

European and U.S. Perspectives on Electronic Documents and Electronic Signatures

Christina Hultmark*

I.	INTRODUCTION	124
II.	FORM REQUIREMENTS GENERALLY	125
	<i>A. The Historical Development</i>	125
	<i>B. The Function of Form Requirements</i>	126
III.	REQUIREMENTS OF WRITING	128
	<i>A. Methods of Interpretation</i>	128
	1. The Semantic Method	128
	2. Legislative Interpretation Rules	129
	3. The Functional Equivalent Approach	130
	<i>B. Requirements of Writing in Contracts</i>	131
	1. Intention of the Parties	131
	2. Application of the Functional Equivalent Analysis	131
	a. Step One	131
	b. Step Two	132
	3. Outcome of the Functional Equivalent Analysis	133
	<i>C. Requirements of Writing in Law</i>	134
IV.	REQUIREMENT OF A SIGNATURE	136
	<i>A. General Description of the Problem</i>	136
	1. The Semantic Approach	137
	2. Legislative Interpretation Regulations	138
	<i>B. Requirements of a Signature in Contracts</i>	139
	1. The Functional Equivalent Approach	139
	a. Step One	139
	b. Step Two	140
	2. Outcome of the Two-Step Functional Equivalent Analysis	141
	<i>C. Requirement of a Signature in Law</i>	142
V.	DEALING WITH ELECTRONIC SIGNATURES AND DOCUMENTS IN PRACTICE	144
	<i>A. Users of Electronic Communication</i>	144
	1. General Remarks	144

* Professor of Commercial Law, University of Göteborg, Sweden. The author would like to acknowledge the very helpful input from John Gregory, Anna Nordén, Jan Ramberg, and Joan Remsu.

2. Particular Remarks Concerning Policies for
Communication with State Authorities 144

3. Problems Relating to a Lack of Usage 146

4. Recommendations to Users with Respect to Legal
Form Requirements..... 146

B. *Drafters of Contractual Texts* 147

C. *The Legislature*..... 147

1. Definitions of Writing and Signature 147

2. Legislation Aimed at Evidentiary Issues..... 150

D. *The Judge*..... 151

VI. CONCLUDING COMMENTS..... 152

I. INTRODUCTION

The traditional mode of communication by paper covered with letters in ink, and sent in envelopes, is now gradually being replaced by digital documents that are electronically exchanged. Legislation and contracts frequently provide that a message should be in “writing,” and sometimes that a “signature” is required; traditionally, when pen and paper were used, such provisions rarely caused any trouble. When using electronic means of communication, however, the meaning of the writing and the signature requirements is no longer self-evident.

In this Article, I will present a method of interpreting legislation and contractual texts containing writing and signature requirements, and a description of how recent legislative initiatives in the U.S. and in Europe regulate these issues. The Article also seeks to provide advice to users, drafters of contracts, judges and legislators on how best to deal with electronically produced texts and signatures.

When analyzing problems arising out of electronic commerce, it is often necessary to adopt an international perspective. It is not of much help to analyze a problem from a purely domestic point of view, since electronic communication is quite unaffected by national borders. Reflecting this, legislative processes dealing with these areas of law have indeed been of an international nature: the flow of inspiration, from discussions in international fora (such as UNCITRAL) and in other countries, to national legislations, is unusually apparent.¹ The problems analyzed in this Article are of the

1. See Amelia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform*, 72 TUL. L. REV. 1931 (1998).

same nature in every jurisdiction, and the methods of solution suggested here are largely applicable worldwide.

II. FORM REQUIREMENTS GENERALLY

A. *The Historical Development*²

Originally, the form requirements referred to oral promises exchanged by parties *inter praesentes* in a specified way (*stipulatio*). Gradually it became common to use instead documents with evidentiary functions: The written document in such a case purported to prove that an oral offer and acceptance had been exchanged between the parties *inter praesentes* in the required way.³

Later still, the requirement of orally exchanged promises (*stipulatio*) by parties *inter praesentes* was abolished, and the informal contract based on the meeting of the minds came to be accepted as the cornerstone of contractual obligations. When we think of formal transactions today, we see the form as something *accompanying* the legal act; it is usually a requirement that has been introduced by the legislator, for specific reasons, as an *additional* requirement for the validity of that act. But this represents a relatively modern legislative technique. Originally, compliance with form was what actually *gave rise to* (as opposed to being only a necessary requirement of) the existence and recognition of a legal effect.⁴

With the increase in the use of writing there was a shift from “effective form” to “protective form.”⁵ The protection sought by form requirements, however, is not that of the party relying on a signature, but instead that of the signer, from the making of a hasty decision. Modern form requirements purport to protect the true intention of the parties. The requirement of a signature provides an opportunity for the signer to carefully consider if he is willing to commit himself. This is particularly the case with the recently increasing form requirements in the area of consumer law.⁶ It is true that form requirements also establish some level of evidence as to the identity

2. See in more detail REINHARD ZIMMERMANN, *THE LAW OF OBLIGATIONS: ROMAN FOUNDATIONS OF THE CIVILIAN TRADITION* 68-95 (1996).

3. *Id.* at 79.

4. *Id.* at 82; see also JAMES GORDLEY, *THE PHILOSOPHICAL ORIGINS OF MODERN CONTRACT DOCTRINE* (1991).

5. ZIMMERMANN, *supra* note 2, at 84.

6. It has been called “la renaissance du formalisme,” KONRAD ZWIEGERT & HEIN KÖTZ, *INTRODUCTION TO COMPARATIVE LAW* (Tony Weir trans., Clarendon Press 3d ed. 1998), with reference to Ghustin. The requirements of form are generally somewhat relaxed in commercial transactions, see *id.* at 372.

of the signer, and can thereby be described as protection for a party relying on another signature. This evidentiary function, however, is not part of the underlying purpose of a signature requirement, but rather a practical advantage usually following from the use of signatures.

B. The Function of Form Requirements

In order to understand form requirements it is important to make a distinction between *formalistic* claims and *evidentiary* claims. The two are intertwined and closely connected, but still different in kind. The distinction is best understood by studying two possible lines of argument that may be put forward in the course of litigation. An argument making a claim of an *evidentiary nature* would be as follows: “I did not sign this document. The signature on the document is not mine. It is forged in order to create the false impression that I signed it, but I did not in fact sign it.” Or as follows: “The content of this document is not as it was when I sent it. It has been manipulated.” In these cases the court is faced with a problem of an evidentiary nature. The judge must evaluate the evidence in order to discover whether the signature was made by the apparent signer and whether the text has been manipulated. If the judge finds that there has been no forgery, the signer will be held liable. If the judge finds that the signature has been forged, the party who relied on the signature will have to bear the consequences of the forgery, unless it can escape them on another ground, such as, for example, that the person committing the forgery had authorization to sign, or that the apparent signer had acted negligently.

A claim of a *formalistic nature* would be as follows: “I admit that I sent this document and that my name is on it, but since it is not signed, it is not valid according to the law, and I am therefore not bound to honor the contract.” Or that: “I admit that I have sent this document, but since it is digital, the text does not constitute ‘writing’ and it should be treated as a nullity.”

Form requirements of writing and signature can be said to fulfill two main functions: to provide *evidence* of the parties involved and of the terms of the transaction, and to induce *caution* in the parties involved. The cautionary function protects a party from making a hasty decision, by giving an opportunity to think twice before the commitment; the evidentiary function protects the party relying on a commitment, by serving as a reminder to secure evidence of the commitment. Form requirements are also said to fulfill a third,

“channeling,” function.⁷ According to this view, form requirements may influence the parties’ behavior to the benefit of society as a whole. It is a good thing for society if contracts are made in writing, since this promotes predictability as to the evaluation of evidence in court proceedings and also establishes predictability for parties and lawyers outside court proceedings. Form requirements create a general incentive for parties to make their contracts in writing, and the positive benefits of having written evidence outweigh the insignificant cost and inconvenience such requirements impose on the individual parties.

Form requirements are dangerous, however, in that a minor flaw can, by making it possible to assert formalistic claims, have grave, harsh and unexpected consequences, and lead to highly unsatisfactory results. If a person admits that he made a promise, why should he not be liable to keep it, simply because a form requirement has not been met? And if the content of a text can be established, why would it not be taken into consideration simply on the ground that it does not constitute writing? This concern has been provocatively expressed by Grant Gilmore: “Unless the formalities were accomplished, there could be no contract, and, consequently, no liability. The austerity of doctrine would not be tempered for the shorn lambs who might shiver in its blast.”⁸

Whenever a transaction is held invalid due to a formal mishap, one’s sense of equity is offended. A strict and uncompromising application of the law under these circumstances is often denounced as “formalistic.” Equitable inroads have therefore from time to time been made into the domain of statutory forms.

One of the most notable instances has been the willingness of the German Federal Supreme Court to enforce contracts for the sale of land which lack the form prescribed in the German Civil Code,⁹ if the basic principle of good faith so demands: this, in the view of court, is the case if the result would otherwise be “plainly intolerable” for the party relying on the validity of the transaction.¹⁰

Another example is the Anglo-American Statute of Frauds. The aim of this statute was to prevent fraudulent plaintiffs from bringing claims on nonexistent contracts, but it gave equally unscrupulous defendants the opportunity of avoiding obligations which they had in

7. Lon Fuller, *Consideration and Form*, 41 COLUM. L. REV. 801 (1941).

8. GRANT GILMORE, *THE DEATH OF CONTRACT* 23 (Ronald K.L. Collins ed., Ohio State Press 1995).

9. § 131, Bürgerliches Gesetzbuch (BGB).

10. ZIMMERMANN, *supra* note 2, at 87.

fact assumed, though only by word of mouth. Both in England and the United States, a variety of methods have been used to make this formalistic legislation less harsh.¹¹

In my view, the *only* legitimate purpose of the form requirement of a signature is the cautionary one: to protect the signer and to give him an opportunity for careful consideration. The purpose is not to protect the party relying on the signature by establishing evidence of the identity of the signer. This is a practical matter, and not a matter of formalism, as is shown by the fact that no particular requirements as to the nature of handwritten signatures are established in law. A simple “x” is sufficient to fulfill the formal requirement. In some states an image of a signature on a fax is enough, even though it provides very little evidence of the identity of the signer. Independently of the form requirement, a party relying on a signature must determine whether it accepts the level of security provided by the signer (for instance whether it accepts an inked “x” on a piece of paper, a signature on a fax, or an e-mail signed with a digital signature). The need to secure *sufficient evidence* of the content of a document or the identity of a signer should be distinguished from the purpose of *form requirements* of writing and signature.

The “channeling function” is, in my opinion, not very persuasive. The interest of securing evidence creates incentives to use written and signed documents, which in turn promotes predictability and efficient court proceedings. These do not need to be reinforced by also having form requirements; sufficient incentives are given by the practical need to secure evidence.¹²

III. REQUIREMENTS OF WRITING

A. *Methods of Interpretation*

1. The Semantic Method

An interpreter of legal texts (whether private texts or legislation) usually looks first at the words as such. Usually this is not very problematic: if the legal text says that something should be written “on paper” and it is in fact written in sand, the requirement in the legal text has obviously not been met.

11. ZWEIGERT & KÖTZ, *supra* note 6, at 373-74. In the United States, form requirements related to the Statue of Frauds and to the doctrine of consideration have caused an intensive debate, which I will not refer to in detail here.

12. Fuller, *supra* note 7, at 803.

If the provision does not specify the medium to be used for a message “in writing,” such a semantic method is not sufficient. We do know that “writing” includes a text written with a pen on a piece of paper; but could it include anything else? Is it text carved into wood with a knife? Is it text written with a piece of coal on a stone wall? Is it text made with chalk on a blackboard? Is it letters written in wet sand? Is it text produced by digital impulses appearing on a computer screen as syllables, capable of being read on the screen and printed on paper?¹³

2. Legislative Interpretation Rules

Some jurisdictions have adopted definitional rules. The English Interpretation Act 1978 defines writing as “typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form.” A similar definition is found in the U.S. Uniform Commercial Code section 1-210(46): “printing, typewriting, or any other intentional reduction to tangible form.” These definitions are not much more help than the dictionary definition when it comes to determining the legal status of electronic documents; clearly, however, they do not exclude electronic documents.¹⁴

Some countries have, in recent legislation, explicitly defined the word “writing” in the electronic context. An example is the U.S. Uniform Electronic Transaction Act (UETA) Section 2(7) where an

13. In Webster’s dictionary, “write/written/writing” is defined as:

l a (1): to draw or form by or as if by scoring or incising a surface (2): to trace (a symbol or combination of symbols) by carving or scoring: INSCRIBE *b* (1): to form or trace (a character or series of characters) on paper or other suitable material (-7 instead of 9) (2): to form or record (a meaningful sign) by a series of written characters (- the word *dog*) (3): to spell in writing *c*: to write characters upon (-a check) 2 *a*: to set down in writing *b*: to draw up: DRAFT *c* (1): to be the author of COMPOSE (2): to compose in musical form (-a string quartet) *d*: to express by means of words *e*: To communicate by letter (s that he is coming) *f*: to use or exhibit (a specific script, language, or literary form or style) in writing (-Braille) (-s French with ease) *g*: to write contracts or orders for; esp: UNDERWRITE 3: to make a permanent impression of 4: to communicate with in writing 5: ORDAIN, FATE (so be it, it is in *written*—D.C. Peattie) 6: to make evident or obvious (guilt *written* on his face) 7: to force, effect, introduce, or remove by writing 8: to take part in or bring about (something worth recording)—*vi l a*: to make significant characters or inscriptions; also: to permit or be adapted to writing *b*: to form or produce written letters, words, or sentences 2: to compose, communicate by, or send a letter 3:*a* to produce a written work *b*: to compose music.

WEBSTER’S SEVENTH NEW COLLEGIATE DICTIONARY 1032 (1967). This is a very broad definition which provides a rather obscure impression of the word “writing.”

14. See MICHAEL CHISSICK & ALISTAIR KELMAN, ELECTRONIC COMMERCE—LAW AND PRACTICE 81 (1999) (expressing doubts as to the interpretation).

electronic record is defined as a “record created, generated, sent, communicated, received or stored by electronic means.” Section 7(c) of this Act stipulates: “If a law requires a record to be in writing, an electronic record satisfies the law.” The Canadian Uniform Electronic Commerce Act (UECA) similarly stipulates in its Section 7: “A requirement under (enacting jurisdiction) law that information be in writing is satisfied by information in electronic form if the information is accessible so as to be usable for subsequent reference.”¹⁵ The European Union (EU) Directive on Electronic Signatures does not cover the requirement of writing.¹⁶

3. The Functional Equivalent Approach

The UNCITRAL Model Law on Electronic Commerce prescribes a useful method of dealing with the problem of interpreting the term “writing” when it is not specifically defined in legislation. It is called the functional equivalent (or equivalence) approach.¹⁷ According to this method, the interpreter must take two steps; first, analyze the purposes of the provision; and second, determine the extent to which these purposes can be satisfied by using electronic means of communication as compared to old-fashioned paper communication. This method can be used to interpret many terms

15. A different approach is taken in the Portuguese Decreto-Lei n. 290-D/99 art. 2(a) and 3(1): “Documento electrónico: documento elaborado mediante processamento electrónico de dados,” “O documento electrónico satisfaz o requisito legal de forma escrita quando o seu conteúdo seja susceptível de representação escrita.”

16. Directive of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L, 19 January 2000, at 0012-0020.

17. In the UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 20 (1996) [hereinafter UNCITRAL Guide], it is explained:

The Model Law thus relies on a new approach, sometimes referred to as the “functional equivalent approach,” which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic commerce techniques. For example, among the functions served by paper document are the following: 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. It should be noted that in respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper, and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met. However, the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment.

other than the ones being discussed here—writing and signature—such as “place,” “original,” “record,” “presence,” or “document.”¹⁸ The functional equivalence approach formulated in the UNCITRAL Model Law has inspired much recent legislation, such as the UETA, the UECA and the EU Directive on Electronic Signatures.

B. Requirements of Writing in Contracts

Stipulations that messages should be in writing are frequent in contractual texts. Contracts commonly provide, for example, that the parties shall give notice in writing of any breach of contract to the party in breach. Has the requirement of writing been met if the notice is given via e-mail? Has proper notice been given? In other words, does the term “writing” encompass e-mail?

1. Intention of the Parties

A common method of interpreting a writing requirement laid down in a contractual text commences by trying to establish the common intention of the parties at the time the contract was concluded. This method is difficult to use in practice, since upon the occurrence of a dispute, the parties often disagree as to this common intention. Furthermore, at the time of the conclusion of the contract, the parties normally would not have had *any* actual thought as to how the word “writing” should be interpreted. It makes no sense, in such cases, to try to establish the common intention of the parties, since the method is hypothetical and its result invariably fictitious.

2. Application of the Functional Equivalent Analysis

a. Step One

What functions are served by stipulating that a notice should be given in writing?

1. To create certainty about the *time* at which notice has been given.
2. To create certainty about the *kind of breach* alleged.
3. To create certainty as to the *remedies* being claimed.

18. The method is well known in most jurisdictions and elaborated under different headings in legal theory. It can be generally applied in most areas of law (with some restrictions in criminal law and tax law due to the principle of legality, *nulla poena (tributum) sine lege*). The functional equivalence method is particularly relevant to electronic communication since it is most useful when interpreting old rules in new environments.

4. To establish *evidence* that notice has been given at a certain *time*.
5. To establish *evidence* of the *content* of the notice.

b. Step Two

Does an e-mail satisfy the purposes of the writing requirement, as indicated above?

1. When sending e-mails, logs are produced at the locations of both the sender and the receiver, which provide certainty as to the time of notice.
2. Certainty as to the kind of breach alleged depends upon what is actually said in the letter or e-mail. In this respect, it makes no difference whether the notice was given in an e-mail or on a piece of paper.
3. Certainty as to the claimed remedies also depends upon the words used in the notice, making it irrelevant whether it was given on paper or in an e-mail.
4. With respect to evidence of the time of notice, the contractual writing requirement can be seen as a reminder to the parties that if the required form is not used, it may be difficult to prove in court that notice was given in due time. A judge will often interpret an agreed form requirement as a rule of presumption: if the form is not adhered to, the starting point for the evaluation of proof will be that no notice has been given. As argued above,¹⁹ form requirements should be kept distinct from evidentiary issues. The time-logs of e-mails can be forged. This is also true for time-stamps on letters sent by traditional means. Since the system normally provides time-logs at both ends, the undetectable forgery of time-logs is not an easy matter. One should also bear in mind that for an expert, it is not a very complicated matter to forge time-stamps on envelopes. Thus, the fact that the “time-stamp” of an e-mail can be forged does not preclude it from being in conformity with an agreed requirement of writing. Time-stamps on envelopes can be forged, but a letter still satisfies an agreed requirement of writing. There is no reason why electronic messages should be treated any differently.
5. Does an e-mail produce evidence of the content of the notice? If a handwritten message is forged, it usually shows

19. See *supra* pp. 126-128.

that the text has been manipulated, since handwriting is very individual. If the text is produced on a typewriter, a forgery can be detected by letters being scraped and replaced. However, manipulation may be more difficult to detect when one page has been totally replaced. We can conclude, therefore, that text on paper can be manipulated and that such manipulations can be difficult to detect. Digital text can also be forged. It is an easy matter to change a letter or a word in an electronic document without it being apparent to the reader that the document has been changed. Normally, however, the computer will produce information indicating when the document was last changed. Furthermore, the e-mail-log saves the e-mail and the attachments of incoming e-mails. There are encryption techniques available which make it very difficult to forge digital documents.²⁰ When not using such techniques, it is possible and sometimes quite easy to forge digital documents. But the fact that a document can be forged (whether it is a paper document or an electronic one) does not prevent it fulfilling an agreed requirement of writing. The function of creating evidence should be kept distinct from form requirements.²¹

3. Outcome of the Functional Equivalent Analysis

A contractual stipulation that a message must be in writing is rarely essential to the contract's purposes, when the contract is viewed as a whole; rather, its purpose is to create an incentive to provide messages that in clear words communicate the sender's errand. Such messages can be communicated digitally as well as on paper. Reflecting this, the UNCITRAL Model Law on Electronic Commerce, Art. 6(1), contains the following provision: "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 suitable for subsequent reference."²²

20. W. FORD & M. BAUM, *SECURE ELECTRONIC COMMERCE* (1997).

21. *See supra* note 19.

22. In the Guide to Enactment, the following comment accompanies the article:

The use of the word "accessible" is meant to imply that information in the electronic message should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained. The word "usable" is not intended to cover only human use but also computer processing. As to the notion of "subsequent reference," it was preferred to such notions as "durability" or "non-

Art. 6 refers only to cases where the requirement is laid down in law, but it also provides a useful tool for the analysis of a requirement stipulated in a contractual agreement. According to the functional equivalent analysis, an electronic message would in most cases constitute writing, as long as it is received by the receiver as a readable file.

It is not necessary to apply the functional equivalence method where the UETA is applicable, because Section 7(b) itself stipulates, in harmony with the functional equivalent approach, that a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation. Section 5(b) provides that, for UETA to be applicable, the parties must have agreed to conduct their transaction by electronic means. Since, in the present example, there was no explicit agreement in this respect, it must be determined whether an implicit agreement can be inferred “from the context and surrounding circumstances, including the parties’ conduct.” The fact that both parties were available at e-mail addresses may be enough to establish an implied agreement to provide notices by electronic means. If this is not considered sufficient, the UETA is not applicable and the general functional equivalence method must be used. The end result will probably be the same: the e-mail constitutes writing.

As mentioned above, the EU Directive on Electronic Signatures does not address the problems related to requirements of writing. In European jurisdictions one must either resort to specific national legislation or case law on writing or, in the absence of such law, to the functional equivalence method.

C. *Requirements of Writing in Law*

The example discussed above, of a notice in writing, deals with a form requirement that is contractually agreed. If the requirement is instead laid down by law (by legislation or in case law), the same kind of functional equivalent analysis can be made. In some jurisdictions, great importance is attached to the intention of the legislature, which is sometimes expressed in preparatory works. However, since most of the legislative provisions containing a requirement of writing were enacted long before the digital age, this method rarely provides a

alterability” which would have established too harsh standards, and to such notions as “readability” or “intelligibility,” which might constitute too subjective criteria.

UNCITRAL Guide, *supra* note 17, at 34.

solution. In such cases it is preferable to use a more objective method and to look at the functionality of the provision.

When Art. 6 of the UNCITRAL Model Law was drafted, there was discussion of the functions performed by a statutory requirement of writing. This resulted in an extensive list of different functions.²³ This list is not exhaustive and not every form requirement is meant to perform all the different functions contained in the list. Generally speaking, my view is that a form requirement of writing must be approached in a minimalist way (because of the potential for excessive form requirements to give rise to unjustifiably harsh effects).²⁴ Since electronic messages can usually be read and reproduced, it would be proper to conclude that most electronic means of communication satisfy a legislative requirement of writing. Such a conclusion is in harmony with Art. 6 of the Model Law. If the legislature wishes to achieve more than readability and reproducibility, explicit exemptions must be made in the legislation.²⁵

The UETA stipulates that an electronic record fulfils a requirement of writing in law, Sec. 7(c). An electronic record is broadly defined as “a record created, generated, sent, communicated, received, or stored by electronic means,” Sec. 2(7). A record is defined as “information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.” Thereby, the UETA, like the UNCITRAL Model Law, reduces the relevant issues to readability (perceivable) and capability of being reproduced (retrievable).

Since the EU Directive on Electronic Signatures does not deal with “writing,” one must resort to national law. In the absence of

23. The nonexhaustive list is available in the UNCITRAL Guide, *supra* note 17, at 32: (1) to ensure that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves; (2) to help the parties be aware of the consequences if they are entering into a contract; (3) to provide that a document would remain unaltered over time and provide a permanent record of a transaction; (4) to allow for the reproduction of a document so that each party would hold a copy of the same data; (5) to allow for the authentication of data by means of a signature; (6) to provide that a document would be in a form acceptable to public authorities and courts; (7) to finalize the intent of the author of the “writing” and provide a record of that intent; (8) to allow for the easy storage of data in a tangible form; (9) to facilitate control and subsequent audit for accounting, tax or regulatory purposes; and (10) to bring legal rights and obligations into existence in those cases where a “writing” was required for validity purposes.

24. See *supra* note 19.

25. See for instance the proposed Irish legislation stipulating in section 8.5 that wills, trusts, and powers of attorney are outside the scope of the Act. It is, however, uncertain whether this should be interpreted *e contrario* (that is to say, that the excluded transactions can not be made electronically) or if these transactions may be made electronically but that this follows from general law and not from the particular Act in question. See <www.ecommercegov.ie/s8.html> (last visited July 24, 1999).

specific law on electronic documents, the UNCITRAL Model Law may be of importance as a “soft” source of law.

IV. REQUIREMENT OF A SIGNATURE

A. General Description of the Problem

As demonstrated above, the requirement of writing is normally not a problem in relation to electronic communication. The requirement of a signature, however, is a more complicated matter, since a signature fulfils more intricate purposes than a simple requirement of writing. The requirement of a signature is found in contracts as well as in legislation: in contracts, for example, when negotiating parties decide that they are not bound by their offers and acceptances until they have signed a contract; and in legislation, as is the case in many countries, when the law requires that the sale of real estate must be signed. High-value transactions or transactions establishing a security are other examples where a signature is often required by law. The legal requirement of a signature is also frequent in cases where citizens communicate with state authorities (with respect to, for example, tax returns, procurement and appeals in courts).

The question under consideration here is whether an electronic signature fulfils such agreed or legislative requirements of a signature. In the normal situation, a name written with a pen on a piece of paper is perceived as a signature. But is an “x” drawn with a pen on a piece of paper a signature? Is a thumbprint made with ink a signature? Is another person’s name written by me in fact my signature? Is my name written with chalk on a blackboard a signature? Is my name typed on paper with the keyboard of a typewriter a signature? Is the image of my signature on a fax a signature? Is my name typed at the bottom of an e-mail with a computer keyboard a signature (in combination with the e-mail sender’s e-mail address at the top of the e-mail)? Is a computerized signature made with a “pen” on a pad producing a digital record of my handwritten name a signature?²⁶ Is my thumbprint on a computerized pad a signature? Is a digital photo of my iris a signature? Is my digitally recorded voice saying “I hereby sign” or “I hereby approve” a signature?

26. See <www.penop.com/penop/penop.nsf/htmlmedia/how_penop_works.html> (last visited June 30, 1998).

1. The Semantic Approach

The word “signature” does not in itself specify which tools must be used in order to produce a signature. Dictionaries are of as little help here as in the case of writings. In Webster’s, a signature is defined as “the name of a person written with his own hand.” Under this definition one must first establish what constitutes the “name of a person.” For example, if I usually choose to write not my name, Christina, but instead Christine, would this be a signature? Or if I write “x” as a symbol for myself, would that be a signature? Neither would amount to a signature under this dictionary definition, since neither “Christine” nor “x” is my name. But typing “Christina” on the keyboard of my computer would, since it would be in accordance with this part of the definition of a signature.

Secondly, it must be determined what “written” means, and as the discussion above demonstrates,²⁷ if composing music is “writing” under the dictionary definition, then creating digital records with a computer keyboard is also writing.

Finally, the meaning of “with his own hand” in the definition of a “signature” must be determined. Using my thumb to make a thumbprint would probably fall within this part of the definition (since the thumb is part of my hand), but a thumbprint is not a “name of a person.” If I wrote my name with the pen in my mouth, it would not be written “with [my] own hand,” which would also be the case if a person born without arms used her feet to write, since according to the dictionary definition, she would not have produced a signature “with [her] own hand.” On the other hand, if I wrote my name by pressing the keys on the keyboard (with the fingers of my hands) and produced the letters that form the name “Christina,” it would, according to the dictionary’s definition, be a signature written “with [my] own hand.”

These examples show that using the semantic method does not produce satisfactory answers. Some of the conclusions above—for instance that a handless person cannot create a signature—are obviously wrong. Once it is initially established that a word is difficult to interpret in relation to electronic means of communication, it is better to abandon semantics and instead undertake a functional equivalent analysis.

The problems related to the English meaning of a “signature” appear in most other languages. In Dutch we have the same problem interpreting “handtekening,” and in German and Swedish, the

27. See *supra* note 19.

corresponding words “Unterschrift” and “namnteckning.” In most Roman languages, too, words for “signature” (such as “sottoscrittura” in Italian) give rise to the same problems as described above in relation to the English term.

2. Legislative Interpretation Regulations

Some jurisdictions have legal definitions of a “signature,” which are often somewhat more informative than the dictionary definitions. For instance, the Civil Code of Quebec Art. 2827 stipulates: “La signature consiste dans l’apposition qu’une personne fait sur un acte de son nom ou d’une marque qui lui est personnelle et qu’elle utilise de façon courante, pour manifester son consentement.” Since there is a requirement that the signature be “personal,” and be made in the way in which “it is normally made,” this definition could be said to prescribe a certain level of evidentiary value. However, the meaning of “personnelle” is highly uncertain (for example is the use of a password personal?) and the requirement of “de façon courante” does not exclude electronic signatures if the signing person frequently signs documents electronically. Furthermore, it should be observed that the definition is placed in a section of the Code dealing with evidentiary matters.

In recent times some countries have introduced special legislative interpretation rules referring to electronic signatures. Singapore has introduced three definitions; one for an electronic signature, another for a secure electronic signature, and a third for a secure digital signature.²⁸ The same distinction between signature techniques providing high and low evidentiary value can be found in the EU Directive on Electronic Signatures.²⁹ In the United States, the UETA does *not* make such a distinction, but treats all kinds of electronic signatures equally.³⁰ In the UETA Sec. 2(8), an electronic signature is broadly defined as “an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with intent to sign the record.”³¹

28. SINGAPORE ELECTRONIC TRANSACTION ACT arts. 8, 17, 20 (1998).

29. See definitions of “electronic signature” and “advanced electronic signature,” EU Directive, *supra* note 16, art 2. The Portuguese regulation also distinguishes between “assinatura electrónica” and “assinatura digital” (Decreto-Lei n. 290-D/99).

30. A similar regulation can be found in the Canadian Electronic Commerce Act section 1: “In this Act . . . ‘electronic signature’ means information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with the document.”

31. In the ongoing work of the UNCITRAL Working Group on Electronic Commerce it has been vividly discussed whether or not to create special rules for electronic signatures with

B. Requirements of a Signature in Contracts

A common contractual situation arises when negotiating parties stipulate in a Letter of Intent that they shall not be bound until they have signed a written contract. The question is whether this contractual requirement of a signature can be satisfied by electronic means of communication, such as an e-mail with the name of the party typed at the bottom. As indicated above, the dictionary is not an appropriate tool for solving this kind of problem, and an analysis of the subjective common intention of the parties also fails to provide a solution.³²

1. The Functional Equivalent Approach

Can ordinary e-mails fulfill an agreed requirement of a signed written contract? Let us consider a case in which both negotiating parties have sent an e-mail to the other with the contractual text and have written: "This is the final version of our contract to which I agree." Their names are typed at the bottom of the e-mails.

a. Step One

Why is it frequently stated in Letters of Intent that the parties are not bound until they have signed a written contract?³³

1. Since many contracts come into being through the exchange of oral offers and acceptances, it is important for the parties to avoid being bound unintentionally while still negotiating. They can feel free to express different suggestions when they know that they are not finally bound until there is a signed written contract.
2. A written contract provides certainty and evidence as to the detailed obligations of the parties.
3. A signature provides certainty and evidence as to the identity of the other party.

high evidentiary value of the signer's identity. For the reports of the working sessions, see <www.uncitral.org/en-index-htm>.

32. See *supra* note 19.

33. In the UNCITRAL Guide, *supra* note 17, at 35, the following list of functions of a signature is given:

to identify a person, to produce certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document. Furthermore, a signature might attest to the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text; the intent of a person to associate itself with the content of a document written by someone else; the fact that, and the time when, a person had been at a given place.

b. Step Two

Now that the purposes underlying the provision in the Letter of Intent have been analyzed, it should be considered how far the exchange of ordinary e-mails corresponds to these purposes.

1. Is there a risk that the e-mails may render the parties unintentionally bound during negotiations? In the realm of pen and paper contracts, most people presume that parties signing a document intend it to be the final expression of their agreement. Such a silent presumption cannot be transferred into the electronic environment. The “magic” of signing the contract is not present in the electronic world, but must be transferred there. Or to put it in other words: It is necessary to create a procedure which puts it beyond doubt whether the text contained in the exchanged e-mails is a final document. Such a procedure can be established in the electronic environment, but it requires a larger amount of explicit wording than in the traditional paper and pen world. It is also necessary that the procedure by which the intent to be bound is given have a security function, in order to ensure that the electronic message is not mistakenly sent (as may happen, for example, when a sender’s hand “slips,” sending the e-mail unintentionally).
2. Do e-mails provide certainty as to the content of the parties’ obligations? Every contract, whether oral, written on paper or consisting of a digital document, may be uncertain as to the obligations of the parties. It does not matter much which medium is being used, since the problem is that parties often fail to express themselves clearly, or fail to cover every potential question in their express agreement. The text in the digital document is the equivalent of that of a paper document in this respect. Do e-mails produce good evidence of the content of the contract? This concern is not related to the signature but to the text in the document. This problem has been examined above,³⁴ and the conclusion reached that the fact that the text in a document (whether paper or electronic) can be manipulated does not prevent it fulfilling the contracted requirement of a “signed written document.”

34. See *supra* note 19.

3. Do e-mails produce certainty and evidence of the identity of the other party?³⁵ When an apparent signer of a document repudiates and claims that the signature was forged by someone else, it must be established whether the apparent signer did sign the document. A traditional handwritten signature produces evidence of the identity of the signer. It can be established with some certainty whether a signature was produced by the apparent signer or someone else. However, that certainty depends on many factors. If the signature only consists of an “x” it is more difficult to establish this certainty than in a case where a long sequence of syllables has been used. Normally, an expert on graphology provides, on a scale of certainty from 0-5, the probability that the apparent signer signed the document. Only rarely is it wholly clear whether the handwritten signature was forged or not. E-mails, too, can be manipulated so as to appear to be coming from somebody other than the true sender. The fact that a signature, whether made with pen on paper or electronically, can be manipulated or forged, does not prevent it being a signature.

2. Outcome of the Two-Step Functional Equivalent Analysis

According to the foregoing analysis, the requirement in a Letter of Intent of a “signed written contract” can be satisfied by the exchange of electronic messages, but not invariably so. The outcome depends on the extent to which the parties’ intentions to be bound by the contract have become evident. By using a handwritten signature, the parties implicitly consent to be bound by the contract. When the contract is sent in electronic form, something more than the mere name at the bottom of the electronic message is needed in order to make sure that the signing party consents to be bound, such as express wording stating that it is the final version and that the signing party accepts the text. According to this line of argument, it is irrelevant how securely the technique establishes the identity of the signer. The truth of a claim by a party that he did not sign must be evaluated by examining the evidence presented by each party. A claim that the form requirement in the contract had not been met should not be

35. It is frequently disputed who the other party actually is. Is it the signer personally or the company where he is working that is bound by the contract? This problem is not solved by using handwritten signatures, nor by using e-mails. It all depends on what is said in the contract (or implied from the behavior of the parties).

accepted simply on the grounds that the electronic signature can be forged.

The UETA stipulates that electronic signatures may not be denied legal effect or enforceability solely because they are in electronic form, Sec 7(a). This is true also when the form requirement is explicitly or impliedly agreed by the parties, Section 5(b).

The EU Directive on Electronic Signatures does not cover the question in this example, since it is not applicable to questions of validity and formation of contracts, Art. 1. Consequently, national law in the different member states must be applied, and in absence of specific legislation on electronic signatures, the functional equivalence method can be used.

C. Requirement of a Signature in Law

As indicated above, the requirement of a signed document is often laid down in legislation.³⁶ Analysis of the underlying purposes of such legislative requirements often leaves the matter unclear. The UNCITRAL Model Law on Electronic Commerce, Art. 7, focuses on the two basic functions of a signature, namely, to *identify* the author of a document, and to confirm that the author has *approved* the content of that document.³⁷

The approval of content function is not performed by the signature itself; rather, the signature requirement often implicitly performs a warning function: “Think twice before you sign and before you thereby commit yourself.” This warning (or approval of content) function can easily be transferred to an electronic transaction by requiring the signing party to explicitly express its approval by clicking on a box saying (for instance): “I confirm that the information given here is correct,” or: “I hereby agree to sell this real estate according to the enclosed contractual agreement.” Such

36. Sometimes such requirements are combined with requirements of witnessed signatures or notarial authentication. The requirement of a signature can also at times be replaced by a stamp or must be combined with a stamp.

37.

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

a method is used to identify that person and to indicate that person’s approval of the information contained in the data message, and that method was 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.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

procedures may also involve digital voice messages. As said above,³⁸ a form requirement of a signature primarily serves the cautionary function of making certain that the signer thinks twice, by providing an opportunity for careful consideration. Consequently, the form requirement of a signature is satisfied by any procedure that ensures that the signing party agrees to accept the consequences to which it is committing itself. In *practice* the signature also provides evidence of the identity of the signer, but the party relying on this function of a signature must determine the level of evidence that it needs. This does not relate to the form requirement, but is purely a question of how much proof the relying party needs in case the apparent signer repudiates and claims that he has not signed the document.

The UETA focuses upon the question whether there was the intention to sign, and there is no mention of the identification function of the signature. UETA Sec. 2(8) defines an electronic signature as follows: “‘Electronic signature’ means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.” Taking the opposite stance, the EU Directive attributes no significance to the intent to sign, but only deals with the identification function. It stipulates: “‘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.”

The explanation of the different approaches in the UETA and in the EU Directive lies probably in the differences in their respective scopes of application. Since the EU Directive does not seek to harmonize national rules concerning contract law, and particularly not the formation of contracts, it would have been strange to refer to the intention to sign.³⁹ It is, however, quite unclear how this limited scope of application relates to Art. 5 regarding the legal effects of electronic signatures. Art. 5 stipulates that Member States shall ensure that advanced electronic signatures⁴⁰ satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as hand-written signatures satisfy those requirements in relation to paper-based data. It is possible that the EU Directive is

38. *See supra* note 19.

39. According to the preamble the directive is without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts. Also in article 1 is stipulated that the directive does not cover aspects related to the conclusion and validity of contracts where there are requirements as regards form in national law.

40. “Advanced” refers to signatures created in a particularly secure way when it comes to identification of the signer.

aimed only at evidentiary issues (most of Art. 5 concerns the evidentiary effects of electronic signatures); if so, its focus on the identification function is understandable.

The UETA deals with formation of contracts and commitments generally (as well as evidentiary matters), and consequently emphasizes the intention to sign function.

V. DEALING WITH ELECTRONIC SIGNATURES AND DOCUMENTS IN PRACTICE

A. *Users of Electronic Communication*

1. General Remarks

Users of electronic communication, senders as well as receivers, face the practical problem of developing a strategy as to the techniques to be used in their business transactions: they must determine what level of security is needed for their transactions. If the transactions are subject to a high risk of fraud (for instance, in the transfer of money via banks) tight security is needed to prevent the content of the message from being manipulated, and the electronic signature from being forged by unauthorized persons. If, on the other hand, the transaction is not subject to a great risk of fraud (for instance, in the selling of books at an Internet bookstore) a high level of security is not needed.

It is also vital for users to introduce procedures in connection with their use of electronic communication, whereby the signer has an opportunity to consider carefully whether he wishes to be exposed to the liability a signature might impose. Such procedures could include boxes to click on, questioning whether the signer really wants to be bound or is ready to commit himself. Such procedures are necessary in order to serve the cautionary function (or think twice function), and to establish an express communication of intent to be bound. This is particularly relevant for transactions where the other party is typically in need of careful consideration, such as in consumer transactions, or in transactions involving large-scale commitments.

2. Particular Remarks Concerning Policies for Communication with State Authorities

Many transactions involving communication between state authorities and citizens require, by law, the form of writing and signature. At the same time, such transactions are often exposed only to a minimal risk of forgery. For example, the probability of

somebody sending in a tax return in somebody else's name is very small. Another example is appeals in court proceedings, which are rarely (if ever) forged.

The state may have an interest in using the same means of communication and identification irrespective of the kind of transaction. The state thereby contributes to a standardization of electronic means of communication. Instead of placing the burden on each and every authority to determine what standard techniques it requires, a general policy can be established with respect to electronic communication with all state authorities. When such general requirements are specified, the security needs of the transaction with the highest risk of forgery and repudiation must be taken into account. Appeals in court do not need the same level of security as applications to an authority to register the ownership or pledge in a particular piece of property (in order to establish a security). The risk of forgery is much higher in the latter case. If the state wishes to use the same means of electronic communication for all transactions, the security level appropriate to the most sensitive transaction will have to be chosen (in the example, the security level appropriate to the creation of a security right in property). Such a regulation will be excessively secure for most transactions involving communication with the state (such as appeals). High security techniques are often cumbersome to use, and are normally more expensive than less secure techniques; but standardization promotes an efficient and cost effective infrastructure and thereby partly balances the negative effects of excessive security.

In Europe, standardization is considered crucial. The EU Directive on Electronic Signatures, Arts. 9 and 10 establishes an Electronic Signature Committee. This Committee is a body in charge of elaborating standards for high security electronic signatures, capable (within certain limits) of taking into account technological changes.

The UETA does not address the question whether standardization is preferable or needed. The UETA makes it possible, in Sec. 8(b), to provide for extra legislative requirements, probably so as to ensure that the electronic record is perceivable to the receiver and capable of being processed by the computer system of the receiver. This will most probably be of particular importance in communications with state authorities, and might in practice come to serve as a source of standardization.

In the Canadian Uniform Electronic Commerce Act (1999), Art. 8 and Art. 10 first stipulate that not a great deal is needed in order to satisfy the form requirement. A particular authority may, however,

impose extra regulations by deciding what kind of electronic documents are acceptable.⁴¹

3. Problems Relating to a Lack of Usage

At present there is no established usage relating to electronic communication. Parties need to make an active decision as to the level of security they need. Usages or standards will probably be established in due course, and more quickly if the pace of technological development slows. Parties will then be able to behave “normally”—i.e., they will then be able to rely passively on the efficiency of usages and common behavior of those engaged in the transaction in question. In times of great technological change it is necessary to allow some time for practices, usages and standardization to evolve. This process cannot successfully be rushed by legislation.

4. Recommendations to Users with Respect to Legal Form Requirements

A particular problem arises for users when a transaction is regulated and the law contains a form requirement of writing and/or signature. Due to the present uncertainty as to the kinds of electronic communication that conform with such form requirements, users ought to be very careful when using electronic communication in such transactions. In this Article, I have argued that electronic documents and signatures often ought to be treated as equivalent to traditional pen and paper documents and signatures as far as the satisfaction of form requirements is concerned.

In the case of jurisdictions that have not yet specifically addressed the question of form requirements in relation to electronic communication, I would hesitate to recommend full reliance on the argument of functional equivalency advocated in this Article, since a user who does so runs the risk of coming up against an excessively conservative judge in court. Consequently, for the time being my

41. An electronic signature is broadly defined as “information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with the document.” Article 10 states, “(1) A requirement under (enacting jurisdiction) law for the signature of a person is satisfied by an electronic signature. (2) For the purposes of subsection (1) the (authority responsible for the requirement) may make a regulation that, (a) the electronic signature shall be reliable for the purposes of identifying the person, in the light of all the circumstances, including any relevant agreement and the time the electronic signature was made; and (b) the association of the electronic signature with the relevant document shall be reliable for the purpose for which the electronic document was made, in the light of all the circumstances, including any relevant agreement and the time the electronic signature was made.”

advice to users is to secure transactions where a signature is required with an old-fashioned handwritten signature with ink on paper. However, if the law requires writing (but not a signature), I would venture to recommend the use of electronic documents, so long as the format used is normally readable to receivers, or if the user has implemented a procedure whereby the receiver confirms that it has received and read the document.

B. Drafters of Contractual Texts

One of the main purposes of drafting a contract is to avoid uncertainties. Ambiguous wording should therefore not be used in contractual texts. In the era of electronic communication the meaning of formerly easily interpreted words such as “writing” and “signature” becomes uncertain. In old contracts, such uncertainty ought to be dealt with by using the functional equivalent method. When drafting new contracts, certainty could be obtained by defining these words in the contract’s list of definitions, such as for instance by stipulating: “Writing includes any digital message produced in a format comprehensible to the receiver.” Another means of creating clarity is to include the relevant electronic means of communication directly in the material contractual text. For instance: “Notice shall be sent by fax or e-mail within two working days. . . .”

A disadvantage of such a provision is that the contract might then become inflexible or incapable of encompassing new technological developments and new forms of user behavior. It is advisable to avoid too much specificity in the contract as to the technological solution that is required. This is particularly important for long-term contracts and standard contracts. On the other hand, a technique-specific contractual text enables the parties to make a clear and predictable rule, appropriate to the level of security they intend to use, and specially designed for their particular needs.

At present, it is not advisable for the drafter to use the words “writing” and “signature” without clarification in the contract, since it is highly unpredictable how these terms will be interpreted by judges in courts.

C. The Legislature

1. Definitions of Writing and Signature

As long as there are no legal definitions of “writing” (stating, for instance, that in law it only means text on paper put there by means of a pen) or “signature,” there are no alternatives to using the functional

equivalent approach, since the semantic approach usually fails to produce helpful answers. This is perhaps an unfortunate conclusion, since the method does not provide a simple answer to the question. Undertaking a functional equivalent analysis is time consuming and does not provide a solution generally applicable to all situations.

On the other hand, a positive aspect of the functional equivalent method is that it shows that explicit legislation is not necessarily needed. Indeed, legislation expressly rendering electronic messages equivalent to paper messages may even turn out to be disadvantageous. One problem with such legislation is that it would often include descriptions of specific techniques, and consequently would soon become outdated by technological change. The parties and the courts would then be faced with a very delicate problem. Should the legislation be interpreted *e contrario* or *ex analogia*? Should the judge then state that since the new way of communicating electronically is not covered by express legislation, the form requirement has not been met (interpretation *e contrario*)? Or should the outcome be based on the argument that since a particular kind of electronic message is explicitly recognized by law, the new way of communication should also be valid (interpretation *ex analogia*)?

Another disadvantage of enacting a technology specific legislative rule is that it is static. As Boss has explained,⁴² technological security is not monolithic; there are many technological methods of security, with different strengths and weaknesses, and technology is in a constant stage of development. Promoting particular technologies or particular implementations would therefore be counterproductive. This approach—the technological neutrality approach—also recognizes that the law is of limited utility in encouraging certain types of behavior: people will use security procedures because it is good business, not because the law gives special legal effects to certain procedures. The marketplace, rather than the legislature, provides the solutions and support.⁴³ Despite the fact that the legislation of most states commences with the bold assertion that the new legislation is meant to enhance and facilitate electronic commerce, it has in fact frozen technological development and promoted increased bureaucracy and administration; this is the

42. Amelia H. Boss, *Searching for Security in the Law of Electronic Commerce*, 23 NOVA L. REV. 585, 611-17 (1999).

43. This approach has been taken, for instance, by Australia, see <<http://law.gov.au/ecommerce>>, Canada, see UNIFORM ELECTRONIC COMMERCE ACT, and the United States, see UNIFORM ELECTRONIC TRANSACTION ACT.

case, for example, with legislation in Utah and in Germany on digital signatures.

Technological neutrality has been very difficult to achieve in the ongoing work of UNCITRAL concerning electronic signatures.⁴⁴ If the rules are made wholly technologically neutral, they become too general and provide only limited guidance;⁴⁵ but if they are technologically too specific, their area of application becomes very narrow and the regulation may soon be outdated by new technology.⁴⁶ The EU Directive on Electronic Signatures has to some extent solved the problem of technological neutrality by creating an Electronic Signature Committee, responsible for taking account of new technology. The path chosen by the United States in the UETA is very general, but it still provides specific guidance.⁴⁷ The Act defines an electronic signature very broadly and stipulates that an electronic signature satisfies any legislative form requirement of a signature.

Due to the very narrow scope of application of the EU Directive on Electronic Signatures, there is a risk that the message its drafters tried to convey (the functional equivalency approach) will not be considered applicable outside the sphere of evidence law. This may lead to the impact of the Directive being very limited, leaving it to the member states to determine how electronic signatures and writing relate to form requirements from a validity point of view.

In contrast to the EU Directive, the UETA is very broad. It covers any kind of transaction apart from wills, codicils and testamentary trusts, Sec. 3(b)(1). However, in adopting the UETA a state may also state exemptions from the scope of its application. The UETA even provides an extensive list of suggested exemptions, in Sec. 3(2) and (3). To the extent that the UETA will be adopted by different states without limited scope of application, it will provide a solid ground for acknowledging any kind of electronic document and electronic signature as satisfying legal form requirements.

The explanation for the different approaches in the U.S. and Europe is at first sight difficult to discern. Both were facing the problem that the member states were unilaterally enacting specific legislation in relation to electronic signatures, and thus risking the creation of obstacles to trade between them. The initiative taken by

44. See <www.uncitral.org/en-index.htm>.

45. See, e.g., THE MODEL LAW ON ELECTRONIC COMMERCE art. 7 (technology neutral and also very general).

46. Examples of this are the Utah, and the German and Italian legislation on digital signatures.

47. For the legislative development in the United States, see Boss, *supra* note 1.

the EU was partly aimed at putting an end to such specific member state legislation. EU directives are negotiated with representatives of the member states and are then mandatory upon the member states. This legislative process often results in very narrowly applicable directives. The legislative process in the U.S. is quite different. There, too, there is the need to harmonize legislation in relation to electronic commerce and to create an alternative to specific state legislation. The UETA, however, has not been negotiated in a political manner and will not be imposed upon the states, but will merely serve as a recommendation. It has been possible to create an instrument of high quality ranging over a wide area, since its adoption will take place on a voluntary basis.

This is not the proper place to elaborate on, and compare, the different legislative processes in the EU and the U.S. The conclusion when comparing the effects of the EU Directive and the UETA is that the U.S. has formed a basis which will facilitate electronic communication and create predictability as to the legal effects of electronic documents and electronic signatures, whereas the limited scope of the EU Directive in effect leads to the need to use the functional equivalence method in Europe. At present legislation is different in different member states, both in the United States and the EU, which in turn may hinder interstate trade. If the UETA is widely adopted this problem may to a large extent disappear. In the EU, another directive, with a wider scope of application, is needed to harmonize law related to electronic communication, and the adoption of a directive regarding electronic commerce is underway.⁴⁸ It should be noted that the UETA addresses questions other than the legal requirements of writing and signatures, as does the proposed EU Directive on Electronic Commerce. This Article, however, is limited to form requirements.

2. Legislation Aimed at Evidentiary Issues

An important task of the legislature is to determine the extent to which electronic evidence can be admitted in court. Electronic evidence should neither be favored (by presumptions), nor be given a lower status than oral or paper means of evidence. Constant technological change makes it necessary to acknowledge that the judge, possibly with guidance from technologically expert witnesses, is the most appropriate evaluator of evidentiary issues according to

48. The proposed European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market.

the principle of free evaluation of proof. It is hardly feasible to provide legislative guidance for the judge in this respect (in the form, for instance, of presumption rules), since different transactions need different levels of security depending on the extent to which they are exposed to fraud.

Many of the EU member states have a basic principle of admitting any kind of evidence in court proceedings and providing the judge with the authority to evaluate the evidence—this is true, for instance, in the Scandinavian countries, and in Germany, Austria and the Netherlands. Other member states, such as France and the U.K., are more restrictive in admitting evidence and providing for its free evaluation. The EU Directive on Electronic Signatures, Art. 5, states that electronic evidence must not be denied legal effectiveness or admissibility as evidence in legal proceedings solely on the ground that it is in electronic form. The UETA promotes the use of electronic evidence by stipulating in Sec. 13: “In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.” It is important that these provisions clearly abolish formalistic obstacles related to electronic evidence in court proceedings. The UETA goes further than the EU Directive in that it covers both writing and signatures, whereas the EU Directive only covers signatures. It seems likely to me that EU member states implementing the directive with regards to signatures will take the opportunity also to allow electronic documents as evidence. But the procedures for the implementation of directives vary from member state to member state, and the results are difficult to predict.

D. The Judge

My own experience, in giving seminars to Swedish judges and having discussions with judges, indicates that they are often reluctant to conclude that an electronic signature fulfils the legal form requirement for a signature. This probably stems from the reluctance of judges to abandon traditional perceptions, such as that “a signature is made with ink on paper”. Judges sometimes use a “backward” approach, in that they determine whether the new electronic medium could be accepted under the law by starting with the presumption that it cannot be accepted. Instead they ought to use the approach suggested in the Model Law Art. 5: “Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.” According to Art. 5, the starting point would be that the new means of communication should be accepted if

there is not a convincing argument against it. Art. 5 indicates that the form in which certain information is presented cannot be the *only* reason why that information would be denied legal effect.⁴⁹ Good arguments frequently cannot be produced for why an electronic document or an electronic signature should be denied legal effect when they are used to satisfy legal or contracted form requirements. However, accepting the electronic document or the electronic signature as *fulfilling a form requirement* does not prevent the judge from giving it low *evidentiary* value in a case where the apparent signer repudiates the signature, or the sender claims that the document has been manipulated.⁵⁰

Future developments in case law should prove very interesting, because among other things they will permit us to compare how judges from different legal traditions approach these problems, and to what extent they are ready to apply the functional equivalent method. In the future, the possibilities open to a judge, independently to elaborate on the functional equivalent method, will probably be limited by explicit legislation regulating the extent to which electronic documents and signatures satisfy legal form requirements.

VI. CONCLUDING COMMENTS

The judicial system must encompass both traditional means of communication (paper and oral) and present electronic techniques. It must also be flexible enough to apply to techniques that are as yet unknown. A technology specific regulation is not apt to handle such a vast and changing field. Instead, it is necessary to elaborate general and open rules in which all the relevant circumstances can be taken into account.

The new means of electronic communication poses a great challenge to lawyers. It necessitates an analysis of terms that were formerly crystal clear. Hence it is essential to avoid a plain semantic

49. See also the opinion given in *Clyburn v. Allstate*, 826 F. Supp. 955 (D.S.C. 1993): "in today's 'paperless' society of computer generated information, the court is not prepared, in the absence of some legislative provisions or otherwise, to find that a computer floppy diskette would not constitute 'writing' within the meaning of (the Statute)."

50. As pointed out by M.B. Andersen, it is necessary for a lawyer analyzing aspects of contract formation by computers to have some understanding of the underlying technology and a clear understanding of the basic concepts behind private law in general and contract law in particular. He furthermore emphasizes that such dual knowledge is not always available as far as legislators and the administration are concerned, which demonstrates the need for close co-operation between academia and administrators. M.B. Andersen, *Electronic Commerce: A Challenge to Private Law?*, Centro di studi e ricerche di diritto comparato e straniero, saggi, conferenze e seminari 27-32, Roma 1998. We can also foresee an expanding need for lawyers to work in close co-operation with technical expert witnesses.

interpretation, and instead to use the functional equivalent method and to search for the underlying purpose of the provision. Such an analysis is not always quickly made, and it does not provide a single solution for every case. The functional equivalent method instead provides a flexible tool for people and businesses using electronic communication. This may disappoint formalistic lawyers who prefer a rule that is foreseeable to lawyers, but not necessarily practical for the users of the technology. However, it should be remembered that law does not exist for its own sake; it exists to facilitate societal needs. Formalism is often an obstacle to trade. It is my hope that electronic commerce will not be drowned in excessive formalism when it comes to interpreting words such as “writing” and “signature.” Recent legislation, such as the EU Directives on Electronic Commerce and Electronic Signatures and the U.S. Uniform Electronic Transaction Act, is very promising in this respect.