national borders[227]. On the Internet, it does not matter at all whether a site lies in one country or another because the networked world is not organized in such a fashion[228]. Remote log-on, telnet[229], gopher[230], and the World Wide Web all render political borders obsolete[231]. For example hypertext on the World Wide Web enables users to "visit" one location (called a page or a site), where they are then presented with an opportunity to visit any of a number of other locations, in any of a number of other countries. Frequently, users are unaware that they have even "crossed" a political border in the course of their virtual travels[232]. The well-known jurisdictional doctrines consequently lose meaning in Cyberspace.

Under elementary legal principles, an out-of-state defendant must satisfy a two-pronged requirement in order to be bound to respond to claims field against it in a distant forum state.

---

[226]Alchemie Int'l, Inc. v. Metal World, Inc., 523 F.Supp. 1039, 1050 (D. N.J. 1981).

[227]David Johnson, "Addressing the the Daunting New Problems that will Arise with Universal Communications", COMPUTERGRAM, Reuters. Info. Svcs., June 23, 1994: "Jurisdiction based on place can no longer be viable".

[228]Matthew R. Burnstein, *supra note 4*, p. 82.

[229]Telnet allows users to "log on" to a remote host computer as if they were sitting in front of that computer.

[230]Gopher is a menu-based way to navigate through the Internet by allowing the users to quickly access information elsewhere and download that information to their own computers.

[231]Dan L. Burk, "Patents in Cyberspace" (1993) 68 Tul. L. R. 1, at 3.

[232]*See* Danny Hills, *Kay & Hillis*, Wired, Jan. 1994, at 103.

Burger King Corp. v. Rudzewicz[233] and *World-Wide Volkswagen Corp. v. Woodson*[234] have set forth the following two-pronged personal jurisdiction analysis: (1) does the out-of-state business have sufficient minimum contacts with the forum state? ("minimum contacts prong") and (2) is it reasonable to require the out-of-state business user to answer the claims filed against it in the forum state? ("reasonableness prong").

When applying the minimum contacts prong, the *Burger King* United States Supreme Court articulated a two factors analysis that courts should apply: (1) purposeful availment and (2) foreseeability.

In *International Shoe Co. v. Washington*[235], the United States Supreme Court originally defined "purposeful availment" as:

> "[To] the extent that a corporation exercises the privilege of conducting activities within a state, it enjoys the benefits and protection of the laws of that state. The exercise of that privilege may give rise to obligations; and, so far as those obligations arise out of or are connected with the activities within the state, a procedure which requires the corporation to respond to a suit brought to enforce them can, in most instances, hardly be said to be undue".[236]

This purposeful availment test is established if an out-of-state defendant purposefully directs its activities toward the forum state[237].

Alternatively, the Court in *World-Wide Volkswagen* established that the foreseeability test is satisfied only if the out-of-state defendant's activities in connection with the forum state are such that he should reasonably expect to be subject to the distant forum state's jurisdiction[238].

The reasonableness prong was first established by the *International Shoe* United States Supreme Court when it explained that "subject[ing] a defendant

---

[233] 471 U.S. 462 (1985).
[234] 444 U.S. 286 (1980).
[235] 326 U.S. 310 (1945).
[236] *International Shoe*, 326 U.S. at 319.
[237] *Burger King*, 471 U.S. at 476.
[238] *World-Wide Volkswagen*, 444 U.S. at 297.

to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'"[239].

However, the *World-Wide Volkswagen* United States Supreme Court expanded on this definition by setting forth a five factor analysis that courts should consider: 1) the burden on the defendant; 2) the forum state's interest in adjudicating the dispute; 3) the plaintiff's interest in obtaining convenient and effective relief; 4) the interstate judicial system's interest in obtaining the most efficient resolution of controversies; and 5) the shared interest of the states in furthering fundamental substantive social policies[240].

By contracting through the Internet, an out-of-state business user can confer financial benefits and actively participate in the performance of a contract without physically entering the forum state.

However, establishing personal jurisdiction through the Internet has recently been rejected by a Florida appellate court in *Pres-Kap, Inc. v. System One, Direct Access, Inc.*.[241] The court reviewed whether a New York defendant's on-line access and business use of a computer database, located in Florida, constituted sufficient minimum contacts to establish personal jurisdiction[242] under the Florida long-arm statute[243].

---

[239]*International Shoe*, 326 U.S. at 319.

[240]*World-Wide Volkswagen*, 444 U.S. at 292.

[241]636 So.2d 1351 (Fla. Dist. Ct. App. 1994).

[242]In *Burger King*, 471 U.S. at 479, the United States Supreme Court defined "minimum contacts" as: "prior negotiations and contemplated future consequences, along with the terms of the contract and the actual course of dealing that must be evaluated in determining whether the defendant purposefully established minimum contacts within the forum." .

[243]Determining whether a court has personal jurisdiction over an out-of-state defendant requires an analysis of the law of the forum state, referred to as the "long-armstatute."

The plaintiff, System One, Direct Access, Inc. ("System One"), was a Delaware corporation with its principal place of business in Miami, Florida. System One's office in Florida owns and operates a computer database providing airline, hotel and car reservation systems for travel agencies. System One also maintains a branch office in New York, New York.

The defendant, Pres-Kap, Inc. ("Pres-Kap"), was a New York travel agency in Rockland County, New York. All of Pres-Kap's business was conducted out of its New York office. In December 1989, System One, through a representative in its New York office, solicited and negotiated a lease contract with Pres-Kap. Under the lease contract, System One provided Pres-Kap with computer terminals and granted on-line access and use to System One's database in Florida in exchange for a monthly fee. The lease contract was subsequently forwarded to System One's office in Florida for final execution. Disputes between the parties were directed to System One's branch office in New York. The lease contract at issue did not have a forum selection clause that would allow System One to sue Pres-Kap in a Florida court in the event of a dispute. But the contract contained a choice-of-law provision that specified Florida law governed the lease.

In March 1991, Pres-Kap stopped making its payment. Subsequently, System One brought an action against Pres-Kap in a Florida state court for breach of the lease contract. Pres-Kap moved to dismiss this action for lack of personal jurisdiction. The circuit court denied the motion to dismiss. On appeal, the court reversed in favor of Pres-Kap and dismissed the action.

The *Pres-Kap* court addressed whether Pres-Kap's connection to System One in Florida through the Internet constituted sufficient minimum contacts that would subject Pres-Kap to personal jurisdiction in Florida.

First, the court analyzed whether Pres-Kap satisfied the two requirements of the minimum contact prong of the personal jurisdiction test.

To ascertain if Pres-Kap had purposefully availed itself of Florida law, the court reasoned that though Pres-Kap may have benefited financially from the information accessed through the computer database, the financial benefit arose from a lease contract negotiated between the two parties in New York. In addition, Pres-Kap conducted all of its business in New York and was "solicited, engaged, and serviced entirely" by System One's branch office located in New-York. Therefore, the court concluded that the purposeful availment test was not satisfied because the lease contract was essentially "a financial gain arising from a New York, not a Florida-based business transaction".

Regarding the foreseeability test of the minimum contacts prong, the *Pres-Kap* court determined that mailing all rental payments and accessing a computer database through the Internet were insufficient contacts and held consequently that Pres-Kap could not reasonably expect to be subjected to suit in a Florida court. The court also stated that contracting with an out-of-state party alone does not establish sufficient minimum contacts. The court did not take into account the additional factor that the lease contract pertained to a computer database located in Florida.

Second, turning to the reasonableness prong, the *Pres-Kap* court determined that "[t]he maintenance of the suit against the defendant, based on the totality of the circumstances, offend[ed] traditional notions of fair play and substantial justice". The court inferred that because the minimum contacts' prong was not satisfied, neither was the reasonableness prong.

Thus, the court reversed the trial court's denial of Pres-Kap's motion to dismiss for lack of personal jurisdiction.

According to Michael J. Santisi, however, the *Pres-Kap* court erroneously failed to invoke the Florida long-arm statute.

First, the court incorrectly ruled that Pres-Kap had not purposefully availed itself of Florida law for two reasons:

(1) the court failed to recognize that Pres-Kap derived direct economic benefits from its on-line access and use of System One's computer database:

According to the Supreme Court in *Burger King corp. v. Rudzewicz,* personal jurisdiction may be established when an out of state defendant "purposefully derive[s] benefit" from the forum state[244].

Under this rule, the United States District Court for the District of Colorado in *Plus System, Inc. v. New England Network, Inc.*[245] held that an out-of-state defendant can purposefully avail itself of a plaintiff's forum state through the Internet because of the economic benefits derived directly from the on-line access and use of the plaintiffs' computer database.

(2) the court failed to recognize that Pres-Kap on-line access and use constituted active participation in the course of performance of the lease contract:

Indeed, according to previous cases, connecting through the Internet constitutes active participation in the course of performance of the contract and is another way to satisfy the purposeful availment test. For instance, in *Computac, Inc. v. Dixie News Co.*[246], the Supreme Court of New Hampshire held that the out-of-state defendant purposefully availed itself by routinely delivering information to the in-state plaintiff by mail or telephone. The court reasoned that the defendant had a sufficient connection with the forum

---

[244]*Burger King,* 471 U.S. at 473-474.
[245]804 F.Supp.111 (D. Colo. 1992).
[246]469 A.2d 1345 (N.H. 1983).

state to justify exercising personal jurisdiction because this activity was continuous and deliberate, and neither unilateral nor isolated.

Likewise, by sending queries for reservation availability information, Pres-Kap had continuous and purposeful contacts with System One in Florida. In turn, the computer database processed the queries and relayed the information back to Pres-Kap. This routine exchange of information during the course of performing the lease contract, was "continuous and deliberate". Therefore, the *Pres-Kap* court erroneously concluded that the computer interaction did no satisfy the purposeful availment test.

This solution is confirmed by *Sherman v. Kansas Aviation Ctr., Inc.*[247], according to which if an out-of-state defendant uses the Internet to provide a product or service to the forum state, then that contact by itself is sufficient to subject the out-of-state defendant to the jurisdiction of the forum state.

Second, in Michael Santisi's opinion, the Pres-Kap court failed to consider all the totality of the circumstances surrounding the Internet connection, in light of the foreseeability test.

He refers to the *Burger King*'s case which said, with respect to situations involving advanced communications:

> "Although territorial presence frequently will enhance a potential defendant's affiliation with a State and reinforce the reasonable foreseeability of suit there, it is an inescapable fact of modem commercial life that a substantial amount of business is transacted solely by mail and wire communications across state lines, thus obviating the need for physical presence within a State in which business is conducted."[248]

Because Pres-Kap contracted with System One and made payments to Florida for the on-line access and the use of the database over a nine year period, it

---

[247] 92-2211-GTV, 1993 WL 191369. at *5 (D.Kan.1993).

[248] *Burger King*, 471 U.S. at 476.

had ample notice that it was subject to jurisdiction in Florida. One particular factor to which the court gave insufficient weight was that Pres-Kap rendered payment to Florida for the on-line access of a computer database located in Florida. Mailing these payments suggested, as did the Florida choice-of-law provision, that Pres-Kap had contracted with a business in the forum state[249]. Furthermore, the *Computac* court held that the foreseeability test was met merely by the defendant's awareness that the contract it entered into was substantially connected to the plaintiff in the forum state[250]. In that case, the out-of-state defendant routinely sent information to the in-state plaintiff for processing. Similarly, by rendering payment for the on-line access, in conjunction with a provision specifying that Florida law governed the previous contracts for such access, Michael Santisi infers that Pres-Kap had adequate notice that System One was substantially connected to Florida.

Finally, the Internet not only provided Pres-Kap with reservation information, but it contributed to Pres-Kap's financial prosperity by booking reservations for its customers. Thus, this on-line access, coupled with the other circumstances, satisfied the foreseeability test and therefore, by failing to consider the Internet in its appropriate context, giving full weight and consideration to this type of advanced communication and its surrounding circumstances, the *Pres-Kap* court erroneously failed to invoke the Florida long-arm statute. Advancements in computer technology have added a new difficulty to personal jurisdiction law and have required courts to take a more adaptive approach.

---

[249]The *Plus System* court also held that the foreseeability test of the minimum contacts prong was satisfied in circumstances remarkably similar to those in Pres-Kap where there was online access: *Plus System* , 804 F. Supp at 118.

[250]*Computac*, 469 A.2d at 1347

Third, the *Pres-Kap* court erroneously reasoned that hosting the suit in a Florida court was unreasonable when holding that the minimum contacts' prong was not satisfied. According to Michael Santisi, the reasonableness prong was satisfied because Pres-Kap failed to show a compelling reason that invoking the Florida long-arm statute would be unduly burdensome.

Indeed, in the event that the minimum contacts prong is satisfied, *Burger King* indicates that the out-of-state defendant must prove that exercising personal jurisdiction would be unduly burdensome[251].

Besides, comparing other cases to *Pres-Kap* illustrates that subjecting an Internet user to the jurisdiction of a distant forum state is not unreasonable: in *Info-Med, Inc. v. National Healthcare, Inc.*[252], 104 the United States District Court for the Western District of Kentucky held that the out-of-state defendant's failure to render payment to the forum state plaintiff was reasonable grounds to exercise jurisdiction. The court recognized that the forum state's "substantial interest in seeing that its residents get the benefit of their bargain" outweighed the defendant's burden of responding to a claim filed against it in a distant forum state.

Similarly, in the *Computac* case, the court, noting that the forum state's "manifest interest" to provide recourse for its residents in the event of a contract dispute outweighed the defendant's burden, found that it was reasonable to exercise jurisdiction over an out-of-state defendant[253]. Comparing these decisions to *Pres-Kap*, it was not unreasonable to subject Pres-Kap as an Internet user to the jurisdiction of a Florida court. The underlying rationale is that if the two tests within the minimum contacts prong are met, then System One has a substantial interest to seek recourse in

---

[251] *Burger King*, 471 U.S. at 477.

[252] 669 F. Supp. 493 (W.D. Ky. 1987).

[253] *Computac*, 469 A.2d at 1348.

its forum state, Florida[254]. Therefore, the *Pres-Kap* court erred by not invoking the Florida long-arm statute.

Another case, nonetheless, *CompuServe v. Patterson*[255], confirmed the *Pres-Kap* court position. It held that the actions of a Texas shareware developer calling CompuServe and leaving a program on the network was insufficient to subject the shareware developer to the jurisdiction of the state where CompuServe was located, even though the CompuServe user agreement states it is "made and performed in Ohio", and that shareware developer's software resides in "the computer system in Columbus, Ohio"[256]. This appears to be one of the first Federal cases, if not the first, to make direct reference to the term "information superhighway," and provides a detailed analysis of existing law, e.g., *International Shoe* and the due process clause of the United States Constitution, and its application to the information age.

The solution adopted by the *Pres-Kap* and the *CompuServe* courts is, however, disputable. To the extent that an Internet user actually knows where the other party with whom it is dealing with, is located, and that the contract pertains to a computer database, from which it thus benefits, located in this same state, it seems reasonable to assume that the party is aware (at least it should be) that it is subject to the laws of this state and thus can expect to be sued in this state (especially if, as in the *Pres-Kap* case, the agreement contains a choice of law clause designated the law of this state). Therefore, in this case, the other party should be given the possibility to sue it in its state.

---

[254]*Burger King*, 471 U.S. at 482-483.

[255]No. C2-94-91, S.D. Ohio 1994, 1995 U.S. Dist. LEXIS 7530.

[256]Brian Livingston, "CompuServe Suit Sparks Freedom-in-Cyberspace Controversy" (Sept. 5, 1994) InfoWorld 29.

2. Alternative dispute resolutions for electronic contracts

The difficulties with electronic transactions with regard to the dispute settlement method is twofold: first, the status of the Internet as a new electronic medium and the rights of Internet users are not well defined in law. To date there are no specific statutes prescribing how electronic transactions are to be conducted, nor have many electronic related disputes been resolved through courts' judgments. Legal guidance can be found only in the general law of contracts and through analogies to existing law applicable to other information technologies such as telegraph and telex. Second, the computer technology industry is rapidly changing and evolving, whereas the disputes involving the technology are better settled when it still applies.
Furthermore, the keys of electronic transactions are to save time and costs.

Thus, considering these characteristics and to be consistent with the objectives which electronic transactions attempt to achieve, the method to settle dispute in the event of a dispute arising out of or relating to the use of the Internet should be one of rapidity and efficacy. That's why arbitration and mediation seem to be the more appropriate ways to solve such disputes, as alternative dispute resolution forms to the classic court system which is slow and uncertain when the applicable law is itself not well defined.
What is more, these procedures offer the benefit of privacy.

But before the arbitration procedure, Richard A. Shiffer advocates that the parties enter into a mediation procedure as the gentler way to solve the

dispute[257]. Mediation, like arbitration, is a quick way to settle disputes. It is based upon the parties themselves controlling the timing of the resolution process and it is not subject to the burdens of bureaucracy. Considering the gap between the speed at which the electronic industry is developing and the snail's pace extension of the law, mediation can be a bridge permitting parties to retain control over their dispute. Like arbitration, the procedure in mediation has the advantage to be private. Finally, mediation has the essential benefit to preserve the business relationship of the parties. Indeed, mediation means "mediated negotiation"[258]. Mediation is voluntary and either party can withdraw at any time. The mediator, in contrast to the arbitrator, does not have the power to decide. He will refrain from even giving his opinion, since his task is to remain neutral, bringing the parties together into an amicable settlement.

But, Richard A. Shiffer acknowledges that should the parties fail to reach an agreement on their dispute through the aforesaid mediation, then the dispute shall be finally resolved by arbitration.

2.1. Under the ABA Model Agreement

The ABA Model Agreement, indeed, recommends to the parties to adopt the arbitration clause of the American Arbitration Association[259]. An advantage to arbitration for trading partners to consider is the fact that an arbitration panel selected to resolve disputes arising out of electronic communications would likely have expertise relating to the technology and

---

[257]Richard A. Shiffer, "The Use of Mediation in Resolving Disputes in Electronic Data Interchange" (1991) 6 Computer Law and Practice 55.

[258]*Id.*

[259]ABA Model Agreement §4.7. American Arbitration Association, Commercial Arbitration Rules 2 (1988).

would be in a better position to readily appreciate the respective responsibilities and faults.

2.2. Under the UNCITRAL Draft Model Statutory Provisions

Notable is the fact that many of the model agreements contain arbitration clauses[260]. Also the UNCITRAL Working Group on EDI, which recommends that consideration be given to electronic procedures for concluding arbitration agreements and to statutory provisions supporting the validity of such arbitration agreements[261].

Conclusion Section 6

We think that if a party, who provides access to its computer databases according to the agreement, and therefore gives benefit to the other party, were to sue it, it should be given the possibility to sue it in its state, since this party may be presumed to have expected such a possibility.

But the best way for the parties to have their dispute settled in a easier and fair manner is to resort to an arbitrator or a mediator.
They should therefore provide for at least an arbitration clause, such as the American Arbitration Association one, if not for a mediation clause associated with an arbitration clause in case the mediation should fail, since these procedures are the more swift and reliable in the electronic

[260]Besides the ABA Model Agreement §4.7, *See* the Australia Interchange Agreement clauses 15.1-15.3, the Canada Interchange Agreement §10.01, the TEDIS European Agreement Article 12.
[261]Report of the UNCITRAL Working Group on EDI, *supra note 58*, n°32.

environment. The arbitror or the mediator won't be hampered by an inadapted law and especially will have the technical knowledge allowing him to judge in a fair fashion.

CONCLUSION

As we have seen, modern electronic contracting practices on the Internet raise a myriad of legal issues regarding the fit between technology and practice, and legal traditions. American case law is just beginning to address the issues raised by Cyberspace. Many US courts openly have expressed frustration with the inadequacy of current law to deal with problems on the Internet.

But if the lack of decided cases is obviously a difficulty in establishing a code of conduct in the Cyberspace world, it has not proved to be an obstacle to the expanding growth of electronic transactions. The failure of the U.C.C to specifically accommodate the electronic communication of data, has not been, however, fatal to the continued growth of electronic commercial practices. The provisions of the Code have a measure of flexibility so that, while the fit is less than ideal, contracts formed with the use of electronic technology have been placed within the coverage of the Code.

Nonetheless, the traditional paradigm of two human actors creating a contract relationship has to be revisited to accommodate interaction of programmed information systems and therefore to better adapt to the new needs of participants. In this age of Cyberspace and global connectivity, reliance on statutes and *stare decisis* cannot keep up with a rapidly evolving technological environment. Traditional law, then, might condemn rules regulating conduct in Cyberspace to perpetual obsolescence.

When policy considerations that underlie an existing rule still make sense as applied to Cyberspace, this rule needs not be completely changed, but at least has to be adapted to encompass the new technology and its new language. For instance, when analogies to new technologies such as the telephone, the fax or the telex make sense when applied to computer technology, the law needs only to adapt to it by taking it into account. That is the case for the validity of the electronic contract, its time and its place of formation.

But sometimes, a new logic is needed for a new technology, without which it impedes its development. For example, the requirements of a "writing" and a "signature" are meaningless and obsolete: the concept of "record" and the new electronic methods of authentication (such as the digital signature), which then need to be clearly defined, is more useful. The risk of errors in the transmission must be redefined since the technical possibility of the computer technology are new and must therefore be taken into account. Also, the hearsay rule and the best evidence rule are not adapted and must be removed concerning electronic messages (the only requirement for an electronic message to be admissible in court being the trustworthiness and reliability of its retention procedure). Finally, the advent of the Internet defies the concepts of sovereignty, territoriality, and even location. Here again, a new approach is needed to determine the law applicable to the transaction and the competent jurisdiction.

Nevertheless, law reform does not appear to be forthcoming and is anyway not the best way to adapt the law since it is a slow process. Law reforms would be rapidly overtaken compared to the computer technology which is taking gigantic steps forward. The technical possibilities offered by

the computer technology, the number and variety of services being offered on-line, are growing at astonishing rapidity. In the face of this very dynamic situation, one ought to be reluctant to impose law that is inflexible and uniform beyond the needs of the situation.

That is why, for the time being, it is preferable to let the parties tailor their own rules adapted to their own present needs. This, through the means of trading partner agreements or interchange agreements. They can, for instance, help the parties to structure their transactions to assure, to the extent possible, that all legal requirements are met.

However, even such agreements have drawbacks. First, the transaction costs involved in complex interchange agreements may inhibit parties from enacting such an agreement or possibly even from implementing electronic communications. Second, it is not certain to what extent the parties are allowed to agree by contract to waive Statute-of-Frauds requirements or to establish their own rules of evidence. Finally, trading partner agreements can only feasibly be used between established trading partners, and are not feasible in an open environment. Here, the need for an external set of default rules increases.

What rules, in the absence of statutes, might grow up to govern the relations among those who deal with each other on a frequent basis, but do not have prior agreements? The suggestion is that electronic practices will become established usages and customs, which will themselves become *de facto* binding and form the Law Cyberspace - following the example of the Law Merchant. Electronic messages themselves which are selected may carry with them certain "interchange profiles" which incorporate technical,

security and legal requirements. The existence of trading partner agreements may, over a period of time, begin to establish the existence of certain trades practices or usages with respect to electronic commerce. In the meantime, industry groups should continue to develop standards with broad application and acceptance, and must work with international organizations to ensure that development of electronic transactions within countries or trading areas has common ground with that taking place in other areas. Such a creation of Law Cyberspace would not only reduce uncertainty, but also protect expectations, provide flexibility, and promote efficiency.

Finally, it may be necessary to conceive the conclusion of international conventions on electronic transactions. Affirmative action, through international treaties, is needed to eliminate the barriers between countries. Much like the United Nations Convention for the International sales of Goods, contracts' matters, including requirements for formation, offer and acceptance, etc., and jurisdictional matters, could be settled by an Internet convention.

Finally, as Richard A. Shiffer says: "[Electronic transactions] is a business with a short history, an active present, and an enormous potential for the future.[262]"

* *
*

[262]Richard A. Shiffer, "The Use of Mediation in Resolving Disputes in Electronic Data Interchange" (1991) 6 Computer Law and Practice 55, p. 56.

BIBLIOGRAPHY

Books

- Baum M. & Perritt H., *Electronic contracting, Publishing and EDI law* (New-Jersey: John Wiley & Sons Inc., 1991).

- Cavazos Edward and Morin Giavino, *Cyberspace and the Law: your Rights and Duties in the On-Line World* (MIT Press, 1994).

- Evans James, *Law and the Net* (Berkeley: Nolo Press, Jan. 1996).

- Johnston David, Johnston Deborah & Handa Sunny, *Getting Canada Online-Understanding the Information Highway* (Toronto: Stoddart Pub. co. Ltd., 1995).

- Katsh Ethan, *Law in a Digital World* (New-York: Oxford University press, 1995).

- Morgan Richard & Stedman Graham, *Computer Contracts Fifith Ed. Commercial Series* (FT Law & Tax, 1996).

- Nimmer Raymond T., *The law of computer technology* (Warren, Gorham, Lavont, 1992).

- Rose Lance, *Netlaw: your Rights on the On-Line world* (Osborne McGraw-Hill, 1995).

- Trotter Hardy I., *The Effects of Electronic Mail on Law Practice and Law Teaching* (Buffalo, 1994).

- Walden Ian, *EDI and the LAW* (London, 1989).

- Wright Benjamin, *EDI, E-Mail and Internet: Technology, Proof and Liability, The law of Electronic Commerce* (Boston: Little, Brown & Co., 2nd ed., 1995).

Articles

- Abeyratne RIR, "Some Recent Trends in Evidential Issues on Electronic Data Interchange - the Anglo-American Response" (1994) 10 Computer law and Practice 41.

- Angel John, "Legal Risks of Providing Services on the Internet" (1995) 11 Computer Law and Practice 150.

- Baired Freddie, "Legal Isssues and the Internet: Heading West Along the Information Superhighway" (1995) 58 Texas Bar Journal 1138.

- Baum Michael S., "Commercially Reasonable Security: a Key to EDI Enforceability" (1991) 6 Computer Law and Practice 52.

- Baum Michael S., "Electronic Contracting in the U.S.: The Legal and Control Context", *in* I. Walden, *EDI and the law*, London, Blenheim Online, 1989, p. 135.

- Bhala Raj, "Self- Regulation in Global Electronic Markets Through Reinvigorated TradeUsages" (1995) 31 Idaho L. R. 863.

- Boss Amelia H., "Electronic Data Interchange Agreements: Private Contracting Toward a Global Environment" (1992) 13 Northwestern J. of Int. Law & Business 31.

- Boss Amelia H., "The Emerging Law of International Electronic Commerce" (1992) 6 Temple Int'l & Comp. L. J. 293.

- Boss Amelia H., "The Internet Commercial Use of EDI and Electronic Communication Technology" (1991) 48 Business Lawyer 1787.

- Boss Amelia H., "Developments on the Fringe: Article 2 Revisions, Computer Contracting, and Suretyship" (1991) 46 Business Lawyer 1802.

- Bradgate R., "The Computer, the Court, and the Curate's Egg: it is Hearsay or Not?" (1991) 7 Computer Law and Practice 174.

- Burnstein Matthew R., "Conflicts on the Net: Choice of Law in Transnational Cyberspace" (1996) 29 Vanderbilt J. of Transnational Law 75.

- Byasse William S., "Jurisdiction of Cyberspace: Applying real world precedent to the virtual community" 30 Wake Forest Law Review 197.

- Castell Stephen, "Evidence, Authentication and Security: is Technology 'Legally Reliable'?" (1991) 6 Computer Law and Practice 46.

- Chesler Lawrance, "Contractual Issues in the Remarketing of Systems" (1991) 11 Computer/Law Journal 247.

- Computer Law Strategist (ed), "Implications of Re Mesa" (1991) 8 Computer Law Strategist 1.

- Davies Clive, "Law and the Internet" (1995) 11 Computer Law & Practice 106.

- Davies Clive, "Legal Aspects of Digital Signatures" (1995) 11 Computer Law and Practice 165.

- DiPaolo Sharon F., "The Application of the UCC Section 2-201 Statute of Frauds to Electronic Commerce" (1993) 13 The Journal of Law and Commerce 143.

- Gliniecki Judith Y. & Ogada Ceda G., "The Legal Acceptance of Electronic Documents, Writings, Signatures, and Notices in International Transportation Conventios: A Challenge in the Age of Global Electronic Commerce" (1992) 13 Northwestern J. of Int. Law & Business 117.

- Gordon Hughes & Cosgrave David, "The Internet--Legal Questions" (1995) 69 Law Institute Journal 326.

- Gordon Mark L. & McKenzie Diana J.P., "A Lawyer's Roadmap of the Information Superhighway" (1995) 13 Journal of Computer & Information Law 177.

- Grayton Brian D., "Canadian Legal Issues Arising from Electronic Data Interchange" (1993) 27 University of British Columbia Law Review 257.

- Gruner Richard, "Electronic Commercial Practices' (1991) 46 The Business Lawyer" 1777.

- Hulbert Bradley J., "Recent Developments in Computer Law: an Update" (1993) 12 Journal of Computer & Information Law 395.

- Johnson Mark A., "Computers Printout as Evidence: Stricter Foundation or Presumption of Reliability" (1992) 75 Marq. L. R. 439.

- Johnson David R. & Marks Kevin A., "Mapping Electronic Data Comunications onto Existing Legal Metaphors: Should we let our Conscience (and our Contracts) be our Guide?" (1993) 38 Vill. L. R. 487.

- Katsh Ethan, "Law in a Digital World: Computer Networks & Cyberspace" (1993) 38 Vill. L. R. 403.

- Kirby, The Hon. Justice Michael, A.C., C.M.G., "Legal aspects of transborder data flows" (1991) 11 Computer/Law Journal 233.

- Kotch Kevin J., "Addressing the Legal Problem of International EDI: the Use of Computer Records as Evidence in Different Legal Systems" (1992) 6 Temple International & Comparative Law Journal 451.

- Kuner Christopher, "Legal Aspects of Encryption in the Internet" (1996) 24 International Business Lawyer 186.

- Lars Davies, "An Introduction to the Legal Principles of the Internet" (1996) 24 International Business Lawyer 151.

- Lloyd Ian, "Shopping in Cyberspace" (1994) 1 Int'l J. of L. and Information Technology 335.

- McKenzie Diana J.P., "Commerce on the Net: Surfing Through Cyberspace Without Getting Wet" (1996) 14 Journal of Computer & Information Law 247.

- McKeon Robert W., "Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena" (1994) 12 Journal of Computer & Information Law 511.

- Millard Christopher & Carolina Robert, "Commercial Transactions on the Global Information Infrastructure: a European Perspective" (1996) 14 Journal of Computer & Information Law 269.

- Morrin John P., "Custom Requirements and International Trade" (1991) 6 Computer Law and Practice 42.

- Miller Clifford G., "Computer-generated Evidence--Implications for the corporate computer user, Part 1" (1990) Computer Law and Practice 178.

- Miller Clifford G., "Computer-generated Evidence--Implications for the corporate computer user, Part 2" (1990) Computer Law and Practice 72.

- Nicoll Christopher, "EDI Evidence and the Vienna Convention" (1995) 95 The Journal of Business Law 21.

- Nimmer Raymond T., "Electronic Contracting: Legal Issues" (1996) 14 Journal of Computer & Information Law 211.

- Nimmer Raymond T., "Uniform Codification of Commercial Law" (1992) 18 Rutgers Computer & Technology Law Journal 465.

- Peritz Rudolph J., "Computer Data and Reliability: A call for Authentication of Business Record Under the Federal Rules of Evidence" (1986) 80 Northwestern Univ. L. R. 956.

- Reed Chris & Walden Ian, "Legal Problems of Electronic Bulletin Board Operators" (1994) 2 International Journal of Law & Information Technology 287.

- Reed Chris, "Advising Clients on EDI Contracts" (1994) 10 Computer Law and Practice 90.

- Reed Chris, "EDI--Contractual and Liability Issues" (1991) 6 Computer Law and Practice 36.

- Reed Chris, "Authenticating Electronic Mail Messages--Some Evidential Problems" (1991) 4 Software L. J. 161.

- Reynolds Phillip, "Admissibility of Computer-produced Documents as Evidence" (1994) 10 Computer Law and Practice 188.

- Ritter Jeffrey B., "Defining International Electronic Commerce" (1992) 13 Northwestern J. of Int. Law & Business 3.

- Rubin Harry, Fraser Leigh and Smith Monica, "US and International Law Aspects of the Internet: Fitting Squares Pegs Into Round Holes" (1995) 3 Int. J. of L. and Inf. Tech. 117.

- Rustad Michael & Eisenschmidt Lori E., "The Commercial Law of Internet Security" (1995) 10 High Technology Law Journal 213.

- Santisi Michael J., "Pres-Kap, Inc. v. System one, direct access, Inc.: Extending the Reach of the Long-Arm Statute Through the Internet" (1995) 13 Journal of Computer & Information Law 433.

- Sherry Donna M., "Choice of law and forum selection" (1991) 7 Computer Law Strategist 3.

- Shiffer Richard A., "The Use of Mediation in Resolving Disputes in Electronic Data Interchange" (1991) 6 Computer Law and Practice 55.

- Trotter Hardy I., "The proper legal regime for 'Cyberspace'" (1994) 55 Univ. Pitt. L. Rev. 993.

- Troye Anne, "Electronic Commerce and the Invoicing Circle" (1995) Computer Law and Practice 158.

- Tunick David C., "How has the Computer Changed the Law?" (1994) 13 Journal of Computer & Information Law 43.

- Walden Ian, "Contractual Harmonisation in the European Union: A New Approch towards Information Technology Law?" (1995) 11 Computer Law and Practice 2.

- Walden Ian, "EDI and the Law: an Introduction" (1991) 6 Computer Law and Practice 34.

- Weiss Peter N., "Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Stepts Toward Developing a Security Policy" (1993) 12 Journal of Computer & Information Law 425.

- Wheble Bernard, "UNCID rules and Interchange Agreements" (1991) 6 Computer Law and Practice 62.

- Wright Benjamin, "Authenticating EDI: the Location of a Trusted Recordkeeper" (1991) Software Law Journal 173.

- Wilkerson Deborah L., "Electronic Contracts under the UCC Cection 2-201 Statute of Frauds: are Electronic Messages Enforceable?" (1992) 41 Kansas Law Review 403.

- Carol Xueref & Pascal Brousse, "EDI: 'Editerms' would help to cope with EDI legal issues" (1992) 1 Computer & Telecoms Law Review 3.

Reports

- Burk Dan L., "U.S. Jurisdiction Over Cyberspace", e-mail message to the CYBERIA-L listserv, Jan. 16, 1995.

- Electronic Messaging Services Task Force, "The Commercial Use of Electronic data interchange- A Report" (1990) 45 The Business Lawyer 1647.

- Insight Conference, "Developing Multimedia Products--Legal and Business Issues", held on April 28-29, 1994, Insight Press, Toronto.

- Office of Technology Assessment, "Legal issues and Information Security", Congres of the United States, Washington, D.C., U.S. government office, Sept. 1994.

- Permanent Editorial Board of the Uniform Commercial Code, "PEB Study Group: Uniform Commercial Code, Article 2 Executive Summary"(1991) 46 The Business Lawyer 1869.

- Report of the Working Group on Electronic Data Interchange (EDI) on the work of its twenty-fifth session, New-York 4-15 January 1993, A/CN.9/373.

- Report of the Working Group on Electronic Data Interchange (EDI) on the work of its twenty-sixth session, Vienna, 11-22 October 1993, A/CN.9/387.

- Report of the Working Group on Electronic Data Interchange (EDI) on the work of its twenty-seventh session, New-York, 28 February-11 March 1994, A/CN.9/390.

- Takach Gabor G.S., "Law in the World Without Borders", The Canadian Institute, Toronto, 14 May 1996.

- United Nations Commission on International Trade Law, Report of the Secretary-General, "Electronic Data Interchange: Preliminary Study of the Legal Issues related to the Formation of Contracts by Electronics Means", New-York, 25 June-6 July 1990.

- Wires David E, "The Security of Information on the Internet: Professional Responsability, Privilege and How Safe is Safe?", The Canadian Institute, Toronto, 14 May 1996.

Documents

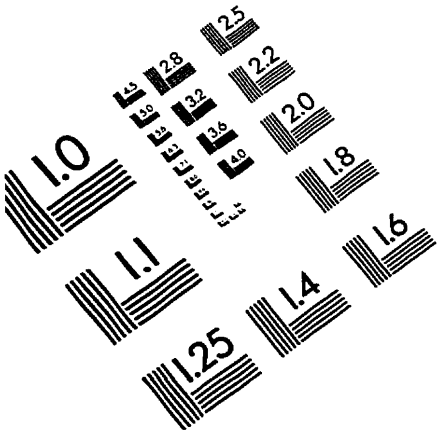
- "Model Electronic Data Interchange Trading Partner Agreement and Commentary" *in* The Business lawyer, vol 45, June 90, p. 1717.

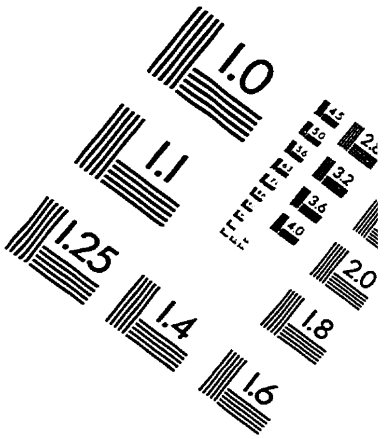
- UNCITRAL Draft Model Statutory Provisions on the Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Data Communication" *in* UNCITRAL Documents A/CN.9/WG.IV/WP62 of 20 July 1994 (for Articles 1-10) and A/CN.9/WG.IV/WP.60 of 24th January 1994 (for Articles 11-15) available under the name of "EDI-TXT" in the Library 0 of the CompuServe Legal Forum.

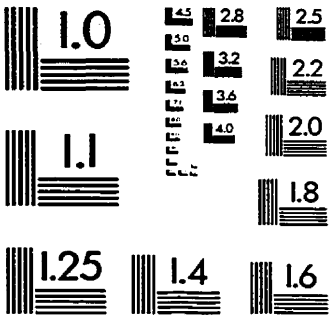
Internet sites (among others)

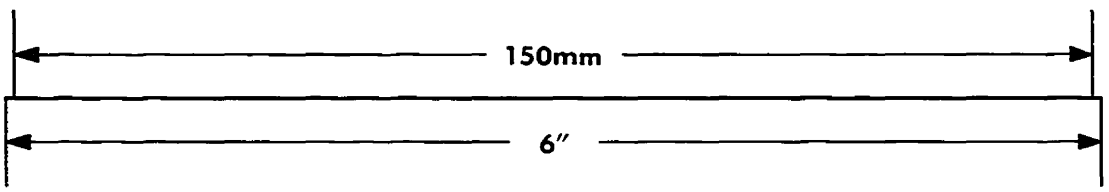
- http://www.lectlaw.com
- http://www.inter-law.com
- http://www.eff.org.com
- http://anause.irv.uit.no/law/nav/trade_law
- http://www.law.cornell.edu/jol/jol.table.htlm
- Internet listserver CYBERIA-L

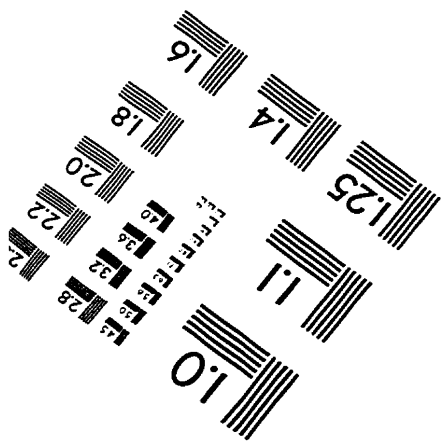
IMAGE EVALUATION
TEST TARGET (QA-3)

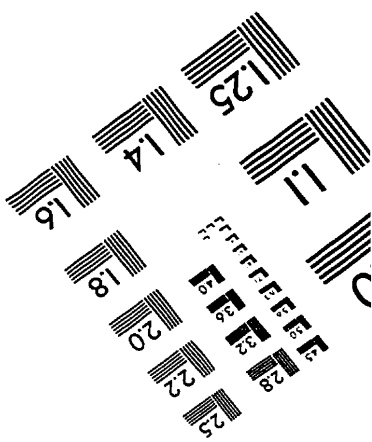












APPLIED IMAGE, Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989