

Electronic contracts

The Impact of the UNCITRAL Model Law on international legal systems

Saudi Arabia information technology development from a legal perspective

Farhan AL-Farhan*

2002

GOD ALMIGHTY SAID:

“ ARE THOSE EQUAL, THOSE WHO KNOW AND THOSE WHO DO NOT KNOW? IT
IS THOSE WHO ARE ENDOWED WITH UNDERSTANDING THAT RECEIVE
ADMONTION.”

THE HOLY QURAN, SORA: AL ZAMER XXXIX, VERSE 9

Contents

Abstract.....	4
---------------	---

Introduction.....	6
Chapter one: The new trend in the international commercial arena	8
1-1 What is the digital signature?	8
1-2 Can Digital Signatures achieve Legal Validity	11
1-3 The legal aspects of the electronic contract.....	12
1-4 Legal issues concerning EDI in the formation of the electronic contract	14
1-5 Do we need electronic contracts?	15
1-6 Protection of electronic contracts through digital signature	16
Chapter tow; Imaginary scenario to create a secured system for electronic contracts under UNCITRAL Model Law	18
2-1 Is co-operation is the right method or is a theoretical approach needed to achieve the harmonization?.....	19
2-2 The legal development.....	22
2-3 The speed of the technical and legal development	Error! Bookmark not defined.
2-4 Is the legal development efficient to secure electronic contracts?	Error! Bookmark not defined.
Chapter three: The legal aspects	Error! Bookmark not defined.
3-1 The legal aspect of electronic contracts.....	Error! Bookmark not defined.
3-2 The enforcement of the electronic contracts.....	Error! Bookmark not defined.
3-3 The recognitions of the electronic contracts in different legal systems	Error! Bookmark not defined.
3-4 The recent development in the international arena.....	Error! Bookmark not defined.
3-5 The US Position.....	Error! Bookmark not defined.
3-6 The EU Position.....	Error! Bookmark not defined.

Chapter four: The international system and how it can help to develop the electronic contracts**Error! Bookmark not defined.**

 4-1 UNCITRAL Model Laws.....**Error! Bookmark not defined.**

Chapter five: Overview and what the future holds**Error! Bookmark not defined.**

 5-1 To what extent does this development afflict the future of On-Line Contracts? ..**Error! Bookmark not defined.**

Chapter six: Case study.....**Error! Bookmark not defined.**

 Saudi Arabia information technology development from a legal aspect..**Error! Bookmark not defined.**

 6-1 the important of IT strategies.....**Error! Bookmark not defined.**

 6-2 The Effect of Information Technology.....**Error! Bookmark not defined.**

 6-3 The Importance of Information Technology**Error! Bookmark not defined.**

 * The Importance of Information Technology in National Development **Error! Bookmark not defined.**

 6-4 IT conditions in KSA.....**Error! Bookmark not defined.**

Conclusion**Error! Bookmark not defined.**

Abstract

Traders and individuals are becoming more and more reliant on information technology to smooth the progress of international business transactions and many spectators believe that full-fledged electronic commerce is nearing a reality.¹ Commonly, the business community uses a system known as electronic data interchange (EDI), because EDI offers advantages such as security (closed network), lower costs and quick and efficient access?. It is thought that any international industry would benefit greatly from its adoption, particularly in the areas of bills of lading. But EDI's development has not been as quick as initially expected due to numerous technical and legal obstacles standing in its way such as the law's insistence on paper-based documentation.²

However, several significant steps have been taken to promote the use of EDI and Internet transactions in the legal profession. The purpose of this paper is to briefly describe these developments and to examine the effects of quality on the legal aspects and the rules and how to enforce the new methods of electronic contracts. We will also discuss the level of technology integration in the market on the global spread of e-commerce and report on the primary aspects from an international perspective. The hypotheses, our target, are to evaluate critically the Model Law UNCITRAL Model Law, EC Directive and we will use Saudi Arabia as an example. This paper intends to examine enacted and proposed legislative attempts to validate contracts in an electronic form and it will also discuss the prospects for international harmonization. Taking UNCITRAL's Model Law on Electronic Commerce as a baseline, we intend to compare and analyse the approaches taken in the United States and the European Union.

* BA. Law King Saud University (Riyadh). LLM. Kent University. PhD student at KENT Law School (Canterbury) Diplomas at, Political economy development, Foreign policy analysis, Organization and strategic management (LSE) London You may contact the author at: fmsa2@ukc.ac.uk

¹ EDI is a new way of doing business and it may be the right way forward to cope with the speed of the new communication systems. .

² Livermore J et al, 'Electronic Bills of Lading and Functional Equivalence', 1998 (2) The Journal of Information, Law and Technology (JILT). <http://elj.warwick.ac.uk/jilt/ecommm/98_2liv/>

Introduction

This paper will examine whether international legal systems are able to create the right legal atmosphere which can make EDI possible and recognise with in the open and closed networks. And if the level of technological integration in the international market is related to the global spread of E-commerce as measured by E-commerce returns; Our inquiry is motivated by the current debate among lawmakers and market contributor's in both sectors; that is traders and consumers, on the relationship between the quality of the international legal rules, and their enforcement and the global spread of E-commerce.³ There appears to be a widespread impression that electronic hackers and poor legal rules and enforcement constitute a major threat to the global spread of E-commerce. In particular, many claim that poor legislation and law enforcement create incentives for misuse (hackers) to intensify their fraudulent activities on the Internet. Such fraud is likely to increase the transaction costs of E-commerce and in some cases may create an incentive for. A market participant to withdraw from E-commerce leading to an overall reduction in E-commerce revenue, however, the validity of these claims has not yet been subjected to any empirical examination.

Why is the legal profession seeking to conduct more of its business over the Internet, Because as the E.Global study (1999)⁴ reported the number of people on-line more than doubled from 44 million in 1997 to 95.4 million in 1998, that is in the space of a year and over the same period the total global revenue from e-commerce tripled, from \$10.8 billion to \$37.6 billion. The revenue figures include both business-to-business (B2B) and business-to-

³ Zabala, 2000; Dolven, Slater, & Song, 2000

⁴ http://www.fdi.dk/site_dir/fdih/uploads/3a6f164f5bb80_eeurope_exec_summ_sales.pdf

consumer (B2C)⁵ depending on the Internet. This study predicted that global E-Commerce Revenue (ECR) has the potential to grow to beyond one **Trillion**⁶ dollars by 2003 if illegal activity on the web can be controlled. Therefore, our argument here will rely on the co-operation⁷ theory as one of the principals that can work to secure the network globally. The projected growth in the size of E-markets is likely to reduce the cost of transacting globally; making E-commerce, in time, a more attractive resource for the processing of transactions compared to the traditional paper-based method and even to electronic data interchanges (EDI).⁸

However, the growth of Internet-based commerce is likely to depend on, among other things, the quality of the legal rules and enforcement in ensuring that transaction data is protected and secured from electronic misuse worldwide. As already stated this concern, if not adequately addressed, is likely to reduce the incentive to transact on the Internet. Consistent with this prediction⁹ it has been shown that high transaction costs led to a reduction of trading liquidity in US equity markets¹⁰. In related studies,¹¹ it has been shown that countries with a poor tradition of law and order have smaller equity and debt markets relative to countries that have high-quality law and order.¹² Presumably, an important aspect of creating the willingness to transact on the Internet can depend on the transaction costs incurred, which tend to decrease as the quality of law and enforcement in a Country increases.

⁵ see, Federica Greggio and Andrea Platania THE COMPETENT JURISDICTION IN B2C CONTRACTS International Company and Commercial Law Review ICCLR 2000,11(6),193-195The main topic of discussion derives from the full adoption of the country of destination rule, set forth in Article 15 of the draft, as to the establishment of the jurisdiction on disputes arising out of business to consumer (B2C) contracts.

⁶ The explosive growth of electronic commerce conducted via the Internet is leading to changes in the ways that people conduct their lives and provoking interest by businesses and governments alike. A key factor in this growth has been the relative lack of regulatory barriers. For the most part, entrepreneurs have been free to create innovative products and services that respond to the opportunities and demands of the new electronic marketplace. The results have been impressive, with global revenues expected to reach half a trillion dollars by 2002 <http://www.microsoft.com/piracy/news/documents/ElectronicCommerceWP.doc>.

⁷ Barbara K. Charles L , and Duncan S. the rational design of international institutions. A journal of political and economic affairs (International Organization)vol.55,no 4, autumn 2001

⁸ Baum, Chen, & Granitsas, 2000 Also see UNCTAD, report 1998.

⁹ Diamond and Verrecchia (1991)

¹⁰ Bartov and Bodnar (1996)

¹¹ La Porta et al. (1997)

¹² Dolven et al. (2000)

So the use of advanced electronic transaction in business could contribute significantly to the efficiency of the market by allowing for the rapid dissemination of information in a more cost-efficient manner than traditional paper-based methods. The commission concludes that the use of advanced technology in business decreases cost relative to the paper-based economy. We can argue that the global spread of E-commerce depends on the level of technology integration (co-operation) in each country. Therefore, we hypothesize that technology integration is positively related to the global spread of E-commerce, particularly in the long-term when economies of scale and costs substitution have taken place.

Chapter one: The new trend in the international commercial arena

1-1 What is the digital signature?

Signing a document is a fundamental legal act, so much so that almost every commercial document of any importance is signed. In spite of this, the signature as a legal artefact has received very little analytical attention.¹³ This is perhaps unsurprising; the paradigm case of the signature is the signatory's name, written in his or her¹⁴ own hand, on a paper document¹⁵ (a 'manuscript signature'), and this is so commonly understood by lawyers and non-lawyers alike that it requires no special conduct. However the English courts have considered

¹³ Authors have examined specific issues, such as the signing of wills and deeds by the use of a mark (Meston & Cusine, 'Execution of Deeds by a Mark' (1993) JLSS 270), the effectiveness of signatures on faxed indictments (Queries (1993) 157 JP 736), electronic signatures of international trade documents (Economic Commission for Europe, Committee on the Development of Trade Working Party of Facilitation of International Trade Procedures, 'Review of definitions of 'Writing', 'Signatures' and 'Document' employed in multilateral conventions and agreements relating to international trade' [1998] 5 EDI LR 3) and signatures of telexes (Smith, 'Electronic Signatures' [1996] 2 CTLR T-17). However, no detailed analysis of English law's basic requirements for a valid signature appears to have been undertaken, although some short articles on digital signatures do make reference to these matters - see e.g. Davies, 'Legal aspects of digital signatures' (1995) 11 CL&P 165..

¹⁴ For ease of reading 'he' and 'his' are used hereafter to stand for 'he/she' and 'his/her', following the convention used for statutory drafting.

¹⁵ This distinction of 'paper document' is important, as will be seen below. The legal concept of document is extremely wide, extending to such things as photographs of tombstones and houses (*Lyell v. Kennedy (No 3)* (1884) 27 Ch D 1), account books (*Hill v. R.* [1945] KB 329) and drawings and plans (*Hayes v. Brown* [1920] 1 KB 250; *J. H. Tucker & Co., Ltd. v. Board Of Trade* [1955] 2 All ER 522). For evidential purposes in civil actions, a document is 'anything in which information of any description is recorded' (Civil Evidence Act 1995 s.13).

variations on this theme from time to time, ranging from simple modifications such as crosses¹⁶ or initials¹⁷, through pseudonyms and identifying phrases,¹⁸ to printed names¹⁹ and rubber stamps.²⁰ In all these cases the courts have been able to resolve the question of whether they constitute a legitimate signature by drawing a correspondence with a manuscript signature.

For this reason, perhaps, it has never been felt necessary to define the term ‘signature’ in the Interpretation Act nor have definitions been included in those statutes, which specifically impose requirements for signatures. However, the increasingly widespread use of electronic communications demands a reassessment of what constitutes a valid signature. Correspondences with manuscript signatures may no longer be appropriate or even possible.²¹

This question is the main point in this section of the paper, Are digital signatures legally valid? To answer this we have to look at it in the context of the contract and the law, Is a written signature required to make any document valid in the eyes of the law²² or not? When we talk about writing we can argue that the digital message or the data message can be

¹⁶ *Baker v. Denning* (1838) 8 A&E 94.

¹⁷ *Hill v. Hill* [1947] Ch 231.

¹⁸ *Cook, In the Estate of (Deceased). Murison v. Cook and Another* [1960] 1 All ER 689 (holograph will signed ‘your loving mother’).

¹⁹ *Brydges v. Dix* (1891) 7 TLR 215; *France v. Dutton*, [1891] 2 Q.B. 208. Typewriting has also been considered in *Newborne v. Sensolid (Great Britain), Ltd.* [1954] 1 QB 45.

²⁰ *Lazarus Estates, Ltd. v. Beasley* [1956] 1 QB 702; *London County Council v. Vitamins, Ltd., London County Council v. Agricultural Food Products, Ltd.* [1955] 2 QB 218.

²¹ The clearest explanation of the reasons why a personal signature might be required is that given by Denning LJ in his dissenting judgment in *Goodman v. J. Eban Ltd.* [1954] 1 QB 550, 561:

‘In modern English usage, when a document is required to be ‘signed’ by someone, that means that he must write his name with his own hand on it. It is said that he can in law ‘sign’ the document by using a rubber stamp with a facsimile signature. I do not think this is correct - at any rate, not in the case of a solicitor’s bill. Suppose he were to type his name or to use a rubber stamp with his name printed on it in block letters, no one would then suggest that he had signed the document. Then how does the facsimile help it. Only by making it look as if he had signed it when in fact he had not done so. It is the verisimilitude of his signature, but it is, in fact not his signature. If a man cannot write his own name, he can ‘sign’ the document by making his mark, commonly the sign of a cross, but in that case he must make the mark himself, and not use a typewriter, or rubber stamp, or even a seal. The virtue of a signature lies in the fact that no two persons write exactly alike, and so it carries on the face of it a guarantee that the person who signs has given his personal attention to the document. A rubber stamp carries with it no such guarantee, because it can be affixed by anyone. The affixing of it depends on the internal office arrangements, with which the recipient has nothing to do with. This is such common knowledge that a ‘rubber stamp’ is contemptuously used to denote the thoughtless impress of an automaton in contrast to the reasoned attention of a sensible person.’

²² Electronic Communications Act 2000 Also See Christopher Reed 2001

treated as a new version of writing. There is no doubt that it can be made by an exchange of electronic messages when it is secured by any type of interruption. If we can provide this kind of security to the 'digital contracts' data message digital contracts could then be treated as any other form of contracts generated, transmitted, received or stored by telegram, fax or telex, which have been recognised and it includes the responsibility to the relating parties.²³ We can use the digital signature as a support tool to increase the confidentiality and validity of **Cryptography**²⁴ and in this case digital signatures can encourage the trade transactions by electronic means with the result of speeding up business and trade globally. There is a special need to make this type of contract valid and reliable, but only if we can find a new legal mechanism that can empower the digital signature and make it into hard evidence. This development could be governed by a self-regulating system or [(Self-Policing) could be a solution to this conflict)], if the interest groups gather to protect their interests through a Trusted Third Party (TTP).²⁵

Nowadays the commonest form of signature is the writing by the signatory of his or her name (or often in practice a stylised and unreadable version of it which is nevertheless consistent and recognisable). But, as stated above, the courts have recognised alternatives to this e.g. the name of an organisation instead of an individual, a signature made by an agent for his principal, or using text or any method other than a name, or by direct or indirect mechanical means (rubber stamp, type-written, printed or those sent by remote telex or facsimile

²⁴ see, *William Fox 2001*. Digital signatures are created and verified using cryptography, the branch of applied mathematics concerned with transforming messages into seemingly unintelligible forms and then back again. Digital signatures are created by performing an operation on information such that others can confirm that a holder of a secret performed the operation and that the signed information has not subsequently changed. In a symmetric key system, both the sender and receiver need to be privy to the secret. In the public key cryptographic system, the holder of the private (secret) key signs information, but anyone with access to the public key can confirm that the signature is valid and as an evidence, see, *Lord, Templeman 1997*. The novel feature of Public Key(PKI) Cryptography is that knowledge of the -public key used to confirm signatures does not reveal information about the private key itself. Also see *F.L.Bauer, Decrypted Secrets: Methods and Maxims of Cryptology 25-26(1997)* and *OECD Guidelines for Cryptography Policy, available at <http://www.oecd.org/dsto/sti/it/secur/prod/e-crypto.htm>*. Also see, Ian Lloyd (2000) pp.261-263

²⁵ see, *William, Fox 2001*. also see, the Insurance Company Proposal as (TTP) at the end of this essay. Examples showing that self regulation or self-policing can provide security and enforcement include traders arranging this services to protect their contract and to encourage trade transactions, families can protect their children from being offended by child pornography, and the state can protect its national security. All these options are under self-interest. see also *Telecommunications Security; Trusted Third Parties; Requirements for TTP Services* available at <http://www.pda.etsi.org/exchangefolder/eg201057V010102p.pdf>. also see, Ian Lloyd (2000) pp.252-255

machine). The common element in all of the above examples is the signatory's intent to build his consideration to validate the document, and where the means adopted can include some uncertainty, it is the objective that may have to be guaranteed by a third party. The problems of proving intention in the case of a digital signature are no greater than for any other kind, and may even prove to be less; and digital signatures overcome the great weakness of electronic media as compared with traditional style of written contracts.

1-2 Can Digital Signatures achieve Legal Validity²⁶

This will depend on the statutory source of the requirement for a written signature, and on how "*writing*" is defined. The general meaning of "*writing*" in legislation is that as laid down in Article 6 of the model law, which states that "*writing*" is a conflicting point due to the nature of the writing within the network when it includes typing, printing, lithography, photography and scanning and other modes of representing or reproducing words in a visible form, Article 9. The effect of this definition is that when a document is in electronic form, the model law distinguishes between three aspects; Writing, Originality, and Signature. We can argue that the model law is able to treat these elements in a better 'legislative' way if; they are gathered into one aspect of security procedures or methods, Article.7 (1). The concept of the written validity of data messages secured by digital signature requires the identification of the originator and a reliable method to support the data message or contract.²⁷ But there is no hesitation with regard to the originality and the signature. We might argue that a document which can be read with any supporting methods (software programs) is like writing a document in pencil; this type of writing is not recognisable in court, due to the ability to change it at any time without the notion of the addressee or the creator of the original. The model law manages to give the functions of writing from a legal perspective. On the other hand the model law can be criticised for not being able to deal with the crucial element of the digital signature when it does not provide the necessary support or protection to the contracting parties. The idea of 'Accessibility and Skills' is the cornerstone to digital signature security. We can argue that, if we manage to control this area by self-regulation, it would limit network misuse, in other words it can provide the digital signature with the

²⁶ Ian Lloyd (2000) pp.244-248

²⁷ See, *Christopher Reed 2001*.

reliability, and security and technical support it needs to ensure that data messages are trustworthy within the network.²⁹ These arguments spell out;

1-3 The legal aspects of the electronic contract

Usage of modern means of communication such as electronic mail and electronic data interchange (EDI) for the purpose of international trade transactions have been increasing rapidly. With the development of information technology and growing Internet accessibility worldwide, international trade is soon expected to change its traditional way of doing business. However, this development may be hindered by the lack of a globally accepted means of using the Internet to create (formate) a contract and make payment. Businesses may run into legal difficulty because they are completely unaware of some of the legal issues that are associated by its nature with E-Commerce.

The latest (2001)³⁰ updating of the UNCITRAL Model Law provides the basic principals with which to control the new trends in EDI/EC Model Law. Through imaginary scenario solutions I will attempt to demonstrate how to develop secure methods to create an electronic commercial contract within the network:

Since we are discussing a digitalized contract we can argue that any “E.Contract” within the network needs to be characterized by the following: *see figure.1*³¹

- | | | |
|----------------------------|---------------|--------------------------|
| 1-Originality | 2-Reliability | 3-Security |
| 4-Insurance /Banks support | 5-Evidential | 6-Third party protection |

²⁹ Any evidence has a character so in this case the Digital Signature with out security and support may be evaluated as Bad Character. The court in this case has to consider the requirements and the methods, which have been used in each case. *Lord Templeman 1997. P.87-88 See also , Electronic Signature Act section 7 (2000).* also see, *David Wall 1998.* and how the cyber crimes are related to this kind of security measures.

³⁰ See, UNCITRAL Model Law 2001 adopted in 05 July 2001. www.uncitral.org

³¹ See, US. Government Working Group on Electronic Commerce, First Annual Report November 1998.

For the predictable future, electronic commerce is likely to continue to have a fundamental similarity to its counterpart in the physical world. For example, there is much to do in the legal and business communities following the arrival of digital signatures, and it is worth noting that people have been entering into unsigned contracts for hundreds of years. Digital signatures may facilitate certain elements of doubt especially when they are used in the formation of electronic contracts or when legal proof is required in the event of a dispute, and it is not only in the legal profession where their validity needs some kind of verification.³² The general theme of this paper is to apply the fundamental argument which agrees with the use of the Internet and it will look into the possibilities of finding secure methods for establishing electronic contracts.³³

The interest in commercial activity has focused attention on the contractual issues raised by the electronic contract itself. For example, can a contract be formed purely by the exchange of electronic communications? Is an electronic communication a "writing"³⁴ that will satisfy the Statute of Frauds? How can communications over the Internet be "authenticated"? Is a digital signature the legal equivalent of a handwritten signature?

I believe that when we use the UNCITRAL Model Law as the applicable law in our scenario we can apply these methods³⁵ to secure the digital signature³⁶ and EDI, which is the main

³² Legislation needs to cover the use of digital signatures in all fields of activities. There does not seem to be a need for discrimination between various ranges of activities. As for hand-written signatures, all types of activities should be embraced. The legal recognition of electronic signatures should be based upon objective, transparent and non-discriminatory criteria. Common liability rules should support the cross-border recognition of signatures and certificates.

³³ When considering digital Signature policy and development procedures in law, the first thoughts should be with the third party. In order to develop a reasonably effective policy framework for dealing with the issues in electronic commerce based on digital signature, however, Article.7 of the Model Law presents an important principle: the normal and traditional signature is just a data message developed on paper, and the ability of copying or "Hacking" this signature still occurs, so in this case both types of signature are breakable but in different ways and methods.

³⁴ Writing is not insufficient because it omits or incorrectly states a term agreed upon," but the contract is enforceable only as to the quantity shown in the writing. UCC 2-201. Where the transaction is between merchants, the writing does not have to be signed by the "charged" party. A confirmation of a contract, if not objected to in writing within 10 days, will bind the merchant receiving the confirmation.

³⁵ Co-operation can be a solution to both the national and international sector, Government Agencies, International Organizations, Multinational Companies, Trade associations, EU, and UN regulators can agree to develop effective tools or they can agree on "SELF REGULATION" among themselves in favour of the protection of contracting parties and consumers on-line.

³⁶ The term electronic signature is used generally to cover any signature in electronic form, including digital signatures. Written signatures are considered legally valid to demonstrate the signatory's identity and intention to be bound by the contents of a document. Hence, written documents and hand-written signatures play the role

aspects in this issue because validity of the digital signature is the first step toward securing EDI actions on the internet allowing the provision of reliable and legal contracts. Therefore the digital signature is the key to electronic contracts.

1-4 Legal issues concerning EDI in the formation of the electronic contract³⁷

The increasingly transparent and liquid nature of global communications via the Internet is encouraging the world trade society to be more involved. The Internet has transformed our communication patterns from being locally oriented into global networks where distance has become invisible to the users. In a sense, the geometry of our communication distance has diminished to a second or to a click.

- Issue "digital certificates" to known consumers that certify their identities when they punch in personal ID numbers at times of transaction;
- Retain a central repository of certificates that can be updated as circumstances warrant (revocation, new certificate issuance, etc.);
- Offer online merchants a means to clear credit/debit/smart card transactions in real-time through merchant bank accounts;
- Certify the identity of the online merchant to the buyer.

Yet this scenario covers every day actions that we are doing now on the Internet without the vital security aspect. *See figure.2*

of securing the identity of the submitting party and the submitted information. Moreover, the signatory by himself or herself performs and materialises the action.

³⁷ See, Farooq Ahmed (2001) the contracts classified here into two groups are together called on-line contracts and are distinguished from off-line contracts. Yet, the legal issue arising from these two types of the electronic contracts are different; it is for this reason that the present classification has been adopted. Many writers include only Electronic Data Interchange in the category of electronic contracts.

1-5 Do we need electronic contracts?

YES we need them; Electronic commerce has the ability to reduce the time span between ordering, delivery, invoicing and payment by using the Internet. Electronic commerce has the ability to create a global digital economy, but generally national and international legislation does not encourage the uptake of this technology; legislation does not seem to be keeping up with technological advances. The technology needed for electronic commerce already exists and is in place, connecting millions people around the world in a seamless network. Any transaction that is done from a distance by telephone, fax, or mail, can be done cheaper, faster, and easier on the Internet. It is almost unavoidable that the most efficient way to reach the most consumers in the global economy will be via electronic commerce. With the technology and the infrastructure in hand, the challenge before us is to deliver on this promise.³⁸

When we talk about the formation of a contract it is obvious that it is an old procedure, one that is developed with time and human behavior, in old *Arab* trading behavior the contract can be fulfilled by body communication which includes the offer, acceptance and consideration under one physical action which is the "*Hand Shake*".³⁹ Therefore our answer is yes, we need electronic contracts. The *hand shake* can be seen as the "**Click**"⁴⁰ due to the development in the international trade transactions and to the benefits that can be achieved if we used the right legal and technological methods. Moreover when we secure these methods this will make EDI equal to written papers and it will be able to create a reliable contract.⁴¹

To ensure that international transactions are secure on the Internet, we have to provide:

³⁸ See, Weitzenboeck (2001) also see, Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internet market (hereinafter referred to as the Electronic Commerce Directive'), O.J.L178.1,17.7.2000.

³⁹ Under UCC 2-204, a contract is "made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract." While this provision may not in itself solve problems that arise in on-line transactions, it, like the general policy of the UCC encourages the finding of a contract where the parties intended one. UCC 2-206 provides that an offer can be accepted in any reasonable manner. This tempers the common law rule that acceptance had to be made via the identical medium by which the offer was made (e.g., a telephonic offer could only be accepted by telephone.) Accordingly, an on-line offer may be validly accepted under the UCC by electronic communication or by telephone, or any other manner that is "reasonable" under the circumstances.

⁴⁰ See, Weitzenboeck (2001), also see, UETA(1999) section 14(2) and section 10

⁴¹ See Caslav (1999)

Reliable Digital Signatures;
Electronic Records and Signature Generally;
Secure Electronic Records and Signatures;
Electronic Contracts Standards;
General Duties Relating to Digital Signatures;
Duties of Certification Authorities; i.e. banks or insurance companies
Duties of Subscribers;
Regulation of Certification Authorities and Repositories;
Government use of Electronic records and Signatures;
Liability of Network Service Providers;
Computer Crime solutions.⁴²

When establishing contractual relationships for the purchase of goods or services over the Internet, a number of legal issues arise, including:

- Has a valid contract been formed?
- With whom has the contract been formed?
- When and where was the contract formed?

To conclude this part, all the answers to all the questions above will be discussed in the imaginary scenario which will be presented in the next part of this paper;⁴³

1-6 Protection of electronic contracts through digital signature⁴⁴

The use of a digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all the following characteristics:

⁴² See, Wall (2001)

⁴³ See, the attachment “proposal of the digital signature security on-line in order of creating electronic contracts under UNCITRAL Model Law 2001.

⁴⁴ See, section 3 on contracts concluded by electronic means in the EC Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internet market(hereinafter referred to as the Electronic Commerce Directive’),O.J.L178.1.17.7.2000.also see, section 2(6) in the Uniform Electronic Transaction Act (1999) (UETA).www.jetaonline.com/jetaoc.html

1. It is unique to the person using it;
2. It is capable of verification;
3. It is under the sole control of the person using it; and

4. It is linked to data in such a method that if the data is changed, the digital signature is invalidated. I intend that this imaginary proposal will cover⁴⁵ the growing use of the Internet for commercial purposes and, the lack of uniform laws for electronic commerce.

Therefore we will now examine this scenario using UNCITRAL Model Law as the solution to the problem of the Internet in order to provide a scenario that can be useful from a legal and practical perspective if the trade and commercial societies adopt these security methods, through “self regulation or self policing”, because they are protecting their interest which can be harmed if they do not take the necessary action to protect themselves. This needs a global regulatory understanding, which can benefit the international trade transactions in the future.

*See the attachment*⁴⁶

⁴⁵ See, William Fox 2001. The question is how? This proposal could help to provide security to the digital signature since the insurance companies were mentioned in the law draft in article 1. This proposal, I think, is a good way to operate but third parties in the contract on line are just an extra contract with an insurance company and it should be regulated to certain limits, in this case both parts of the contract can ensure their digital signature through the insurance company and the conformation of the validity of the contract and the digital signatures when the insurance company issue the policy number. Moreover if one of the parties breach the contract so the insurance company will be responsible for covering the damage to the plaintiff and it will take legal action against the other .In the end the insurance company as the third party will charge both side of the contract due to the high risk in this type of contract. This solution will help to avoid the clash between laws, such as freedom of trade and contracting, in the EU laws.

⁴⁶ Proposal of The Digital Signature Security On-Line in Order of Creating Electronic Contracts Under UNCITRAL Model Law 2001

Chapter tow; Imaginary scenario to create a secured system for electronic contracts under UNCITRAL Model Law

Although the UNCITRAL Model Law on Electronic Commerce is not designed to create equally binding uniform rules throughout the world, it helps to harmonize legal standards with sensible supranational concepts. At the same time it leaves enough leeway for States to add rules that are specific or desired for their legal system additionally, it facilitates further law reform on a global level. This law making method, from international Model Laws to national legislation, may also pave the way for supranational methods to apply these new legal rules for electronic commerce in a uniform or harmonized manner despite the different legal traditions.

If a truly supranational Model Law, like the UNCITRAL Model Law on Electronic Commerce, is the most desired method to regulate electronic commerce, one has to focus on the most important issue regarding Internet transactions, i.e. trust through legal certainty. Legal certainty in Internet transactions does not primarily mean well-balanced⁴⁷ substantive rules but rather access to fast and efficient court proceedings with fast and efficient (electronic) means for enforcing judgments, arbitration awards and other forms of out of court settlements. As long as there are no attempts for a global framework to enforce efficiently the (substantive) rights of consumers, in particular with small amounts in controversy, any transaction over the Internet will remain riskier than using traditional means. Multinational enterprises and other 'repeat players' will always have enough expertise and/or resources to take advantage of the global market presented by the internet, but it is the consumer, however well informed, who will be left high and dry if he wishes to use the global shopping arena and finds himself in a scenario as per our typical case study. The applicable law could certainly be determined by the traditional national rules of private international law, even if this might be difficult, and calls for new approaches or analogies. Therefore procedural rules on a global level have to be established to enable consumers to enforce small claims efficiently. A Model Law could for instance introduce a class action that could be brought not only by individuals but also by

⁴⁷ in other words the transaction level and type can be governed by different laws and some times can reach to conflicts of law when the contract /transaction is cross boarder

consumer associations or other non-governmental organisations monitoring the 'cyber-market'.⁴⁸ The OECD Guidelines on Consumer Redress ('charge-backs') and the UCITA ('electronic self help') have at least touched upon enforcing legal rights in Internet transactions. As the Internet has new and unique features one has to look perhaps also for new and unique means to establish legal certainty. A Model Law establishing certain forms of electronic self-help, more flexible rules to charge back credit cards or even class actions to enforce legal rights efficiently would certainly point in the right direction.

2-1 Is co-operation is the right method or is a theoretical approach needed to achieve the harmonization?

In order to reach the right formula which can secure the EDI/EC at international level .we need to act under the idea of teamwork and this can be achieved if we adopt the co-operation theory in this field.⁴⁹ EDI/EC is like any other international functions which need to be governed under theoretical and legal aspects. Yet it is a different dilemma and that is why it is hard to be analysed lets tasks any other international aspects which need to be regulated. For example with trade and tax we can argue that due to the needs of the past the international trade society managed to control this aspect under uniform rules and it is able to work within different legal systems. We can argue it is matter of international co-operation since the international parties agreed to work under this understanding, it will be the cornerstone to finding the right solutions to the new trend in international trade which takes over the internet. However we can agree that any type of new trend needs laws to govern the relationships between the contracting parties whether they are States or multinational companies or consumers, in the end it needs an organization or an institution to control this development. .Moreover we agree that in order to universalise any kind of activities or actions within the international arena we need to create or found an institution or organisation which will take care of the international order.⁵⁰ And this order can come if we practise it under institutional mechanism:

Membership rules (membership) i.e. WTO

⁴⁸ See, Barbara K. Charles L , and Duncan S. the rational design of international institutions. A journal of political and economic affairs (International Organization)vol.55,no 4, autumn 2001

⁴⁹ see B.P.Rosendoff and H.V.Milner 2001

⁵⁰ see B.P.Rosendoff and H.V.Milner 2001

Scope of issues covered (scope)

Centralization of tasks (centralization)

Flexibility or arrangements (flexibility)

It is clear that electronic contracts can be seen as repeated games.⁵¹ If we implement this theory in the information technology world the co-operation theory will make the law able to cope with the new development. Since IT is becoming more and more efficient in the international arena especially the trade transactions, this will make the co-operation theory a realistic solution in the long term.⁵²

The parties would therefore have to agree to the level of security needed in order to minimise the risk of fraud or tampering. The need for security has also been recognised by UNCITRAL, stating that:

*...it is clear that the legal reliability of EDI techniques requires that high standards be used to determine legal certainty as to the identity of the sender, its level of authorisation and the integrity of the message.*⁵³

It might also be useful for parties to have their system audited by a security expert at various intervals. The security expert should be independent and must ensure that the required security measures have been implemented. This would provide for an added sense of security between the parties.

⁵¹ Electronic contracts are uncounted on the internet ,a huge amount of contracts could be under formation at any time and the internet will not discriminate between what is international or local or what is B2B OR B2C . In this case we have to make the internet work as a universal arena in order to improve the trade transactions to gain more revenue and taxation when it is needed

⁵² see Friedman 1971; and Fudenberg and Maskin 1986

⁵³ *Electronic Data Interchange* Report of the Secretary General. UNCITRAL 246th Session at Vienna 10-28 June (1991) U.N. Doc. A/CN.9/350 at 23

An interesting development concerning EDI security has been the approval of a resolution by the American Bar Association (ABA) dealing with legal-security issues involving electronic data interchange and electronic commerce.⁵³ According to this resolution, the ABA has to:

- Facilitate and promote the orderly development of legal standards to encourage use of information in electronic form, including appropriate legal and professional education;
- Encourage the use of appropriate and properly implemented security techniques, procedures and practices to assure the authenticity and integrity of information in electronic form; and
- Recognise that information in electronic form, where appropriate, may be considered to satisfy legal requirements regarding writing or signature to the same extent as information on paper or in other conventional forms where appropriate security techniques, practices, and procedures have been adopted.

As has already been mentioned, cryptography offers a viable means of providing security. However, the costs of implementing these measures are often quoted as an inhibitor. This problem was addressed in a workshop (conducted by the National Institute of Standards and Technology of Gaithersburg, Maryland) on Security Procedures for the Interchange of Electronic Commerce.⁵⁴ The cost of implementing cryptographic methods would include software licensing, export filing process, overheads and professional training of staff. It was argued that a premature consideration of costs could eliminate other viable options. The parties would therefore have to evaluate their underlying requirements to determine what level of security is required. Since a bill of lading is a document of title and entitles the holder to claim delivery of the goods, the level of security needed would have to be substantially higher than the security required for a normal receipt. Security services will have the added benefit of providing services that are not possible to provide with paper-based techniques. An example of such a service is non-repudiation. This method ensures that the originator of a document cannot deny the origin of the document, thereby providing irrevocable proof of authenticity.

⁵³ ABA Resolution no. 115 approved on August 19, 1992

⁵⁴ The abridged version of the workshop (NISTR 5247) was obtained from the internet. The workshop was conducted by Michael S. Baum, J.D., M.B.A. who chairs the EDI and Information Technology Division and the Information Security Committee, Section of Science and Technology of the American Bar Associations.

Digital signatures are limited in some respects. Parties making use of EDI or digital signatures will often have to revert to a trusted third party to provide security assurance. The third party will be required to date-stamp, store and keep an audited data log of the transaction. This would provide proof of the time of origination and content of the electronic document. Once again, the liability issues arising from the use of a third party will have to be worked out in the interchange agreement.

Proper message or data authentication will also enhance the evidential value of the message. The court will have to be sure that the message submitted as evidence is authentic. Admissibility of EDI evidence will be dealt with later.

2-2 The legal development

Legal Problems

EDI has been the catalyst for a number of changes in the scope and function of the law. Legal reform has however not always kept pace with technological development. The legal problems involved in implementing EDI on a global basis become apparent when viewed against the relevant statutory requirements imposed by the various jurisdictions. Bills of lading have to meet certain statutory and formal requirements before they become legally enforceable. These requirements will now be examined. Therefore the legal development has to be in the same track in both schools of thought such as common and civil law in order to reach the universal understanding to the uniform rules which can govern the electronic contracts.

Electronic Contracts

Electronic contracting brings new challenges regarding the enforcement and validity of such contracts. Computer documentation, such as the bill of lading, which is transmitted electronically, will require an adjustment to legal practice which is mainly geared towards dealing with paper-based documentation.

The main problems regarding electronic contracting will be to comply with the statutory or formal requirements of contracts. These requirements, for example that the contract has to be in a written form, were devised and developed mostly before electronic contracting became a reality. It has been argued that:

[The] three main issues relating to electronic contracting concern the legal formalities, the time and place that the contract was made and the admissibility of computer evidence in civil proceedings.⁵⁵

It is clear that these issues will have to be resolved in order to provide the necessary legal security to facilitate the growing use of electronic contracting. Parties dealing with EDI will need to be assured that the electronic bill of lading is afforded the same statutory recognition as the traditional paper bill of lading.

The Convention on the International Sale of Goods

The 1980 Vienna Convention on the International Sale of Goods (hereafter 'the Convention') deals with the sale of goods which have an international character. The Convention would also be applicable to carriage of goods by sea. Section 2 excludes the sale of goods for domestic use. For present purposes emphasis will be placed on the issue surrounding the admissibility of computer evidence. The bill of lading is evidence of the contract of the evidential issues that are dealt with will therefore also indirectly affect the status of the bill of lading.

Article 11 of the Convention aims to rectify the situation in a number of jurisdictions where computer evidence would be excluded and provides:

A contract of sale need not be concluded in or evidenced by writing and is not subject to any requirements as to form. It may be proved by any means, including witnesses.

In terms of Article 96 a Contracting State can contract out of the provisions in the Convention regarding the manner in which the contract can be evidenced. This means that a Contracting State can preserve its own domestic provisions regarding these matters.

Writing⁵⁶

⁵⁵ Bainbridge, D *Introduction to Computer Law* 3rd Edition Pitman Publishing (1996) at 212

⁵⁶ The Interpretation Act of 1978 defines writing as...typing, printing, lithography, photography and other methods of representing or reproducing words in visible form, and expressions referring to writing are construed accordingly.

Local laws differ significantly on what documents have to be in a written form. Bills of lading in particular are usually required to be in writing because of their importance in international trade. The bill of lading is a document of title and entitles the holder to take delivery of the goods. The Hague-Visby rules which have been enacted into the South African Carriage of Goods by Sea Act 60 do not explicitly require the bill of lading to be in writing. However, the implication is that the bill of lading is a 'document' and has to be 'issued'. Writing is therefore presumed.

In the absence of any express provisions in the Hague-Visby rules, attention has to be focused on the courts. It would depend on a proper interpretation of these requirements by the courts to establish if EDI can meet them. Writing serves an important function in international trade. UNCITRAL has attributed the following functions to the writing requirement:

*...to provide that a document would be legible by all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts.*⁵⁷

The writing requirements of the various domestic laws can be seen as inhibiting the growth of EDI. This was recognised by the United Nations Commission on International Trade Law (UNCITRAL). The preliminary study of UNCITRAL saw these requirements as a major obstacle to the development of EDI.⁶² The UNCITRAL Model Law on Electronic Commerce deals with the writing requirements. Per Article 6:

Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

Article 6(3) then contains a number of exceptions. Should the model law be adopted it would provide a great impetus to the development of EDI. It would be an impossible task to examine the domestic laws of every country where EDI is used. What follows is therefore a brief examination of how the writing requirement is approached in the context of EDI in a number of jurisdictions. These jurisdictions present a significant part of the global shipping trade.

⁵⁷ UNCITRAL *Report of the Working Group on International Payments* 24th session A/CN.9/360 February 1992 at Part III.A.

As a general observation, it can be stated that the writing requirement is liberally interpreted by both common law and civil law jurisdictions. In the context of EDI writing can be seen as any message that is capable of becoming paper-based.

Signature

The purpose of the signature requirement is to authenticate the document. Furthermore, when a signature is affixed to a document or a contract of sale it symbolises an intention to be legally bound. The traditional concept of signing a paper document has to be re-evaluated in terms of the electronic bill of lading. In an EDI transaction no 'human' signature is required. It has been suggested that such a transaction can be electronically *signed* by means of algorithms contained within their data streams to authenticate the identity of the sender.⁷⁹ This would act as a password which in turn can only be read by the recipient if he is in possession of an electronic 'key'.⁵⁸

However, difficulties still exist with replacing the traditional hand-written signature with an electronic signature. The problems involved in implementing electronic signatures are significant. Signature is used to authenticate a document, making it a unique identifying mark. Computers, however, are capable of producing identical sets of signatures (or symbols) thereby eroding the confidence associated with manual signatures. It must be noted that these problems can (and must be) overcome in order to implement EDI fully. Walden notes that:

*If an electronic equivalent [to the traditional signature] satisfies the core requirement of uniqueness and intention to authenticate, it should be capable of being recognised by the law.*⁵⁹

It is suggested that this is the correct approach, and that such uniqueness is technically achievable.

2-3 The speed of the technical and legal development

⁵⁸ The bill of lading is usually signed by the carrier's agent at the port of loading, thereby acknowledging the condition and quantity of the goods when they were put on board.

⁵⁹ Walden *EDI and the Law* Blenheim Online Publishing London 1989

The legal problems created by the internet are mainly due to its speed, dynamic changes, non-physical existence (no 'domicile') and the possibility of making any digitalized content almost instantaneously available to users around the globe. The vast growth of data exchange via the internet is also due to the trifling costs in comparison to telephone calls, sending the information/data via ordinary mail, going to a library, looking endlessly through yellow pages, commuting to a workplace or going shopping in overcrowded department stores with mysterious opening hours.

The uniqueness of the internet lies in the combination of instantaneous access to digitalized data and the ability of anyone having access to the data to copy and to print it out almost endlessly without loss of quality. So the legal problems are in part off springs of digitalized data, including photos and music, and in part result from the non-physical existence of the data.

No other technical development in the past has brought such a change to our daily life: With a fax-machine one can generally send paper-based information to people with a fixed telephone or fax-number. However the information cannot be copied except with a Xerox-machine resulting in the loss of quality. It used to be even more difficult to copy music, photographs or films, but due to the enhanced speed of computers one can send huge quantities of computer-programs, digitalized books, music or photos in a split-second from one continent to another. A website can be accessed by anyone, anywhere in the world⁶⁰

The complexity of the internet becomes clearer when one considers the key legal aspects in various fields of private law:

- Electronic commerce, electronic cash and electronic signatures (authentication);
- Encryption and export control;
- Trademark, patent and copyright protection (intellectual property);
- Database protection;
- Antitrust;
- Privacy (data protection) and spamming;

⁶⁰ Although the website by itself may exclude access from certain domain-names or the internet-browser may be programmed to limit access to certain websites - sometimes even deliberately set by the access-provider.

- Unfair contract terms and consumer protection; and
- Enforcement of legal rights including access to justice⁶¹

These issues affect every country in the world alike because of the unrestricted flow of electronic information through 'cyberspace'. So the internationalisation of law has all of a sudden become a necessity simply because of the internationalisation of daily life.

The above mentioned legal problems are as such much more complex than other technical advances in the past with which private law had to deal with, e.g. classifying intangible electricity and computer-software as 'goods' in sales contracts⁶²

Legal uncertainty in internet transactions regarding the applicable law, evidence and legal redress exists in various fields of law, i.e. private, public, criminal and tax law, and on different levels, i.e. for consumers and multinational companies alike. Nevertheless, there is the undeniable enormous sales potential in electronic commerce and direct (one-to-one) marketing at almost no cost⁶³ This leads to a new form of global competition in markets for goods and services that were nationally isolated in the past because of high transaction costs. The consumer is benefiting from E-Commerce through lower prices because of global competition and the greater transparency of markets. Both consumers and companies are sharing the advantages of E-Commerce, i.e. saving money, therefore allocating their resources in an economically more

⁶¹ The most comprehensive and recent survey of all legal issues involved in all kind of computerized transactions gives *Lloyd, Information Technology Law*, 2nd Ed., London, Edinburgh, Dublin 1997; in German there is e.g. *Lehmann* (Ed.), *Rechtsgeschäfte im Netz - Electronic Commerce*, Stuttgart 1999, *Marly*, *Softwareüberlassungsverträge*, 2nd Ed., Munich 1997 and *Bothe/Kilian*, *Rechtsfragen grenzüberschreitender Datenflüsse*, Cologne 1992.

⁶² See in respect to electricity the US-decisions *Thomas Helvey v. Wabash County REMC* 278 N.E. 2d 608, 610 (1972), *Bellotti v. Duquesne Light Corporation*, 4 UCC Rep.Serv. 2d 1393 (Pa. Common Pleas 1987) and the German decisions RGZ 86, 12, 14 (Reichsgericht (RG) 1914), BGHZ 23, 173 (Bundesgerichtshof (BGH) 1957); and in respect to computersoftware the US-decision *Advent Systems Ltd. v. Unisys Corporation*, 925 F.2d 670 (3rd Cir. 1991) and the German decision of the Federal Court of Justice (Bundesgerichtshof/BGH), JZ 1991, 17, 19.

⁶³ The internet seems to be the 'incarnation' of the life-long dream of advertising and marketing experts, see *Mankowski*, *Das Internet im Internationalen Vertrags- und Deliktsrecht*, *RebelsZ* 63 (1999) 203, 236 et seq. with further references; the global turnover in e-commerce for the year 2000 is cautiously being estimated at US-\$ 200 billion, see *Thorn*, *Verbraucherschutz bei Verträgen im Fernabsatz*, *IPRax* 1999, 1 (International Herald Tribune of 19th March 1998, p. 1).

efficient way, but they also share the disadvantages of additional costs and mistrust caused by legal uncertainty.⁶⁴

So there is a need amongst consumers and companies alike for legal certainty on a global level regarding substantive and procedural rules for internet transactions. This does not necessarily call for a separate and comprehensive 'law of the internet', but it is of vital importance to address the various legal problems created by transactions over the internet on a global level⁶⁵. The internet does not know any borders. Generally, the problem of finding the applicable law to a contract concluded over the internet can be solved within the existing rules of private international law that were unified for the EU-member states by the Rome Convention of 1980⁶⁶. However, the traditional methods for tracking down the place of business or the place where the contract was concluded might create difficulties⁶⁷. This is particularly true where companies have their physical place of business outside the EU because of tax reasons, e.g. in the Bahamas.

Similar problems occur with finding a competent forum under the Brussels Convention on the Recognition and Enforcement of Judgment in Civil and Commercial Matters⁶⁸. Agreements can be concluded anywhere where there is access to the internet. In respect to the fulfilment of an agreement to sell or license software it is absolutely irrelevant where the customer has their actual presence anywhere in the world. Therefore the place of performance does not necessarily present the proper forum under the Brussels Convention, although it has to be stressed that the aforementioned conventions are only in force among EU-member states and the gates of legal uncertainty are wide open beyond these boundaries.

If international uniform law is regarded as a suitable solution for the various legal problems created by the internet, scholarly thoughts are vital about the means to achieve uniform rules to tame the internet 'beast' that

⁶⁴ A good example for the manifold legal problems created by the internet and e-commerce are not only new law journals focussing on these issues (e.g. the German MultiMedia und Recht/MMR or Kommunikation und Recht /K&R) but also brochures of law firms intended to inform their clients of potential risks, see e.g. Electronic Commerce - Internet and E-Commerce Review (Winter 1999/2000) by Taylor Joynson Garrett, London.

⁶⁵ See also *Mankowski*, supra, *RabelsZ* 63 (1999), 203, 207 who gives a good survey over the conflict of laws-problems in contracts and torts in internet transactions.

⁶⁶ European (Rome) Convention on the Law Applicable to Contractual Obligations of June 19, 1980, see text in *Jayme/Hausmann*, *Internationales Privat- und Verfahrensrecht*, 9th ed., Munich 1998, no. 43, p. 112 et seq..

⁶⁷ See *Mankowski*, supra, *RabelsZ* 63 (1999) 203, 222 et seq.; *Mankowski*, *Internet und besondere Aspekte des Internationalen Vertragsrechts* (II), CR 1999, 581, 584 et seq..

⁶⁸ European (Brussels) Convention on the Recognition and Enforcement of Judgments in Civil and Commercial Matters of September 27, 1968, latest version can be found in Official Gazette of the EC No. C 189 of July 28, 1990, p.1 and in *Jayme/Hausmann*, supra, (no. 72), p. 239 et seq..

charges at the national legal orders at the international level. A solution on a merely European level in a 'Fortress Europe' style would be short-sighted and just a first step from a mythological point of view. Admittedly political reality often requires compromises that are far from the best scholarly or practical solutions.

The following analysis focuses on private law issues with consumer protection as the most striking example.⁶⁹ Public, tax and criminal law involve more intrinsic political questions that vary from country to country. Moreover, companies tend to have sufficient resources to hire lawyers to overcome legal uncertainties.

2-4 Is the legal development efficient to secure electronic contracts?

To answer this we can argue that in order to evaluate the recent developments on whether it is efficient to secure the new trend of electronic contracts or not will be demonstrated in the summary:

Can the digital signature be made to be reliable through the banks & insurance companies support?

I assume that even within the legal and secure digital signature we are not sure and this mean that they are safe or smart. Below are four areas of concern:

1. **Standards.** The new laws, UNCITRAL , EC DIRECTIVE and ESGNCA, do not specify any one technology. Naturally each party in this dilemma will say that our argument or ideas are the best.
2. **Real-life applications.** Many businesses have heralded the arrival of legal e-signatures. Businesses will have to buy or build their own public key and encryption infrastructure.

⁶⁹ See in respect to consumer protection in e-commerce, in particular because of the EU Distance Selling Directive (97/7/EG, Abl.EG No. L 144, p. 19-28) the detailed surveys of *Thorn*, supra, IPRax 1999, 1 et seq. and *Arnold*, Verbraucherschutz im Internet, CR 1997, 526 et seq..

3. **Digital divide.** The new laws allow companies to charge more to customers who cannot or will not go online.⁷⁰

4. **Fraud.** Unfortunately digital signatures will not eliminate criminals.⁷¹

To conclude we can argue that all this efforts are just to demonstrate that the electronic contracts and the data message are not lawless, but the model law UNCITRAL may not been understood in the proper way. and in the end of their day the high speed of this technology will leave us with new types of misuse of network and this will continue to challenge the law makers, and will show if they are capable to cope with the new development in EDI. Yet business cannot wait for the law. the implementation for the formation of the contract process and content will increase the probability that a contract is enforceable. if we enforce the electronic contracts this can expand the markets through on-line commerce and , this mean that we don't need restrictions or complicated regulations. This argument can ably a strong basis for transacting business on-line.

⁷⁰ see, payment for paperless trade: are there viable alternatives to the decumbency credit. E.T Laryea : law and policy in international business vol, 33. no1 2001

⁷¹ See, Proposal of the Digital Signature Security on Line under UNCITRAL Model Law 2001 in the end of this paper .

Chapter three: The legal aspects

3-1 The legal aspect of electronic contracts

The interest in commercial activity has focused attention on the contractual issues raised by the electronic medium itself. For example, can a contract be formed by the exchange of electronic communications? Is an electronic communication a "writing" that will satisfy the Statute of Frauds? How can communications over the Internet be "authenticated"? Is a digital signature the legal equivalent of a handwritten signature? The interest in these issues caused the Working Group on Intellectual Property Rights for the National Information Infrastructure to comment on on-line transactions in its recent report. Appendix B contains those comments.

The Model Law applies to any kind of information that is transferred in the form of a data message used in commercial activities. Ocean bills of lading are one kind of document within the scope of the Model Law. However, the legal aspects of bills of lading are key issues of the Model Law developments, as noted in the UNCITRAL Working Group on EDI of its thirtieth session, 26 February - 8 March 1996. This reported that future work could focus on EDI transport documents, with particular emphasis on maritime electronic bills of lading and the possibility of their use in the context of the existing national and international legislation dealing with maritime transport (UN 1995b).

It should be noted, however, that the Model Law has no legal force of its own. Its provisions will have legal enforcement only if they are enacted in national law. For this reason UNCITRAL also adopted a Guide to the enactment of the Model Law (UN 1996).

Application of Legal Requirements to Data Messages

'Electronic Data Interchange' or 'EDI', as defined by the Model Law, means the electronic transfer from computer to computer of information using an agreed standard to structure the information.⁷² The main issues related to EDI which have been discussed internationally and solutions proposed by the Model Law are:

⁷² The Model Law, article 2 (b). For more definitions of EDI see Benjamin W (1989); The BT Electronic Commerce Innovation Centre (1996).

- Legal recognition of data messages;
- Writing or a 'document' requirement;
- Signature requirement; and
- Document of title and negotiability.

The Model Law is based on the recognition that legal requirements for the use of paper documents are the main obstacle to the development of EDI. EDI itself cannot be regarded as an equivalent of a paper document, both in nature and legal aspects. Therefore, the Model Law introduced a new approach known as the 'functional equivalence approach', which is based on an analysis of the functions of paper-based requirements and determining how those functions could be fulfilled through EDI.

3-2 The enforcement of the electronic contracts

Enforceability Click agreements online generally should be enforceable, equivalent to shrink-wrap agreements. Like any agreement, they must meet all the requirements for contract formation, including that the user agreed to the terms of the click agreement. However we will introduce these two cases as examples of the enforceability of the electronic contracts:

*1- ProCD v. Zeidenburg.*⁷³ In the shrink-wrap license case *ProCD, Inc. v. Zeidenburg and Silken Mountain Web Services*, the United States Court of Appeals for the Seventh Circuit, reversing the district court, found that the shrink-wrap license was enforceable even though the license terms were not disclosed to the buyer before the purchase. The Seventh Circuit found that the purchase of the software constitutes an agreement that its use is subject to the terms of the license; if the license terms are unsatisfactory, the buyer may simply return the software. The Seventh Circuit also found that the district court erred in finding that ProCD's effort to limit use of public domain data by means of a license agreement was preempted by copyright law.

*2- Hotmail v. Van\$ Money Pie*⁷⁴. In the recent junk email case *Hotmail Corp. v. Van\$ Money Pie, Inc.*, a U.S. federal court found that a "terms of service" agreement entered into, performed and breached entirely online was enforceable. Hotmail provided a free email service

⁷³ *Procd,inc.,plaintiff-appellant,--v.—Matthew Zeidenberg, and silken mountain web services, defendants- apples.* on appeal from the united states district court for the western district of Wisconsin civil action no. 95-c-0671-honorable Barbara B. Crabb

⁷⁴ *Hotmail corporation, plaintiff, v. Van\$ Money pie inc.; als enterprises, inc.; LCGM, inc.; Christopher moss d/b/a the genesis network, inc.; Claremont holdings ltd.; consumer connections; palmer & associates; and financial research group; and darlene snow d/b/a visionary web creations and/or d/b/a maximum impact marketing, defendants.* no. c-98 JW PVT ENE, c 98-20064 jw. united states district court, N.D. California. April 16, 1998.

that could be subscribed to over the Internet by clicking a click-wrap agreement. Hotmail sued Van\$ Money for breach of the agreement's prohibition on the use of Hotmail's email service to facilitate the transmission of junk e-mail, also known as "spam."⁷⁵ The federal court found that the click-wrap agreement was a legally binding form of Internet-based contract. It also determined that Van\$ Money was bound by the click-wrap agreement solely by clicking on the "I Agree" button after having the opportunity to view the terms of service.

3-3 The recognitions of the electronic contracts in different legal systems

Most Internet business transactions are consumer transactions. Federal and State consumer protection laws address warranties and disclaimers, regulate product documentation, and provide consumers with remedies not otherwise available at common law or under the UCC. A consumer transaction is one involving a product that is used primarily for personal, family, or household purposes. Most consumer protection laws will apply only in the event of a "sale." Transactions that are deemed the functional equivalent of a sale (such as shrinkwrap licenses) may be covered as well.

Legal recognition and evidential value of data messages

Is the data message or the electronic contracts can be treated as a document and whether it be accepted as evidence in courts. In many countries, (both civil law⁷⁶ and common law systems), computerised records are generally admissible as evidence. For example, the English courts have recognised other means of passing on information than paper documents. In *Derby & Co v. Weldon* (No 9) (1991) Vinelott J.

This mean that the recognition of the electronic contracts or the data message is based on the technology and the mechanisms that able to be used in order to protects these new trends in the international business transactions.⁷⁷

⁷⁵ Ian Lloyd (2000) pp.270-274

⁷⁶ Civil law jurisdictions are generally based on the inquisitorial system. This entails that all relevant evidence is usually admissible and the court will then attach the necessary weight to the evidence. The system does not view the trial as a contest between the two opposing parties but rather as an enquiry into establishing the material truth.⁴⁶ The court will take into consideration all the relevant factors in assessing the weight to be attached to the evidence. This is not always an easy task.

Consequently, the admission of computer-generated evidence would not undergo the same scrutiny afforded to the same evidence admitted in a common law (adversarial) system. However, the court would still be faced with the difficult task of determining what weight should be attached to the evidence.

⁷⁷ It should be noted that in some jurisdictions amendment has already been made to the law of evidence in order to support the use of EDI. For example, the Malaysian Evidence (Amendment) Act 1993 (an Act to amend the Evidence Act 1950) defines 'document' as: 'any matter expressed, described, or howsoever represented, upon any substance, material, thing or article, including any matter

A explanation to the dilemma given by the Model Law is provided in Article 4 that information should not be denied value, validity or enforceability only on the justification that it is in the form of a data message.⁷⁸ Article 8 also provides in indication to acceptability and evidential value of data messages in any legal proceedings, that nothing in the application of the rules of evidence shall apply so as to prevent the admission of a data message in evidence on the ground that it is a data message, or if it is the best evidence that the person adducing it could reasonably be accepted to obtain, on the grounds that it is not in its original form. Article 8 is proposed to make it understandable that no matter how the 'best evidence' or 'hearsay' rules apply to data messages, they will not change the legal recognition and evidential value of such data messages.

3-4 The recent development in the international arena

International Uniform Law via Treaties

International treaties creating international uniform law via conventions are the 'classical solution' to achieve legal certainty in international transactions. By now the Vienna Sales Convention of 1980 (Convention on the International Sale of Goods/CISG) is the most successful convention having regard to the number of contracting states and its acceptance in practice.⁷⁹ The success of the CISG is also due to the fact that sales contracts are the most used kind of contract in international transactions⁸⁰ and UNCITRAL has set up an official data bank with court decisions on the CISG⁸¹.

An improvement of international uniform law is supranational rules in different equally authentic languages. Also a treaty only allows for small changes so that identical rules exist in all contracting states and because of

embodied in a disc, tape, film, sound track or other device whatsoever, by means of - (a) letters, figures, marks, symbols, signals, or other forms of expression, description, or representation whatsoever; ...'

⁷⁸ Data message' means information generated, stored or communicated by electronic, optical or analogous means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex and telecopy.

⁷⁹ Pursuant to the UNCITRAL-website <<http://www.un.or.at/uncitral/en.index>> there are 52 contracting states as of 3rd September 1998; the acceptance is mainly due to the supranational rules tailor-made for the practical needs of the global market, e.g. by introducing the 'concept of reasonableness' (Art. 38 (1) CISG ('... practicable in the circumstances ...'), Art. 39 (1) CISG ('... within a reasonable time ...'); see also *Schlechtriem*, Das Wiener Kaufrechtsübereinkommen von 1980 (Convention on the International Sale of Goods), IPRax 1990, 277, 283; *Magnus*, Das UN-Kaufrecht tritt in Kraft!, *RebelsZ* 51 (1987) 123, 125.

⁸⁰ See *von Caemmerer/Schlechtriem-Herber*, Kommentar zum Einheitlichen UN-Kaufrecht - CISG, 2nd ed. Munich 1995, Preambel, no. 5; *Kahn*, Le Droit de la Vente, in: UNIDROIT (Ed.), International Uniform Law, 1988, p. 359.

⁸¹ See <<http://www.un.or.at/uncitral>>; in addition there are excellent websites of different universities giving a full survey also of the internationally (!) available scholarly writings, e.g. Pace University, New York/USA <<http://www.cisg.law.pace.edu>> and University of Freiburg/Germany (<<http://www.jura.uni-freiburg.de/ipr1/cisg>>).

the preparation of the rules as supranational compromises by international working groups, the final convention can easily, dogmatically and politically be accepted by the contracting States.

Disadvantages are that it more often than not takes a couple of years to draft an internationally acceptable convention and entails diplomatic conferences with all the contracting states participating to introduce necessary changes because of its status as a treaty. Moreover, the necessity of compromises between different legal regimes does not necessarily favour the most suitable legal rules but rather those that are politically acceptable among the contracting States.

3-5 The US Position

The traditional writing and signature requirements found in the United States have steadily been eroded by legislation and judicial interpretation.⁸² For example, the Uniform Commercial Code defines 'writing'⁸³ as 'any intentional reduction to tangible form'.⁸⁴ There are also cases in which electronic substitutes for pen and paper have been found to meet Statute-of-Frauds-type legislative provisions.⁸⁵ Some authors argue that slight changes in various legislative schemes, such as using the term 'record' instead of 'writing', coupled with the ability of US courts to adapt a body of case law through analogy between past authority and present

⁸² See Jeff Dodd and James Hernandez, 'Contracting in Cyberspace', (Summer 1998) *Computer Law Review and Technology Journal*, available online at <http://www.smu.edu/~csr/articles.html>, at 23-24.

⁸³ See Smedinghoff (ed.), *Online Law 83* (Prentice-Hall 1996). See Perritt, *Law and the Information Superhighway* 386 (John Wiley & Sons 1996). Also see, UCC§ 1-201(39). United States is actually composed of 51 legal systems (50 states and the federal government), it is possible to take a broad view to some extent about written signature requirements. In the main speaking, contracts and obligations do not have to be in writing unless the law requires otherwise) Other formal requirements in US law include the "contract under seal" and notarisation), which, however, either have little practical importance nowadays (as in the case of the contract under seal), or are so easily satisfied that the justification for their continued existence is questionable (as in the case of notarisation, which in US legal practice generally means nothing more than having a secretary certify a signature upon request). As a signature can be any mark on a message made "with the present intention to authenticate" it), in US law the emphasis is on whether the signer intended to be bound.) *Hillstrom v. Gosnay*, 614 P.2d 466 (Mont. 1980). *Bazak International Corp. V. Mast Industries Inc.*, 73 N.Y.2d 113, 7 U.C.C. Rep. Serv. 2d 1380 (1989). *Joseph Denunzio Fruit Co. V. Crane*, 79 F. Supp. 117 (S.D. Cal. 1948).

⁸⁴ Kate Marquess, 'Sign on the Dot-Com Line: Electronic Signature Act Facilitates Commerce over the Net', (Oct. 2000) 86 *ABA J.* 74.UCC § 1-201 (46).

⁸⁵ Dodd and Hernandez (1998), *supra* note 72, at 14-15.

conditions is entirely sufficient to keep the law abreast with technology.⁸⁶ The expansion of statutory definitions by the courts through interpretation and analogy may eventually establish a coherent set of rules; however, a more pro-active approach is to legislate in the area taking into consideration the broad picture of efficiency and consumer protection. When dealing with the validity of agreements, and in particular those with an international aspect, the business community needs positive legislation to feel secure.⁸⁷

This last point is made in the international business context. There is certainly a case to be made for self-regulatory measures; however, in light of the varying degrees of legal recognition of electronic forms and signatures discussed below, universal acceptance will require some legislative support. After States have agreed that electronic documents and signatures are legally enforceable, the procedures and standards of care in maintaining the infrastructure will no doubt be industry led.

The need for a coherent set of rules that would promote certainty, predictability and security gave rise to action by US authorities at both State and Federal levels. Proposed and enacted legislation to respond to electronic contracting capabilities are heavily influenced by the UNCITRAL Model Law on E-Commerce and reflect the functional equivalent method to writing requirements.⁸⁸ At the national level, the Electronic Signatures in Global and National Commerce Act, known generally as E-Sign, took effect from October 1, 2000.⁸⁹ E-Sign grants electronic contracts the same legal validity as written ones by stating that form may not be the sole basis for denying the document or signature validity.⁹⁰ E-Sign pre-empts State laws to the contrary as an interim measure ensuring that electronic documents and signatures have equal legal standing with handwritten signatures and records until such time as the individual States have adopted uniform legislation.⁹¹

⁸⁶ See, for example, Donnie L. Kidd and William H. Daughtrey, 'Adapting Contract Law to Electronic Contracts: Overview and Suggestions', (2000) 26 *Rutgers Computer & Tech. L.J.* 215.

⁸⁷ Richard Horning, 'Symposium Presentation: Legal Recognition of Digital Signatures - A Global Status Report', (2000) 22:2 *Hastings Comm. & Ent. L.J.* 191, at 199 regarding the German system.at 195.

⁸⁸ Amelia H. Boss, 'Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform', (1998) 72 *Tul. L. Rev.* 1931, at 1943-1944. , at 1933.

⁸⁹ Pub. L. No. 106-229 , 114 stat. 465, (codified at 15 USC §§ 7001 *et seq.* (2000)).

⁹⁰ Jeffrey P. Cunard, Jennifer B. Coplan and George Vradenburg, 'Selected Topics in Internet and E-Commerce Law', (Nov. 2000) 627 *PLI/Pat* 381, at 464-465.

⁹¹ Christopher T. Poggi, 'Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation', (2000) 41 *Va. J. Int'l L.* 224, at 227., at 239.

In July 1999, the National Conference of Commissioners on Uniform State Law (NCCUSL) approved the Uniform Computer Information Transactions Act (UCITA) and the Uniform Electronic Transactions Act (UETA) as Model Laws to be adopted by the States.⁹² UCITA applies to computer information transactions and has been adopted in several States.⁹³ With respect to contract formation, UCITA recognizes ‘authentication’ even if in electronic form,⁹⁴ and provides that electronic contracts are valid if it is shown that ‘the party against which enforcement is sought authenticated a record sufficient to indicate that a contract has been formed and which reasonably identifies the copy or subject matter to which the contract refers’.⁹⁵

UCITA takes contract validity liberalization further by supporting the ability of electronic agents to make binding contracts for their human masters. This includes, for example, electronic data interchange (EDI), networks that allow computer-to-computer exchanges of information in order to create contracts without human involvement during the formation process.⁹⁶ Acceptance and validity are satisfied if the medium is ‘reasonable in the circumstances’.⁹⁷ It is quite apparent that UCITA is intended to operate in a similar fashion to UNCITRAL’s Model Law on E-Commerce through reliance on functional equivalency and avoiding specific technological requirements.

UETA broadly applies to electronic records and signatures in commercial or government transactions.⁹⁸ While its starting point for contract validity is first a matter of functional equivalence, UETA goes beyond the UNCITRAL Model Law on E-Commerce by explicitly deeming electronic signatures and documents to be in satisfaction of laws requiring signed and/or written contracts.⁹⁹ It is important to note that again the proposed

⁹² The NCCUSL Model Acts are available online at http://www.law.upenn.edu/bll/ulc/ulc_frame.htm

⁹³ Cunard, Coplan and Vradenburg (2000), *supra* note 32, at 460.

⁹⁴ UCITA § 102 (a)(6).

⁹⁵ UCITA § 201 (a)(1).

⁹⁶ Kidd and Daughtrey (2000), *supra* note 28, at 227-229.

⁹⁷ UCITA § 203 (1).

⁹⁸ Jeffrey P. Cunard, Jennifer B. Coplan and George Vradenburg, 'Selected Topics in Internet and E-Commerce Law', (Nov. 2000) 627 PLI/Pat 381, at 464-465

⁹⁹ UETA § 7.

law is not technology specific and therefore, just like the UNCITRAL Model Law on E-Commerce, leaves the door open to functional equivalence. The provisions of UETA are meant to compliment existing State laws rather than supersede them as in E-Sign, as well as to provide a more comprehensive scheme.¹⁰⁰

US Law as a model for Internet regulation?

The latest developments under US law show clearly how much attempts to regulate Internet transactions are still in flux. In 1998 it seemed to be very likely that an extremely ambitious project, a new Article. 2B UCC as a single code for all 'transactions in information' would be promulgated in Spring 1999, but the project was suddenly abolished in April 1999. The reasons given for this sudden change were rather vague. The draft Article. 2B UCC was mainly regarded as comprising of too many and too different legal aspects which do not adhere to the same legal regimes under the present US law (contract, copyright and patent law). At the same time the American Law Institute announced that instead of an Article. 2B UCC a new Model Law, the UCITA (Uniform Computer Transactions Act), a streamlined version of the proposed Article. 2B UCC was on the agenda. No one knows yet whether the UCITA will finally receive the approval of the American Law Institute and/or the National Commissioners on Uniform Law or whether a resurrection of Article. 2B UCC is sooner or later envisaged.

3-6 The EU Position

On 13 May 1998 the European Commission first published its *Proposal for a European Parliament and Council Directive on a common framework for electronic signatures*¹⁰¹, and a Directive was enacted in January 2000¹⁰² ('the Directive'). This Directive, once transposed into UK law, will validate certain types of electronic signature.

For the purposes of the Directive, electronic signatures are defined by Article. 2(1) as follows:

¹⁰⁰ For an excellent comparison of E-Sign and UETA, see Patricia Brumfield Fry, 'A Preliminary Analysis of Federal and State Electronic Commerce Laws', 2000, Baker & McKenzie, *Global E-Commerce Law Website*, <http://www.bmck.com/ecommerce/topic-esignatures.htm>.

¹⁰¹ COM(1998) 297 final.

¹⁰² Directive 1999/93/EC on a Community framework for electronic signatures, OJ L13 p. 12, 19 January 2000.

‘1. ‘electronic signature’ means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. ‘advanced electronic signature’ means an electronic signature that meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.’

The Directive establishes a two-tier system of electronic signatures¹⁰³:

- Simple electronic signatures, which have merely to meet the definition in Article. 2(1); and
- Certified advanced electronic signatures, where the identity of the signatory is confirmed by a certificate issued by an appropriate third party¹⁰⁴ and complying with other provisions of the Directive (a ‘qualified certificate’¹⁰⁵) and the certificate is created by means of a secure-signature-creation device.¹⁰⁶

¹⁰³ The terminology of ‘simple’ and ‘certified’ signatures is not found in the Directive, but is adopted here for ease of reference.

¹⁰⁴ A ‘certification-service-provider’, defined in Article. 2(10), i.e. a Certification Authority national accreditation body" means an institution, legally distinct and functionally independent of a certification service provider, charged by a Member State with the elaboration of, and supervision of compliance with, accreditations. <http://www.chiark.greenend.org.uk/pipermail/ukcrypto/1998-April/001484.html>

¹⁰⁵ Article. 2(10). The certificate must fulfil the requirements of Annex I, and it must be issued by a certification-service-provider who meets the requirements of Annex II.

¹⁰⁶ Under Article. 2(6) such a device must meet the requirements of Annex III.

The distinction is important because the main purpose of the Directive is not to make provision for the validity of electronic signatures, but to ensure that national laws do not impose barriers to the free flow of certification services in the European Community.

It should be noted before proceeding with this section that the ‘current EU position’ involves special considerations not present in the US - mainly, the implications of developing uniform laws between sovereign Nations with vastly different legal traditions at the same time. The difficulty in predicting EU behaviour as opposed to that of the US is heightened because it is a novel and not yet fully understood entity. Although the EU borrows ideas, concepts and institutions from existing legal systems, it is incomplete and expanding, thereby leaving its relationship with domestic laws of member countries not yet fully determined.¹⁰⁷ To comprehend the difficulty, one must remember that the goal of the Union is not to create a uniform legal order as such, but to facilitate trade, investment and the mobility of citizens.

Therefore, although harmonization of laws is present in some cases, it is merely one of several means to achieving the overall goal, and therefore is not itself a goal. Despite this, common approaches are necessary at times to facilitate Community goals. The most important legislative tools used by the EU to give effect to its decisions are regulations or directives.¹⁰⁸ Regulations are binding on States when adopted with no internal legislative action necessary. They immediately become part of the member States’ laws and may not be amended by domestic legislation. The total surrender of sovereignty required for regulations tends to limit their use, so the more common method is the directive. This sets out a binding result that must be achieved within a set time period through member State domestic legislation, but leaves the form and method up to the individual States. Use of the directive, therefore, is a far more desirable solution in a union of States containing some very different legal traditions. Harmonization amongst member States appears inevitable given the tools available; however, since the choice of how to implement directives is left to each member, it is minimum harmonization of underlying principles and not specific technical rules. Thus, transaction costs may not be optimized by the electronic commerce community because they still have to respond to different criteria for contract validity in different countries. The recognition of electronic contracts as a general principle after all, does not prevent differing opinions on implementation questions such as whether to use

¹⁰⁷ Noreen Burrows, ‘European Community: The Mega Mix’, in Esin Öricü, Elspeth Attwooll and Sean Coyle, eds., *Studies in Legal Systems: Mixed and Mixing* (Boston: Kluwer Law International, 1996) 297-312.

¹⁰⁸ summary of EU methods of unifying and harmonizing laws through the use of regulations and directives. <http://www.ejcl.org/53/art53-1.txt>

specific rules tied to existing technologies, or if Statute-of-Frauds-type legislation need be rewritten or merely reinterpreted to allow for a functional equivalence exception.

In order to examine the European experience, it is necessary to review the recent use of electronic-contract-related directives and the subsequent treatment by key member States. There are two directives relevant to this study: the Electronic Commerce Directive 2000 (ECD), which was due to be implemented by member States before January 17, 2002,¹⁰⁹ and the Electronic Signatures Directive 1999 (ESD), which was due to be implemented by July 19, 2001.¹¹⁰ Although transactions made under the purview of the Distance Contracts Directive 1997 will certainly involve electronic forms, it is geared to monitoring the content of contracts from a consumer protection standpoint, rather than setting out standards of legally recognized media.¹¹¹ Indeed, it does not specify the type of communication to be used and therefore will be subject to the ECD and the ESD. Whereas this paper is confined to the formal validity of electronic forms, it is not concerned with the content of the Distance Selling Directive, which is directed toward the rights of parties after formation.

The ECD applies to all Information Society services provided by service providers in the EU Information Society Services are defined under Article 2 as including any service ‘normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services’.¹¹² This Directive is meant to be a general electronic commerce framework under which the individual member States are left considerable discretion with respect to its implementation.¹¹³ Article 9 requires States to give effect to electronic contracts and forbids the creation of barriers to their use or the denial of legal validity based solely on form. The obligations and benefits flowing from the ECD apply only within the EU, however, and therefore trade with non-member-country businesses is not particularly facilitated by the Directive.

¹⁰⁹ Council Directive 2000/31/EC, [2000] OJ L178/1, available online at EUR-LEX site http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html (implementation Art. 22(1)).

¹¹⁰ Council Directive 1999/93/EC, [2000] OJ L013/12, available online at EUR-LEX site http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399L0093.html (implementation Art. 13(1)).

¹¹¹ Council Directive 1997/7/EC, [1997] OJ L144/19, available online at EUR-LEX site http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0007.html .

¹¹² Art. 2 incorporates this definition by reference to Art. 1(2) of Council Directive 98/34/EC as amended by Council Directive 98/48/EC that can be found on the EUR-Lex site at http://europa.eu.int/eur-lex/en/consleg/main/1998/en_1998L0034_index.html .

¹¹³ David M. Gourlay and Jeremy Warner, ‘Further Developments in Electronic Commerce in the EU and the UK’, (United Kingdom) (Aug. 2000) *Copyright World* 13-17.

The ESD is a far more detailed directive and sets out a framework for the recognition of electronic signatures and certification service requirements for member States. Article 1 states that the objective of ESD is to facilitate the use of electronic signatures and to contribute to their legal recognition while ensuring the ‘proper functioning’ of the internal market by implementing a legal framework. If this is the case, the ESD will promote cross-border electronic commerce within the EU by encouraging electronic contracts.¹¹⁴ Article 5 provides that ‘electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device’ are equivalent to those in handwritten form. The Article goes on, however, to state that electronic signatures are not to be denied legal effect solely on the basis that they are not produced by a ‘qualified’ source or a secure device. Although the definitions of ‘qualified certificate’ and ‘qualified service provider’ create high standards, the language is essentially technology neutral. The requirements appear to be aimed at ensuring that the security features are as reliable as possible rather than forcing member States to agree upon a single device. The ESD does not name a specific technology, but falls short of neutrality. The definition of ‘advanced electronic signature’ found in Article 2 calls for the following features:

- (a) it is uniquely linked to the signatory;
- (b) it is capable of identifying the signatory;
- (c) it is created using means that the signatory can maintain under his sole control; and
- (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

This goes beyond functional equivalence by requiring a higher standard than one could achieve with handwriting. It does not go so far as to name a specific technology, but it seems to describe a digital signature. Certainly if technological advances lead to a form of identification mark other than a digital signature that meets the requirements of Article 2, it will be acceptable. That fact may on its face lead to the conclusion that the EU is following the UNCITRAL Model Law on E-Commerce to a certain extent. In any event, harmonization of acceptable marks is the goal, first between member States and then on to those countries

¹¹⁴ Caroline Copeland, ‘Digital Signatures: Throw Away Your Pens’, (European Union) (May 2000) 11:5 *Ent. L. Rev.* 112, at 113.

such as Canada and the US, where digital signatures are being used. That conclusion, however, is not yet supported by the practical realities that appear when comparing the actual approaches taken by the individual EU member States at the implementation stage. Furthermore, while the US generally recognizes electronic documents containing evidence of identity, none will be provided under the ESD. If the EU and the US were to adopt similar positions on digital signatures, the harmonization of standards would surely appear based on current industry methods. This, however, may not be the case while electronic signatures remain broadly defined in the US.

EU approaches

It is an open secret that a law-making competition has been going on for quite a while between the US and the EU. The EU has been, so far, quicker than the US:

Another goal of the Directive is the interoperability of electronic signatures. Therefore the Directive introduces the concept of an ‘advanced electronic signature’ that is equivalent to a handwritten signature and not limited to digital signatures¹¹⁵. As the Directive was formally adopted on December 13, 1999¹¹⁶, the member States had, pursuant to its Article. 13, 18 months to implement it into their national laws and to recognize electronic signatures in the same way as handwritten ones, i.e. before 19th July 2001. Therefore the German Signature Act – which focussed just on digital signatures - will just have a preliminary domestic effect.

Global approaches to the regulation of internet transactions

Apart from the EU there are also a few proposals for harmonizing internet related problems with a true worldwide prospectus. The most comprehensive proposal is the ‘**1996 UNCITRAL Model Law on Electronic Commerce**’¹¹⁷ that applies to ‘any kind of information in the form of a data message used in the

¹¹⁵ See Council’s website (<http://europa.eu.int/comm/dg15/en/media/sign/composen.htm>), p. 2.

¹¹⁶ See Council’s website (<http://europa.eu.int/comm/dg15/en/media/sign/99-915.htm>).

¹¹⁷ ‘UNCITRAL Model Law on Electronic Commerce with Guide to Enactment’ of 16 December 1996’ (an additional article 5 bis was adopted in 1998), see UNCITRAL’s website <<http://www.uncitral.org/english/texts/electcom>>.

context of commercial activities’ (Article. 1).¹¹⁸ ‘Data message’ is here defined as:

‘information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy’ (Article. 2 a).

The Model Law deals generally with the formation and validity of (electronic) contracts (Article. 11), the legal recognition of data messages (writing, Article. 6; signature, Article. 7; original document, Article. 8), and specifically with the carriage of goods (transport documents, Article. 17). All in all, the Model Law puts (electronic) data messages in the same category as paper-based messages. Unfortunately, only a handful of States have currently adopted it¹¹⁹.

The Council of the OECD adopted in 1997 ‘**Guidelines for Cryptography Policy**’¹²⁰. The aim of these Guidelines was mainly to facilitate electronic commerce by fostering trust in electronic signatures. The OECD was also in favour of a flexible legal framework allowing the user to choose between different methods of cryptography in an ongoing process of development of (international) standards according to the changes in technology (‘state of art’)¹²¹. OECD recognized that cryptography for the protection of privacy and data security is an essential key to the confidence of users in information and communications infrastructures. Without this ‘electronic confidence’ economic development and world trade would be negatively affected¹²². The Guidelines are no legal rules but policy recommendations primarily aimed at governments’ future enactments in cryptography issues relating to electronic commerce.

¹¹⁸ As to the history of the complex drafting process of the UNCITRAL Model Law on Electronic Commerce, see *Boss*, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform*, 72 *Tulane Law Review* (1998) 1931, 1947 et seq..

¹¹⁹ The 1996 UNICTRAL Model Law on Electronic Commerce has, as of March 5, 2000, been adopted by Columbia, the Republic of Korea, Singapore and the state of Illinois/USA, see UNICTRAL’s website at <<http://www.uncitral.org/eng-index.htm>> , p. 15.

¹²⁰ See more in detail *Lloyd*, supra, p. 483 et seq..

¹²¹ See OECD Guidelines for Cryptography Policy Art. V (Principles) no. 1 (trust in cryptographic methods), no. 2 (choice of cryptographic methods), no 3 (market driven development of cryptographic methods), no. 4 (standards for cryptographic methods) on OECD’s website <<http://www.oecd.org/dsti/sti/it/secur/prod/crypto2.htm>>.

¹²² See Recommendation of the Council concerning Guidelines for Cryptography Policy of 27th March 1997, p. 1 on OECD’s website <<http://www.oecd.org/dsti/sti/it/secur/prod/crypto1.htm>>

Finally, UNCITRAL issued in 1998 ‘**Draft Uniform Rules on Electronic Signatures**’¹²³. These rules favour the concept of a secure electronic signature that is defined by Article. 1 (c) as an electronic signature which is a digital signature, or can otherwise be verified to be the signature of a specific person through the application of a security procedure that is:

- uniquely linked to the person using it;
- capable of promptly, objectively and automatically identifying that person;
- created in a manner or using a means under the sole control of the person using it; and
- is linked to the data message to which it relates in a manner such that if the message is altered the electronic signature is invalidated
- or is commercially reasonable under the circumstances, previously agreed to and properly applied, by the parties.

Given that a data message was authenticated by means of a secure electronic signature, it is presumed by Article. 2 that:

- the data message has not been altered since the time the secure electronic signature was affixed to the data message;
- the secure electronic signature is the signature of the person to whom it relates;
- the secure electronic signature was affixed by that person with the intention of signing the message.

¹²³ See UNCITRAL Working Group on Electronic Commerce, 32nd session (19-30 January 1998), A/CN.9/WG.IV/WP.73 and also UNICTRAL’s website <<http://www.uncitral.org/english/sessions/wg:ec/wp-73.htm>>.

The UNCITRAL rules on electronic signatures are similar to the proposed EU Directive on Electronic Signatures insofar as they also recognize different forms of electronic signatures, not only digital ones. But the value of rebuttable presumptions in favour of electronic signatures in the UNCITRAL draft rules remains doubtful because electronic signatures do not constitute full evidence as handwritten signatures do. So the straightforward EU approach with electronic signatures being equivalent to handwritten ones seems to be methodically sounder. Nevertheless, UNCITRAL is still in draft form and it is still unclear what the final version of the Uniform Rules will contain.

This section attempts to identify some of the underlying factors that lead to key similarities and differences between the legal approach taken in the various countries and regions discussed above. This will help in assessing the prospects for international harmonization or at least common solutions to problems arising from similar facts in different countries. The common baseline of action against which the varying approaches are compared is the UNCITRAL Model Law on Electronic Commerce. It is from there that concepts such as taking the focus off mode and placing it on fulfilment of traditional functions of writing are derived in this paper. The threshold of legal recognition set by UNCITRAL requires that the identification of the sending party and indication of that party's assent to the terms within are present in the electronic contract. This is all made possible by a technology-neutral stance on authentication, which need only be as reliable as appropriate in the circumstances. The legal systems canvassed above range from near imitation of the UNCITRAL approach to heavily regulated, detailed requirements for validity. Factors leading to the divergence are certainly based on different legal structures, cultures and attitudes, and in order to consider the prospect of harmonization in any form it is necessary to identify these elements and speculate on their implications.¹²⁴

The dimensions which affect comparative analysis of these issues include culture, society, economy, history, politics and legal logic.¹²⁵ Legal logic must be considered in light of the other factors and also with

¹²⁴ first step toward such a differentiated set of definitions can be certain international standards which have already been adopted, such as Article 7(1)(b) of the 1996 UNCITRAL Model Law on Electronic Commerce, which defines the security standard an electronic signature must meet as a method "as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement". This in effect sets forth a "reasonableness" standard for written signatures, as it is based on the particular circumstances under which the signature is created and the uses to which it is put. Development of such a standard would have to take place on two levels: first of all, by amending national written signature requirements to bring them in line with the requirements of the Internet age, and secondly, by continuing work on international agreements and policies.

¹²⁵ Hugh Collins, 'Methods and Aims of Comparative Contract Law', (1991) 11 *Oxford J. Legal Stud.* 396, at 398.

consideration of legal processes, institutions and actors.¹²⁶ A further consideration is whether the legal issue is addressed entirely by the identified statutes or if there are other rules that supplement the solutions. Given the infancy of the electronic-contract-related statutes, it is not yet possible to accurately predict how other rules will supplement the proposed and recent amendments to domestic legal systems.

The US is implementing the functional equivalence threshold for legal validity in much the same fashion as contemplated by UNCITRAL. Moreover, electronic signatures will satisfy legal writing and signing requirements under a technology-neutral regime.¹²⁷ The trend is toward letting the market determine how best to regulate the industry. Government-implemented schemes, locking in a particular technology is not consistent with the traditional freedom-of-contract notion with which the parties should govern their activities. With limited exceptions, contractual parties in the US are deemed to be on a level playing field, deciding freely on content and medium. The balance of consumer protection with facilitation of commerce is therefore more receptive in the US of limited standardization of electronic contracts. The overwhelming opinion in the US is that governments should not mandate standards in electronic commerce as this will either lock in outdated technology, thereby causing unnecessary transaction costs, or result in non-tariff trade barriers.¹²⁸ Furthermore, the US economic culture is apparent from the current political disposition, which is less interventionist than that of Germany, for example, and prefers to place reliance on a free market to encourage growth.

The legal institutions and formants in the US further support the competitive use of electronic technology. Part of the reason that consumer protection through stiff electronic signature legislation is not as high a priority as in Europe is that the courts are already equipped to deal with related issues. There is some evidence that the US common law is almost ready to accept electronic records and signatures if they perform all the functions of hard copies and handwriting.¹²⁹ The use of analogy and judicial interpretation is available in the

¹²⁶ John Henry Merryman, 'Comparative Law Scholarship', (1998) 21:4 *Hastings Int'l & Comp. L. Rev.* 771-784.

¹²⁷ With the possible exception of Utah, which is regulating the use of digital signatures only. It is not clear how this will mesh with the states adopting the UCITA and UETA.

¹²⁸ Klaus W. Grewlich, *Governance in 'Cyberspace': Access and Public Interest in Global Communications* (Boston: Kluwer Law International, 1999), at 117.

¹²⁹ See Horning (2000), *supra* note 12, at 195-196.

US to evolve the common law, albeit at a slower pace, with technology.¹³⁰ Thus, judges are encouraged by the system in which they exist to consider the authenticity and weigh consumer protection through the application of functional equivalence criteria.

The apparent departure from the UNCITRAL standard is softened, however, by the allowance for voluntary regulation by the industry, thereby placing reliance on the marketplace. This middle ground is natural considering that historically English contract law was modelled on the commercial transaction.¹³¹ Therefore, English law is more economic and pragmatic than French law, for example. The most relevant principles to the less regulatory scheme found in the UK in relation to the German extreme are the traditional extra weight given to economic consequences in contract, the willingness to allow each party to take care of its own interests and a reluctance to take into account the inequalities between those parties. Influence from Continental Europe and the commercial origins of present-day UK contract law struck a balance whereby electronic contracts and signatures can obtain legal validity but only after formal recognition by various Ministers. Also, market forces can dictate security and authenticity regulation, but with the constant 'parental' threat of a statutory regime if the industry fails in its responsibilities.

crossways the English Channel, functional equivalence of electronic records is accepted in closer accordance with the UNCITRAL Model Law on E-Commerce. So long as a document can be identified with the party creating it and it is recognized under circumstances likely to undertaking integrity, a assumption of power attaches. This is a technology-neutral solution. As for signature requirements, however, the assumption only arises after meeting particular standards that appear technology-neutral, but as a handy matter require digital signature technology. More emphasis is therefore placed on government involvement in the third-party certification of the authenticity process.¹³² a few of the dissimilarity can be accounted for by the civil law tradition in France. Where common law lawyers look to generalizations of explanations to individual disputes, civilian lawyers assume the rules precede the clarifications.¹³³ Legal positivism is the character of a code. Since it is assumed (whether correctly or not) that judges will apply immutable meanings without regard to impractical consequences in order to give effect to the will of the State, more detail is expected.

¹³⁰ See Kidd and Daugherty (2000), *supra* note 28.

¹³¹ Donald Harris and Davis Tallon, *Contract Law Today: Anglo-French Comparisons*, (Oxford: Clarendon Press, 1989) at 386.

¹³² See, the attachment and insurance companies and banks support.

¹³³ Barry Nicholas, *The French Law of Contract*, 2nd ed. (Oxford: Oxford University Press, 1992), at p. 4.

The special problems associated with harmonizing laws between diverse member States inevitably led to directives which left considerable leeway to the enacting State. All three of the EU member States considered here felt the UNCITRAL and US approaches provided too little protection and legal certainty. This in turn produced legislation requiring a higher degree of State involvement. The UK position appears in that respect to be closer to the civil law jurisdictions than to its natural legal correlative in the US common law. Surprisingly, even though there is a strong sentiment amongst some US authors that the common law is capable and willing to apply old rules to new technologies, the prevailing opinion in the UK is that it does not.¹³⁴ This may or may not be a valid opinion, but in any event the barrier is there.

Chapter four: The international system and how it can help to develop the electronic contracts

4-1 UNCITRAL Model Laws

The Model Law on Electronic Commerce was adopted by UNCITRAL in 1996. Its purpose is to help States enhance their legislation with respect to electronic communications and to serve as a reference aid for the interpretation of existing international conventions and other instruments in order to avoid impediments to electronic commerce.¹³⁵ According to Article 1, the law ‘applies to any kind of information in the form of data message used in the context of commercial activities’, but allows for exceptions to be made by individual countries.¹³⁶

The ‘writing’ and ‘signature’ related provisions are contained in Chapter II, entitled ‘Application of Legal Requirements for Data Messages’. Articles 6 and 7 are intended to take the focus off the mode of

¹³⁴ Andrew D. Murray, ‘Entering into Contracts Electronically: The Real W.W.W.’, in: Lillian Edwards and Charlotte Waelde, eds., *Law and the Internet: A Framework for Electronic Commerce* (Portland, Ore.: Hart Publishing, 2000), at 19-20.

¹³⁵ Christoph Glatt, ‘Comparative Issues in the Formation of Electronic Contracts’, (United Kingdom) (Spring 1998) 6:1 *Int’l J.L. & Info. Tech.* 34, at 57.

¹³⁶ UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 (with additional article 5 bis as adopted in 1998), online at <http://www.uncitral.org/en-index.htm>.

communication and place it on the fulfilment of traditional functions of writing. UNCITRAL determined that data messages can satisfy the traditional functions and therefore are 'functionally equivalent'. This is significant because it recognizes that future developments and applications are unforeseeable.¹³⁷ This is preferable to deeming specific communications writings because mere definition of terms will be either too broad to comprehend or too narrow to develop new applications.

Article 6 states that where a law requires information to be in writing, a data message is sufficient if it is accessible to be used for subsequent reference. Article 7, dealing with signature requirements, allows for any method that identifies a person and indicates that person's approval of the information contained in the data message, so long as that method was 'as reliable as was appropriate for the purpose for which the data message was generated or communicated'. The use of functionally equivalent language such as this leaves the Model Law requirements broad enough to allow for new technologies and applications which can meet the traditional purposes of writing and signature requirements. This general 'framework' approach is more conducive to broad international acceptance than a detailed regime of mandatory rules.¹³⁸

UNCITRAL is attempting to support the functional equivalence supplied by Article 7 with the Model Law on Electronic Signatures, which was adopted from the former Draft Rules.¹³⁹ This new law is aimed at harmonizing minimum standards of signature reliability. Article 6(1) states that where the law requires a signature of a person, that requirement is met if an electronic signature is used that is as reliable as was appropriate for the purpose, in the light of all the circumstances, including any relevant agreement. This seems to be in line with current US initiatives. The Working Group on Electronic Commerce identifies non-discrimination against electronic signatures of any type as a fundamental objective of the new law, as evidenced by Article 3.¹⁴⁰ The Working Group did give special attention to digital signatures, however, and the test for e-signature reliability set out in Article 6 seems to describe that type of authenticating mark.

¹³⁷ John D. Gregory, 'Solving Legal Issues in Electronic Commerce', (1999) 32 *Can. Bus. L.J.* 84, at 104.

¹³⁸ A. Brooke Overby, 'Will Cyberlaw Be Uniform? An Introduction to the UNCITRAL Model Law on Electronic Commerce', (Spring 2000) 7 *Tul. J. Int'l & Comp. L.* 219, at 234.

¹³⁹ Working Group on Electronic Commerce 34th sess., Vienna, 25 June - 13 July, 2001, online at <http://www.uncitral.org/en-index.htm> (adopted text link).

¹⁴⁰ 'Draft Guide to Enactment of the UNCITRAL Uniform Rules on Electronic Signatures', 16 August 2000, UN Doc. A/CN.9/WG.IV/WP.86/.

The Model Law on E-Commerce has influenced many States with respect to legislative drafting and proposals. Recent enactments and uniform laws now circulating in Canada and the US were heavily influenced by the Model Law, and drafting committees from the two countries are exchanging ideas on the subjects.¹⁴¹ In the European Union, the Electronic Commerce Directive and the Electronic Signatures Directive were also influenced greatly by the Model Law and Draft Rules.¹⁴² Furthermore, drafting committees for the implementation of these proposed laws appear to be directly influenced by each other's work, thereby reducing diverging interpretations. In spite of this influence, however, harmonization lags well behind technology. This is a product of differing legal systems and a tendency toward comprehensive, detailed law reform in some EU nations contrasted by the less hands-on approach in the US.¹⁴³

¹⁴¹ Poggi (2000), at 238. The Uniform Law Conference of Canada produced its own Model Law based on the UNCITRAL Model. Approved for adoption by Provinces in 1999, the Uniform Electronic Commerce Act (UECA) relies on the functional equivalence approach without requiring authentication from a specified technological source. Saskatchewan's Electronic Documents and Information Act, S.S. 2000, c. E-7.22, for example, contains similar and in some cases identical provisions to the UECA. Nova Scotia's Electronic Commerce Act, S.N.S. 2000, c. 26, received Royal Assent November 30, 2000, and also mirrors the UECA approach to writing and signatures, as does Ontario's Electronic Commerce Act, S.O. 2000, c. 17. Several other provinces have Bills before their legislatures with common approaches along the lines of the UECA. (See Michael Geist, *Internet Law in Canada*, (York University: Captus Press, 2000) at 493-499). This approach is not necessarily dependent on a common law system of interpretation as evidenced by Bill 161 now before the Quebec National Assembly, entitled An Act to Establish a Legal Framework for Information Technology, introduced first as a draft in June of 2000 and later as a full-fledged bill on November 14, 2000. The object of the Draft Bill is stated in s. 1(3) as including the 'functional equivalence of documents and the recognition of their legal value, regardless of the medium used, and the interchangeability of media and technologies'. Therefore, the civil law is also able to contemplate the UNCITRAL Model basic principles. (The text of Quebec Bill 161 can be found online at <http://www.assnat.qc.ca/archives-36leg1se/eng/Publications/Projets-loi/publics/00-a161.htm>.)

¹⁴² See Poggi (2000), at 238.

¹⁴³ see, A. Brooke Overby, 'Will Cyberlaw Be Uniform? An Introduction to the UNCITRAL Model Law on Electronic Commerce', (Spring 2000) 7 *Tul. J. Int'l & Comp. L.* 219, at 234.

Chapter five: Overview and what the future holds

5-1 To what extent does this development afflict the future of On-Line Contracts?

Commercial use of the Internet and on-line services will continue to increase for both the consumer and business-to-business transactions. Many vendors will be experiencing international business earlier than ever before and need to be prepared since such transactions can be an important source of revenue as well as a new set of risks. The on-line trend is moving toward establishing quasi-EDI secure environments where both the vendor and their customers will have more comfort with the medium. Business can't wait for the law. Careful implementation of the contract formation process and content will increase the probability that a contract is enforceable. Finally, businesses looking to expand their markets through on-line commerce should not be awed by the medium. Fundamental principles of contract law and common business sense provide a strong basis for transacting business on-line. nonetheless it will encourage more people to processes their trade transactions via the network with confidant in the future. And this will open the door to a new markets who has been closed in the past or it have been un reachable due to some restrictions and this will lead us to able our case study Saudi Arabia and the affect of UNCITRAL model law and the on-line trans action cross border nature.

Chapter six: Case study

Saudi Arabia information technology development from a legal aspect

According to Toffler ¹⁴⁴, “violence, wealth and knowledge” are the ultimate sources of social power, and their interrelationships define power in society with maximum power being attained by using all three in shrewd conjunction. But this approach ignores the quality of power and the highest quality power comes from applying knowledge and information, which can be used to punish, reward, persuade, transform and augment the available force or wealth. “Winston Churchill once said that ‘empires of the future are empires of the mind’.

Changes in knowledge have and continue to cause enormous power shifts through new systems for creating wealth being based on the mind as opposed to muscle, advanced economies have people acting on information and information acting on people. Japan’s rise in economic status can be contributed to their early heralding and embracement of the *information age* from the 1970’s. Knowledge was the key to economic growth in the 21st century. For example twenty years ago IBM had little competition but now they are just one of many computer manufacturer’s and face stiff competition from a global market.

“Today, in the fast changing, affluent nations, despite all inequalities of income and wealth, the coming struggle for power will increasingly turn into a struggle over the distribution of knowledge,” or rather information.

For any Country to keep any sense of power it is imperative that it keeps up with the developments of the information age. The Kingdom of Saudi Arabia (KSA) has the financial and political stability to be successful but it must not be condemned to call upon foreigners for the accomplishment of tasks indispensable to its survival as a major economic power. It must modernize itself and educate its own people. Why bother with an IT strategy for Saudi Arabia? It would be negligence of the highest order to do otherwise.

KSA has a ‘split personality’ in that it has developed with the aid of foreign expertise mainly western) whose business ethics vary enormously from the high moral, social and religious principles of Islamic society. This makes a study of advanced and expensive IT and the development of an IS strategy and the consequent introduction of a National Information Plan (NIP) into what is a relatively unprepared and non-technological society, of major importance to the Kingdom, and of fundamental importance for the formulation of future national strategies.

¹⁴⁴ Toffler, A., “Power shift: knowledge, wealth, and violence at the edge of the 21st century” Bantam Books, ISBN 0-55-05776-6, November 1990.

6-1 the important of IT strategies

The importance of strategic management has risen significantly in business over the last 40 years but there remains little agreement on what exactly the word 'strategy' means. Ansoff¹⁴⁵ argues that it is the means to the end of effective decision-making behaviour. Mintzberg¹⁴⁶ on the other hand concentrates on actions within ambiguity aimed at achieving business objectives. However it was in the early eighties when 'strategy' came into its own demonstrated by the rise of Michael Porter's influence and the search for competitive advantage etc. Generally IS research has focused on the economic justification of IT, specifically looking at IS, MacDonald concentrated on the alignment between IS and corporate goals, objectives, actions, milestones, budgets and plans. However in most of this work 'strategy' usually concentrates on organisations rather than countries and I believe that the lessons learnt from the growing literature available could be applied at a national level in Saudi Arabia because it can be thought of as an organisation due to its huge governmental influence.

Saudi Arabia has suffered from the misapplication of so many methodologies by westerners ignorant of Saudi/Arabic/Moslem culture; here the legitimacy of the scientific approach still dominates the imagination of most planners. So if a strategy is to be successful it must have the legitimacy of a scientific element, but only within a wider pluralistic approach that takes into account the subtleties of local culture by involving the 'local players' in its development.

I believe that an incrementalist approach (e.g. Mintzberg) is the most appropriate for Saudi Arabia; it would have to be prescriptive to a certain extent and one that stemmed from an active debate with the key stakeholders. The local core competencies and the 'way of doing things' also played a part in the approach and it was important that all the stakeholders treat the process as a learning process so that even if the proposals were not accepted the process itself would be of benefit to Saudi Arabia.

What were the drivers for change? *Figure 1, the character process.*

I consider that some of the previous mistakes made while implementing IT in KSA have been a problem of communication. It is vital to understand the context of the act of communicating within social settings, that context being grounded in the culture of those involved. 'Culture' being the set of beliefs and assumptions associated with any group, community, organization or nation¹⁴⁷. Culture creates the supportive environment for the implementation of the development programmes, similarly, the type and range of programs affect the way culture flourishes or reacts in response to other cultures. KSA is a traditional Islamic society but as stated above most of those currently involved with introducing IT in the Kingdom do not share this culture

¹⁴⁵ Ansoff H.I., "Implementing strategic management", Prentice Hall, Englewood Cliffs, New Jersey, 1984.

¹⁴⁶ Mintzberg H., "Mintzberg on management", Free Press, New York, 1989.

¹⁴⁷ Liecenau J. & Backhouse J., "Understanding Information: An Interdiction", MackMillan London, 1990.

and so there exists a basic mismatch in the communications between the sellers of technology (US, UK, Japan etc) and the buyer. However, this identifies a potential market for Islamic computing and can be used to KSA's advantage provided it gets the strategy right.¹⁴⁸

The uniqueness of KSA and its technological experience requires that the developers of any technological strategy or plan must be part of both the Saudi culture and the culture of technology, no outsider to either group will be able to interpret the information needed from both perspectives.

Below is the strategy that was developed using 'dispositioning';

KSA can no longer rely on its oil income to buy-in the solutions to the problems caused by the ever-increasing global economic complexity. It must develop the required skills amongst its own national workforce and reduce the country's dependence on 'economic mercenaries.

One critical skill-base is expertise in IT, to develop and maintain an IT infrastructure and to improve the quality and timeliness of all decision taking in respect of national and international business. Ways of aiding development need to be developed, i.e. insisting that foreign companies who gain from trade with KSA reinvest some of their profit into IT development. Experts in problem solving and identification need to be linked together into the international business environment, necessary information to the key players needs to be delivered along with clear instructions of the actions that stem from the decisions taken. Concentration must be on relevant software production in areas where KSA has a real chance of creating a commercial competitive advantage, and focusing on the Arabic and Muslim markets, particularly in Arabization, is the most likely to succeed.

It was necessary that those being consulted must have a full understanding of the nature of information systems, in fact systems concepts have recently emerged in KSA and now assume central importance in the thinking and approach of many scientists, technologists, and businessmen. From this stance it was perceived as appropriate that KSA adapt the technology to its unique environment (social, political, organisational and religious). This led to discussions of IS and policy and to the concept of dispositioning and the form and function of a NIP. This also required that KSA be viewed as a system in order to understand its complex disposition in regard to itself, to its environment and to its strategic goals.

The concept of MIS needed to be addressed and the debate over centralisation, decentralisation and outsourcing had to take place so that Saudi decision makers were informed of their importance in modern IT development and could make informed decisions as to which direction KSA should take these complicated issues. It was concluded that KSA must adapt a pluralistic approach that interprets organisations as a collection of groups, each with their own goals but that at a superficial level KSA could consider itself as an organisation.

¹⁴⁸ "Information in Saudi Arabia, Today's Challenges and future horizon", ALiktissad Wal-Aamal, special issue, year no.14, November 1992, pp.25-41 (Arabic)

6-2 The Effect of Information Technology

Today, the world is witnessing a revolution in IT, the development of personal computers and LAN's has opened the way for new uses of the technology. The social implications of this revolution will be tremendous¹⁴⁹. IT has made decision-making increasingly dependent on timely, current, sensitive and precise information.¹⁵⁰ All aspects and levels of social, political and economic welfare of modern societies are affected, countries are developing into 'information societies' that depend on collecting, storing, processing, reading and transferring information. The value of information has become more important, in parallel with a fall in the price of hardware delivered by increased productivity leading to an increase in the importance of secrecy because of the perceived value of information as a commercial resource, thereby increasing the economic gap between rich and poor nations, i.e. Japan has produced 150,000 manufacturing robots compared to the Islamic world that uses only a tiny fraction of that number¹⁵¹.

There is a growing belief that the knowledge gained by a society corresponds directly with the amount of information generated in and by it. 'Information industries'¹⁵² are seen as central to economic development by many sectors of Saudi society and great emphasis is placed on their development. They compete on the international stage, dealing with the transfer and distribution of information as a commodity. Developments in many industries indirectly depend on information sources and computer technology to generate wealth, for KSA enhancement of these fields is vital for national development and KSA must look to information as though it has economic and strategic value. Indeed developing an information industry has become one of the most important aspects of the development plans for many nations.

Peter Drucker¹⁵³ predicted that future organisations will be based on information, and this can be seen as true with the effects of Computer Integrated Manufacturing Systems changing the basic theory of mass production developed during the industrial revolution and overturning ideas of economies of scale.

6-3 The Importance of Information Technology

Technology transfer is vital for any developing nation in terms of the welfare of its citizens, its national security and its economic growth. It has strategic, economic, political and social importance. It is estimated that technology contributes between 30% and 70% to productivity growth¹⁵⁴. Technology products are heavily used in intelligence and defence. The political independence of developing nations depends largely on their economic status¹⁵⁵. Most important of all is that developing nations adapt the technology to suit their

¹⁴⁹ Handy C., "The empty raincoat", Hutchison, London, 1994.

¹⁵⁰ "Industry and Information joint roles", proceeding by ministry of industry and electricity in the 12th national computer conference, King Saud university, Riyadh, Saudi Arabia October 21-24 1990, special studies presented by government ministries and organizations, pp.85-98(Arabic)

¹⁵¹ Rowe R.R., "Information service & use 7", Elsevier Science publishers B.V., North Holland, 1988 pp.189-199.

¹⁵² Bell D., "the social framework of information society", in Detouzos M.L. & Moses J., "THE COMPUTER Age, A twenty year view", mit press Cambridge, Mass., 1979.

¹⁵³ Drucer P., "the effective executive", Heinemann, London, 1986.

¹⁵⁴ Supramanian S. K., "technology, productivity and organization", technological forecasting and social change, 31, pp. 359-371, 1987.

¹⁵⁵ Willenbrock F.K., "Technology transfer and national security", IEEE Technology and society Magazine, sept. 1985, pp.13-15.

own social needs because for as long as these technologies are imported and used along western norms then dependence will continue and the gap will grow even wider¹⁵⁶.

* The Importance of Information Technology in National Development

Driven by new telecommunications technology, the trend towards the globalisation of modern business is a fact of life¹⁵⁷. KSA's leaders recognise that to turn its back on developing links with other networks would be an act of economic folly for KSA. They must try and adapt its IT strategies to its culture by acquiring a high degree of understanding of the effect of information and information systems on national development, while being compatible with the requirements of global business.

The Saudi government has a very centralised and focused planning programme and government spending is the single most important factor in Saudi business meaning that NIP should be delivered so that the flow of information and the means of processing that information is to be available for national development through effective communication of information and the availability of information is inextricably linked to any continuous cultural and economic development of a society without which decision making becomes almost impossible. As KSA is developing, more and more information is being generated and without appropriate means of storing, processing, distributing and retrieving this ever-increasing information, some highly detrimental situations can arise.

It is arguable that the development of a nation is related to the quality of information being communicated around its organisations, and the physical infrastructure of communication channels in the Saudi system are well-established, but a strategic vision of these channels is needed so that relevant information goes to those who need it at the right time.

A National Information Plan(NIP) would provide guidelines on the provision of IT which must be made at the national level so that the problems associated with the individual systems of organisations caused by constant changes and developing technology itself could be used to improve the communication channels at the national level. The role of each organisation in the current scheme of things in generating, distributing, processing, and retrieving information is misunderstood and the culture is lacking where the meaning of information is clearly defined, and the issues of when and to whom it should be communicated are clearly understood.

Any IT strategy developed must increase the Saudi system's ability to generate internal variety so that it can cope with the sudden changes in its environment. In KSA many organisations have invested heavily in state of the art IT systems enabling the Kingdom to develop a sophisticated computerised infrastructure at unprecedented speed but this does vary enormously from one organisation to another. This has compounded to the national communication problems because the national IT objectives were not defined.

How can a policy, or more likely a hybrid, be developed and realised? The uniting factor in the most successful cases is a commonly shared 'vision' about social-economic changes enabled by the exploitation of

¹⁵⁶ Mandoura M., "An Interdiction" to the special studies presented by government ministries and organizations, the 12th national computer conference, King Saud University, Riyadh, Oct. 21-24 1990 (Arabic).

¹⁵⁷ Naisbitt J., "Global paradox", Nicholas Brearley, London, 1994.

the potential of new technologies. Computer societies, national computer centres or other professional, academic or regulatory bodies can all contribute to an agreed national vision.

The policy need to be based on a strategy perspective for a country such as Saudi Arabia and it can be addressed at three levels.

- International;
 - standards and technology issues
 - trade policy issues and response at the WTO

- National;
 - E-commerce policy and strategy
 - special infrastructure to suite the new technology development and speed
 - the state have to be co-operative in order to develop the universal IT legislations

- Business community level.
 - create E-awareness¹⁵⁸ as a public issue
 - training in order to improve the IT and E-commerce
 - the state has to support this development (issue the right legislations)
 - promoting business and government co-operation

6-4 IT conditions in KSA

Current KSA's university graduates are major advocates of PC usage and software process are ridiculously low due to lack of copyright protection but PC's are still not being utilised to their full potential¹⁵⁹. A recent study of informatics in Arab Countries¹⁶⁰ concluded that there is a lack of cooperation and coordination among Arab States. Below is a list of issues and problems related to the application of IT that need to be addressed in the Arab world:

- Integration of the systems, codes and contracts
- Standardisation of operating systems
- Standardisation of quality control of training in Arabic only
- Coordination of exchange data
- Organisation of agencies
- Creation of a strategy for informatics

There is a lack of shrewd IS strategies in the Arab market both as a whole and as individual countries but high investment coupled with education and training could provide many Arab counties with a competitive advantage. Small companies standing alone in these environments are faced with intense and sometimes

¹⁵⁸ 'Eawareness' as a concept is used here to mean both Eliteracy (i.e. the ability to use electronic media) as well as the awareness of the potential of E commerce for business.

¹⁵⁹ "The market to 1990", the Arabian computer news, vol.5 no.2 feb.1990, pp.19-22

¹⁶⁰ Regional seminar for the directors of computer centres in the eastern Arab states, UNESCO-Paris, France 21-22, march 1981 final, royal scientific society, Amman, Jordan April 1981.

unfair competition from multinational companies. No new local company can hope to compete against them without some form of government protection.

Arab countries should place the emphasis on software and particularly Arabization, developed by their own local companies to tie in with Arab culture, at the same time creating local job opportunities and developing IT expertise in-house

How does KSA transfer technology in order to improve the welfare and economic well being of its citizens, to safeguard national security, to furnish political independence, and to close the gap in terms of both wealth and technology? Some problems cannot be solved by throwing money at them so understanding the experiences of others and learning from their experiences are vital to the decision making process.

So what did the disposition approach synthesize out of all the comparative material? When presented to the decision maker's opinion favoured the approaches taken by Japan and Singapore of developing a comprehensive IT industrial policy with certain provisos. Certain aspects of the EU's approach were added in. However opinion was unanimous in that everyone recognised that the importance of the Islamic Faith made KSA different and incomparable to other countries. Free market approaches were dismissed as incompatible for a number of reasons, indeed that is where IT is at present in KSA and it isn't working! In KSA the private sector tends to take its leads from the public sector and the private sector is too small to be influential. Similarly the 'intellectual approach' of publishing a theoretical plan without a corresponding plan of action was seen to be out of the question. That would need a power context before any Saudi takes it seriously and so is problematic for the value judgments underpinning Saudi society. The protectionist approach was rejected since KSA has nothing to protect at the moment and the government of KSA is committed to involvement in the latest round of GATT negotiations, and such an approach would send out the wrong signals.

So since both Japan and Singapore have been successful it was logical to follow their example in the form of a special Saudi hybrid to take into account a different level of infrastructure, both material and human. There was a recognised need for an agreed 'national vision' to be embodied in an explicit national IT strategy that would drive the choices in national information plan NIP, and the formal means of coordinating actions nationally to deliver a situation where the exploitation of the potential new technologies will be possible.

But fundamental to any NIP for KSA is the catch-up priority work on the infrastructure. The necessary resources must be available, society must be prepared to accept and exploit the new technologies, public administration being very important here. KSA also needs to break its dependency on outsiders by reducing the expatriate workforce and lessen the influence of multi-national corporations whilst transferring as much technical knowledge from them as possible.

So in order to prepare (NIP) for KSA we need to develop a suitable infrastructure, change the education systems so as to deliver highly qualified IT experts and managers, ensure there is co-operation between industry, government and training institutions; including the multi-nationals in the equation so that their organizational skill base can be utilised; using the public sector as an exemplar to create an appropriate public perception of technology applications. over all the state has to implements a new laws which can cope with the new trends in the EDI under UNCITRAL model law and it has to be more flexible in this area due to the danger it is represent in the future if the state do not take quick action to prevent the future danger and to avoid to repeat the old mastics.

Now a days Saudi Arabia have to understand that in this new era the technical and economic negotiation take place in the absence of a borders blockades. In this case country like Saudi Arabia need more flexible regulations in order to benefit from the E commerce and the information technology development and to be a new market to such development.

Conclusion

Taking into account the different methods to authenticate users, the most significant protection is that of the private key i.e. the same method that is being used in the commercial (insurance contracts) market and it does seem possible that we can use the same legal features.. Use of some of the techniques and the flexibility that digital signature offers can be effectible from the legal side to make it secure and reliable. UNCITRAL gives the principal of the solution to verify parties identity (Digital Signature) before access is granted. Moreover we manage to explain how the digital signature can be protected against misuse by third parties and how it can be secured from anyone on-line, because it is secured by an insurance contract.

UNCITRAL Model Law includes the solutions to some of the dangers of the digital signature by fulfilling the elements building a public key infrastructure with this criteria for verification of the identity being assured and the certification establishment also complying with other satisfactory security standards (Article 7). The security provided by UNCITRAL Model Law reaches the same grade as security provided by hand-written signatures set under paper-based messages 'if we used the right methods'. Provided that the users get familiarised with the use of digital signatures and electronic messages, the legal solutions to the new technologies described in this paper by the opinions granted by UNCITRAL's and the rules given in the

Proposal of a European Signature Directive are reasonable, adequate and promotional for the usage of digital signed electronic documents with legally binding statements. And what we propose is a scenario that can be useful from a legal and practical perspective if the trade and commercial societies adopted these security methods.

References

A. Brooke Overby, 'Will Cyberlaw Be Uniform? An Introduction to the UNCITRAL Model Law on Electronic Commerce', (Spring 2000) 7 *Tul. J. Int'l & Comp. L.* 219, at 234.

Ahmed Farooq. Electronic Commerce: An Indian Perspective: *International Journal of law and Information Technology*, vol.9 no.2 oxford university press 2001

Amelia H. Boss, 'Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform', (1998) 72 *Tul. L. Rev.* 1931, at 1943-1944.

Anderson, Malcolm 1934. Policing the world: Interlope and the politics of international police co-operation Oxford Clarendon 1989

Andrew D. Murray, 'Entering into Contracts Electronically: The Real W.W.W.', in: Lillian Edwards and Charlotte Waelde, eds., *Law and the Internet: A Framework for Electronic Commerce* (Portland, Ore.: Hart Publishing, 2000), at 19-20.

Andrew D. Murray, 'Entering into Contracts Electronically: The Real W.W.W.', in:

Bainbridge D. *Introduction to Computer Law* 3rd Ed. Pitman Publishing 1996

Baker, S. & Yeo, M. (1999) 'Survey of International Electronic and Digital Signature Initiatives – Part 1', *E-Commerce Law Report*, Vol. 1, No. 8, pp. not available.

Balloon, A. M. (2001) 'From Wax Seals to Hypertext: Electronic Signatures, Contract Formation, and a New Model for Consumer protection in Internet Transactions', *Emory Law Journal*, Vol. 50, pp. 905-937.

Bellamy C and J A Taylor (1998), *Governing in the information age*, Open University Press: Buckingham

Berg, Bruce Lawrence, 1954. Policing in modern society Oxford: Butterworth Heinemann, 1999

Berman, Andrew 'International Divergence The Keys to Signing on the Digital Line' *Syracuse: Journal of International Law & commerce* (28) 2001:125

Breslin, A. J. (2001) 'Electronic Commerce: Will It Ever Truly Realize Its Global

Buckley, P. (1999) 'The Emerging Digital Economy II', [www.ecommerce.gov/ede/chapter1.html], accessed: 17/03/2002.

Catchpole James. *The regulation of electronic commerce: A Comparative analysis of the issues surrounding the principles of establishment 1: International Journal of Law and Information Technology, Vol.9 No.1 Oxford University Press 2001*

Chandler G.F. "Maritime Electronic Commerce for the Twenty-First Century" Paper presented to CMI Panel on EDI June 10th 1997 at Antwerp, Belgium

Chandler, George "The Electronic Transfer of Bills of Lading" *Journal of Maritime Law and Commerce* **20** 1989 at 571-579

Chandler, George *Maritime Electronic Commerce for the Twenty-First Century*. Paper delivered at the centenary of the Comite Maritime International 1997 (50 pages)

Christoph Glatt, 'Comparative Issues in the Formation of Electronic Contracts', (United Kingdom) (Spring 1998) 6:1 *Int'l J.L. & Info. Tech.* 34, at 57.

Christopher T. Poggi, 'Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation', (2000) 41 *Va. J. Int'l L.* 224, at 227.

Church, D., Pullen, M. & Winn, J. K. (1999) 'Recent Developments Regarding U.S. and EU Regulation of Electronic Commerce', *The International Lawyer*, Vol. 33, No. 2, pp. 347-365.

Cronin, Mary J. Doing business on the Internet: how the electronic highway is transforming A. - New York; London: Van Nostrand Reinhold, 1994

David M. Gourlay and Jeremy Warner, 'Further Developments in Electronic Commerce in the EU and the UK', (United Kingdom) (Aug. 2000) *Copyright World* 13-17.

De Boer Th.M. *The Missing Link: Some thoughts on the relationship between private international law and comparative law* in Boele-Woelki *et al* Martinus Nijhoff (Dordrecht) 1994

Debatista C. "Incoterms in Practice" ICC Publication 1995

Delatista, C. *Incoterms in Practice* ICC Publication 1995

Directive 1999/93/EC of The European Parliament and of The Council of 13 December 1999 on Community Framework for Electronic Signatures. *Official Journal of the European Communities*, OJL13, P.12, See also <http://www.europa.eu.int/comm/internal_market/en/media/sign/dir99-93=ecEN.pdf>

Donald Harris and Davis Tallon, *Contract Law Today: Anglo-French Comparisons*, (Oxford: Clarendon Press, 1989) at 386.

Draft Guide to Enactment of the UNCITRAL Uniform Rules on Electronic Signatures', 16 August 2000, UN Doc. A/CN.9/WG.IV/WP.86/.

Eiselen G.T.S. "Elektroniese Dataverwisseling en die Bewysreg" *THRHR* 1992(5)

Eiselen S. "The Electronic Data Interchange Agreement" *SA Mercantile Law Journal* 7 1995

Electronic Communications Act 2000, ISBN 0 10 540700 3

Faber D. "Electronic Bills of Lading" *LMCLQ* Part 2 1996

Faber, Diana "Electronic Bills of Lading" *Lloyds Maritime and Commercial Law Quarterly*, May 1996 at 232-244

Faber, Diana *The Use of EDI in International Trade: Implications for Traders, Banks, Carriers and Insurers*, Paper delivered at 10th BILETA Conference on Electronic Communications, Glasgow 1995

Farlam & Hathaway. *Contract* 3rd Ed. Juta & Co Ltd 1994

Fischer, S. F. (2001) 'Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation', *Boston University Journal of Science and Technology Law*, Vol. 7, pp. 229-238.

Flood Michael. Legal and business aspects of technology strategic alliances in the international environment: International Journal of Law and Information Technology, Vol.7 No.2 Oxford University Press 1999

Forsyth, C.F. *Private International Law* 2nd Ed. Juta (Cape Town) 1990

Fox William 'The International Chamber of Commerce GUID EC Principals Private Sector Rules for Digital Signatures' *International Lawyer* (35) 2001:71

Freibrun, Eric S, *Electronic Data Interchange and the Law* 1993

Furche, Andreas. - Computer money: a systematic overview of electronic payment systems Andre. - Heidelberg: Dpunkt, 1996

George F. Chandler. The Electronic Transmission of Bill of Lading: *Journal of Maritime Law and Commerce*, Vol.20, No.4, October, 1989

Glatt, C. (1998) 'Comparative Issues In the Formation of Electronic Contracts', *International Journal of Law and Information Technology*, Vol. 6, No. 1, pp.34-68.

Gregory D. John. UNCITRAL meeting on Electronic Signatures Ministry of the Attorney General: (Ontario) 10th OCT 2000. <http://rechten.kub.nl/simone/gregory.htm>.

Hill, R. & Walden, I. (1996) 'The Draft UNCITRAL Model Law for Electronic Commerce: Issues and Solutions', *Computer Lawyer*, Vol. 13, No. 3, pp. 18-21.

Hinge, K.C. *Electronic Data Interchange -- From Understanding to Implementation* AMA Membership Publication Division (New York) 1988

Holford, Mark *The Paper Bill of Lading Unravels with Bolero* 1996

Hugh Collins, 'Methods and Aims of Comparative Contract Law', (1991) 11 *Oxford J. Legal Stud.* 396, at 398.

Huntley John. New directions in US telecommunications regulation: the impact of the telecommunications act 1996 on local provision 310. *International Journal of Law and Information Technology*, Vol.8 No.3 Oxford University Press 2000

Jones P. "International Transport Conventions: Obstacles to the Use of EDI" *The EDI Law Review* (1) Kluwer Law International (Netherlands) 1994

Jones R and Basu S. Taxation of electronic commerce: A developing problem 35: *international review of law commerce and technology*, Vol.16 No.1 march 2002

Kate Marquess, 'Sign on the Dot-Com Line: Electronic Signature Act Facilitates Commerce over the Net', (Oct. 2000) 86 *ABA J.* 74.

Kelly, Richard Brett "The CMI Charts a Course on the Sea of Electronic Data Interchange: Rules for Electronic Bills of Lading" *Tulane Maritime Law Journal* , Spring 1992 at 349-375

Klaus W. Grewlich, *Governance in 'Cyberspace': Access and Public Interest in Global Communications* (Boston: Kluwer Law International, 1999), at 117.

Kohl Uta. Legal reasoning and legal change in the age of the internet-why the ground rules are still valid 123: *International Journal of Law and Information Technology*, Vol.7 No.2 Oxford University Press 1999

Kozolchyk B. *Journal of Maritime Law and Commerce* Vol 23 No. 2 1992

Kozolchyk, Boris "Evolution of the Ocean Bill of Lading from a Banking Law Perspective" *Journal of Maritime Law and Commerce* 23 1992 at 161-245

Laryea Emmanuel. Payment for paperless trade: are there viable alternatives to the documentary credit?: Law and policy in international business, Vol.33 No.1 ,2001

Lillian Edwards and Charlotte Waelde, eds., *Law and the Internet: A Framework for Electronic Commerce* (Portland, Ore.: Hart Publishing, 2000), at 19-20.

Livermore & Euarjai "Electronic Bills of Lading: A progress report" *Journal of Maritime Law and Commerce* Vol. 28 No. 1 1997

Livermore, John and Euarjai, Krailerk "Electronic Bills Of Lading, A Progress Report" *Journal of Maritime Law and Commerce* 1997 **28** at 55-59

Lloyd, Ian J. Information Technology Law .3rd ed.,2000, Butterworth's London ,P.571-591

London Parking Appeals Services (1998) Annual Report for 199, London: PAS

Lord. Templeman & Professor, Bell Cedric D .EVIDENCE,1997,Old Bailey Press.P,78-98

Macdonald RA (1999) Global law, local practices or local law, global practices, paper presented to the Canadian council of administrative courts and tribunals, Vancouver

Mazzotta, F. G. (2001) 'A Guide to E-Commerce: Some Legal Issues Posed by E-Commerce for American Businesses Engaged in Domestic and International Transactions', *Suffolk Transnational Law Review*, Vol. 24, pp. 249-277.

Mitchell, A. Bills of Lading Chapman & Hall 1982

Moens MF, Logghe Maarten Dumorties Jos. Legislative Databases: Current problems and possible solutions1: International Journal of Law and Information Technology, Vol.10 No.1 Oxford University Press 2002

Myburgh, Paul "Bits, Bytes and Bills of Lading: EDI and New Zealand Maritime Law", *New Zealand Law Journal*, September 1993 at 324-330

Nicholls, P. (26/03/1998) 'Price Waterhouse Predicts Explosive E-Commerce Growth', [www.internetnews.com/ec-news/article/0,,4_26681,00.html], accessed: 17/03/2002.

Nicoll C. *Journal of Business Law* 1995

- Nimmer, R. T. (1996) 'Electronic Contracts: Part I', *Computers and Law*, Vol. 7, No. 1, pp. 36-42.
- Nimmer, R. T. (1996) 'Electronic Contracts: Part II', *Computers and Law*, Vol. 7, No. 2, pp. 37-40.
- Nimmer, R. T. (1996) 'Electronic Contracts: Part III', *Computers and Law*, Vol. 7, No. 3, pp. 31-36.
- OECD (1999) 'The Economic and Social Impact of Electronic Commerce: Preliminary Findings and Research Agenda', [www1.oecd.org/subject/e_commerce/ebooks/027-054.pdf], accessed: 17/03/2002.
- Overby, B. (1999) 'Will Cyberlaw Be Uniform? An Introduction to the UNCITRAL Model Law on Electronic Commerce', *Tulane Journal of International and Comparative Law*, Vol. 7, pp. 219-235.
- Payne & Ivamy *Carriage of Goods by Sea* 13th Ed. Butterworths (London) 1989
- Pejovic, Caslav. Main Legal Issues in The Implementation of EDI to Bills of Lading: European Transport Law No.2 (1999) p.163-186.
- Phang Andrew and Seng Daniel. The Singapore electronic transactions act 1998 and the proposed article 2B of uniform commercial code 103. International Journal of Law and Information Technology, Vol.7 No.2 Oxford University Press 1999*
- Phang, A & Seng,D . The Singapore Electronic Transactions Act 1998 and The Proposed Article 2B of The Uniform Commercial Code: International Journal of law and Information Technology, vol.7 no.2 Oxford University press 1998
- Pike, Michael S. - The principles of policing. - London: Macmillan, 1985.
- Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues; UNCITRAL Working Group on Electronic Commerce, Thirty- sixth session, New York, , August 2000 A/CN.9/WG.IV/WP.86
- Potential?', *Penn State International Law Review*, Vol. 20, pp. 275-300.
- Proposal for a European Parliament and Council Directive on a common framework for electronic signatures; 1998 – COM (98) 297 COM/98/0297;
- Proposal for a European Parliament and Council Directive on a common framework for electronic signatures; 1998 – in the release of Working Document No 3, 25 January 1999; text established by the secretariat of the European Council after the meeting of the working group on 21. January 1999.
http://europa.eu.int/comm/internal_market/en/media/sign
- Ramberg, C. H. (2001) 'The Ecommerce Directive and Formation of Contract in a Comparative Perspective', *European Law Review*, Vol. 26, No. 5, pp. 429-450.

Reed, C. (2001) 'Legally Binding Electronic Documents: Digital Signatures and Authentication', *International Lawyer*, Vol. 35, pp. 89-106.

Reed, Christopher 'Legally Binding Electronic Contracts Digital Signatures and Authentication' *International Lawyer* (35) 2001:89

Remotti, Luca; Legal and Regulatory Issues for the European Trusted Services Infrastructure.(1997)
<http://www.cordis.lu/infosec/src/stud2fr.htm>.

RETURN TO "[ELECTRONIC DOCUMENT INTERCHANGE](#)" HOME PAGE

Richard Hill and Ian Walden, *The Draft UNCITRAL Model Law for Electronic Commerce: issues and solutions*.

Richard Horning, 'Symposium Presentation: Legal Recognition of Digital Signatures - A Global Status Report', (2000) 22:2 *Hastings Comm. & Ent. L.J.* 191, at 199 regarding the German system.

Ritter J.B. & Gliniecki J.Y. "International Electronic Commerce and Administrative Law: The need for harmonized national reforms" *Harvard Journal of Law & Technology* (6) 1994

Ritter J.B. *Northwestern Journal of International Law and Business* 1992

Rosendorff B and Milner H. The optimal design of international trade institutions: Uncertainty and escape: *International Organization*, Vol.55 No.4 2001

Rudolph B. Schlesinger *et al.*, eds., *Comparative Law: Cases - Text - Materials*, 6th ed. (New York: Foundation Press, 1998), at p. 21.

Savage,N and Walden,I . The legal problems of paperless transactions: *The Journal of Business Law* 102-112 (1989).Stevens & Sons LTD

Schmitthoff's. Export Trade the Law and Practice of International Trade 10th Ed: Sweet & Maxwell London (2000)

Scrutton on Charterparties 19th Ed. Sweet & Maxwell (London) 1984

Sjef van Erp, 'The Formation of Contracts', in: A.S. Hartkamp *et al.*, eds., *Towards a European Civil Code* (Boston: Martinus Nijhoff Publishers, 1994), at 118.

Smedinghoff, Thomas J. (Editor); Online Law, The SPA's Legal Guide to Doing Business on the Internet; Addison-Wesley Developer Press; Reading Massachusetts 1996

Stallings. William. Security on the Data Highways: Prentice Hall 1995 Stallings 1995

The EDI Law Review (3) 1996

The United States report A Framework for Global E-Commerce: *USIA Electronic Journal*, Vol. 2, No. 4, October 1997

Time magazine September (1) 1997

Tulane Law Review Vol 57 December 1982

Uimonen, T. (13/09/1999) 'Europe to See Surge in E-Commerce', [www.e-commerceworld.com/idgns/1999/09/13/IDCFORUMEuropeToSeeSurge.shtml], accessed: 17/03/2002.

UNCITRAL (1999) 'Electronic Commerce Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce', *Tulane Journal of International and Comparative Law*, Vol. 7, pp. 251-310.

UNCITRAL (1999) 'UNCITRAL Model Law on Electronic Commerce', *Tulane Journal of International and Comparative Law*, Vol. 7, pp. 237-250.

UNCITRAL. Draft Uniform Rules on Electronic Signatures.A/CN.9/WG.IV/WP.84

United Nations Commission on International Trade Law, Working Group on Electronic Commerce; Draft Uniform Rules on Electronic Signatures; UNCITRAL 1998 A/CN.9/WG.IV/WP.73 \ working group on 21.

URL: www.bergen.com/editorials/net20000119.htm

URL: www.cooperdunham.com/the_firm.htm

URL: www.faiife.dk/papers/sturges/sturge_e.htm

URL: www.iup.edu/~xnsg/proffessional.html

URL: www.pcworld.com/pcwtoday/article/0,1510,10411,00.html (fraud)

URL: www.sdnf.undp.org/lstarch/mgrs/msg01539.html

URL: www.uea.ac.uk/cpc/conferences/ucisa-tlig/d_police.html

Van Boom W.H. "Certain Legal Aspects of Electronic Bills of Lading" *European Transport Law* 1997

Van Esch R. "Interchange Agreements" *The EDI Law Review* (1)

Walden, *EDI and the Law* Blenheim Online Publishing (London) 1989

Wall, David. Catching Cyber criminals: Policing the Internet: *International review of law computers & technology*, volume 12, number 2, pages 201-218, 1998

Wall, David. Crime and The Internet: (2001) Routledge. London

Weitzenboeck, Emily. Electronic Agents and the Formation of Contracts: *International Journal of Law and Information Technology*, Vol.9 No.3 Oxford University Press 2001

Wheble, B *The EDI Handbook* Blenheim Online Publishing (London) 1988

WIPO (1999) 'Primer on Electronic Commerce and Intellectual Property Issues: Three Legal Issues of Broad Application Posed by Electronic Commerce', [<http://ecommerce.wipo.int/primer/section2.html>], accessed: 17/03/2002.

WIPO (1999) 'Primer on Electronic Commerce and Intellectual Property Issues: Global Electronic Commerce: Its Emergence and Growth', [<http://ecommerce.wipo.int/primer/section1.html>], accessed: 17/03/2002.

Wolk Stuart and Luddy William, "Legal Aspects of Computer Use": Prentice Hall, 1986, pg. 129.

Working Group on Electronic Commerce 34th sess., Vienna, 25 June - 13 July, 2001, online at <http://www.uncitral.org/en-index.htm> (adopted text link).

Yiannopoulos, A.N. *Ocean Bills of Lading: Traditional Forms, Substitutes, and EDI Systems* Kluwer Law International 1995

Zainol Z. *Electronic data interchange (EDI) and formation of contract: Malaysian perspective 256: International Journal of Law and Information Technology, Vol.7 No.3 Oxford University Press 1999*

Zekos, G. (1998) "The Use of Electronic Technology in Maritime Transport: the Economic Necessity and the Legal Framework in European Union Law" *Web Journal CLI*

Table of Abbreviations

B2B Business to Business

B2C Business to Consumer

CA Certification Authority

CCC Contract Coordination Center

CCCC Chief Contract Coordination Center

EDI Electronic Data Interchange

EDIFACT Electronic Data Interchange for Administration, Commerce and Transport

EM-RM Electronic Markets Reference Model

EPC Electronic Product Catalog

SEMPER Secure Electronic MarketPlace for EuRope

UOID Unified Object IDentity

XML Extended Markup Language

TTP Trusted Third Party

SME Small and Medium sized Enterprises

RM EM Reference Model for Electronic Markets

OTP Open Trade Protocol

WWW World Wide Web

UNCITRAL United Nations Commission on International Trade Law

OR Obligationenrecht