

3-1-2002

## Commerical Transactions by Electronic Commerce Involving the United States, Mexico and the European Union


Michael W. Gordon

J. Michael Norwood  
norwood@law.unm.edu

Roger Saldana

John Andrew Spanogle

Follow this and additional works at: <https://digitalrepository.unm.edu/usmexlj>

 Part of the [International Law Commons](#), [International Trade Law Commons](#), and the [Jurisprudence Commons](#)

### Recommended Citation

Michael W. Gordon, J. Michael Norwood, Roger Saldana & John A. Spanogle, *Commerical Transactions by Electronic Commerce Involving the United States, Mexico and the European Union*, 10 U.S.-Mex. L.J. 165 (2002).  
Available at: <https://digitalrepository.unm.edu/usmexlj/vol10/iss1/26>

This Article is brought to you for free and open access by the Law Journals at UNM Digital Repository. It has been accepted for inclusion in United States - Mexico Law Journal by an authorized editor of UNM Digital Repository. For more information, please contact [disc@unm.edu](mailto:disc@unm.edu).

# COMMERCIAL TRANSACTIONS BY ELECTRONIC COMMERCE INVOLVING THE UNITED STATES, MEXICO AND THE EUROPEAN UNION: A PANEL DISCUSSION

MODERATOR: PROF. MICHAEL W. GORDON\*

Panelists: Prof. J. Michael Norwood; Lic. Roger Saldaña;  
Prof. John Andrew Spanogle

**GORDON:** The problem that we are going to deal with is a problem that comes out of the 4th edition of the *International Business Transactions* casebook that I co-authored with Professor Spanogle.<sup>1</sup> The casebook problem involves Professor Pedro, who is Brazilian. We changed the facts to make Professor Pedro Mexican for the purposes of this panel topic.

The problem introduces Professor Pedro, who is on the faculty at the University of Guanajuato, and he is not only a soccer fan but also the coach of the soccer team in his town. He has bought a group of books over the Internet on Rhine.com, a book retailer in Germany. There is no paper contract involved. Pedro gives no identification other than his mailing address and he "borrows" his brother's credit card to pay for the purchase since he does not have a credit card of his own. Pedro's purchase has used up most of what Rhine.com has available in stock, and by automatically programmed computer, a message is sent on to some book distributors to see if there are more of those books available. Rhine.com soon issues a book order for some \$10,000 worth of books to refill its inventory to East Publishing Company, an American firm. That company is set up to receive the information automatically and has the books pulled from inventory storage, packed in a box, labeled, and sent out without any human involvement whatsoever.

Rhine.com is a German company but an American parent corporation wholly owns it. Additionally, it seems that there is a further use of the information that Pedro has given by the American company: the company compiles lists and sells these lists of information about people to whomever might want to purchase them.

This problem raises several issues. There are a series of issues related to contract formation and all of the parties involved would like to know whether they have enforceable contracts. We presumably or possibly have contracts between Pedro and Rhine.com and a separate one between Rhine.com and the East Publishing Company. Another issue is the development of legislation, and it is important so that we examine what is occurring in Mexico as well as in the United States. Finally, there is the issue of privacy, which is important in that we may have different privacy rules in Germany, the United States and Mexico.

**SPANOGLE:** The problem at hand raises probably five different sets of issues, and we probably ought to talk about each set one at a time. One set is contract formation. A second set is jurisdiction. If you are going to go to court, where do you go to court as a private individual or as a public regulator? The third set of issues deals with privacy. The fourth set of issues, which can come up, is credit card issues. The last set of issues is an overview of the problem in regard to

---

\* A summary of the background of each of the participants in this panel discussion follows on the last page.

1. See RALPH H. FOLSOM et al. *INTERNATIONAL BUSINESS TRANSACTIONS* (4th ed, West Group 1999).

legislation. When should you have legislation in this field, and if you are going to have legislation, what kind of legislation should you have?

I will begin with contract formation issues. While there are certainly more, let me raise six of the basic issues. First, is there a writing? The contract that involves the East Company is a contract involving a U.S. party and is, therefore, subject to the Statute of Frauds, which requires a signed writing. Thus, the first issue is whether there is a writing. Is there anything in recent legislation that has obviated that requirement?

Article 2 of the UCC is in the process of being redrafted. The National Conference of Commissioners on Uniform State Laws (NCCUSL) attempted to adopt a final draft in August, but were not able to agree on some provisions. So it is still a work in process. But it is important to know that the committee that was redrafting Article 2 has voted fourteen to nothing about six to ten times to drop the Statute of Frauds altogether because it is totally irrelevant in modern commerce. Then the lawyers who were representing General Electric and the Automobile Manufacturers Association demanded that the committee put back in the Statute of Frauds. Since the NCCUSL very often complies with demands from industry, they in turn demanded that the drafting committee put the Statute of Frauds provision back in, regardless of whether it makes any sense. So for now, there will continue to be a Statute of Frauds provision in UCC Article 2. There are no Statute of Frauds provisions in most civil codes, but according to one of my research assistants who is French, the French civil code has over two-hundred articles in which a written requirement is present. Therefore, it seems that there can be a writing requirement present in the civil codes, even though it is not as broad as the U.S. provision. However, this does not speak to Mexican law.

The second issue is whether there is a signature. Is there anything in these facts that shows that someone has adopted any symbol as something that authenticates an intention to be bound? If so, how does one prove it? This issue will interrelate with the fourth issue.

The third issue is whether there is intent to accept the offer. That is not a big problem with regard to Pedro. The problem arises with the two machines that were involved in making the contract, such that the contract went untouched by human hands and minds. There can be some question as to whether there was any intent, because machines usually are not thought of as having intention. To put it in civil code terminology, the question becomes one of whether there is an agreement. Have they actually come to a "meeting of the minds"? When was the last time a machine was described as really having a mind?

The fourth issue is whether whatever symbol was adopted as a signature was adopted by one of the parties as its signature? Is the symbol the signature of the buyer, Rhine.com, or Pedro? Thus, this raises the question of authentication. There is also a separate question of attribution since the book order could have been put in by Michael Gordon instead of Professor Pedro. How do we know the difference? How do we tell?

The last two issues relate to the basic legal issue of what is admissible in court. Is the contract admissible into evidence since it is really just a bunch of electrons circulating around somewhere? In addition, is the signature admissible into evidence? At common law, there is the "best evidence" rule that can create some interesting problems. The civil codes do not have the same kinds of problems, but

there is still a question as to whether the judge would accept either the contract or the signature as admissible into evidence.

**GORDON:** Let us start off then with Pedro's initial purchase of the books on Rhine.com. Is this a contract under Mexican law?

**SALDAÑA:** Well, let us go step by step. Before I answer that question, I want to elaborate a little bit on what the so-called e-commerce Act represents for Mexico. This Act was just enacted on May 29, 2000, and it has been said that the Mexican Congress did too little too late.<sup>2</sup> Nevertheless, it seems that the Federal Commerce Code was modified to add federal authority to these e-commerce issues. Additionally, the Civil Code for the Federal District was also modified. It followed that the Civil Code was the applicable law in all federal matters in Mexico, but it was not clearly stated as such. The state governments of Mexico generally follow the lead of the Federal District and the intention of the Act was to give a form of common law to all of the states with regard to e-commerce transactions between commercial. However, in particular sales or transactions, like this acquisition that Pedro is making, one must look at the domestic law of each particular state. There are thirty-two states in Mexico, and the Federal District, each with its own Civil Code. For instance, I am not sure if Guanajuato has already enacted any amendments to its civil code to provide for e-commerce transactions. However, we may explore that in relation to the applicable laws on written agreements in the Federal Civil Code.

The first point to make comes from the perspective of having studied law in Mexico, and that is that a selling agreement legally exists when the parties agree on the price and on the object that is being sold.<sup>3</sup> However, there are other issues that are essential to the formation of the contract and whether there was the consent of the parties to enter the agreement. Since the adoption of the E-commerce Act, agreements made by parties using electronic methods are acceptable under both the Commerce Code and in the Civil Code. But are such transactions valid and enforceable under Mexican law? It might be said that this is or will represent a sort of dehumanization of the legal process in which one will find the agreement of the parties done by just a click and this click represents the intent to buy that book, and therefore that person is subject to the terms and conditions provided. In that case, there too are those *contratos de adición* or "addition agreements."

This issue was modified last year when they changed the general rule in which absent parties may contract with each other only if they have signed a previous written agreement. That was sort of the old rule, and therefore, based on that rule, further confirmations of transactions could be done by telephone or telegraph. However, the rule was changed to say that if an agreement is entered using electronic means, and there is no dispute about the intention of the parties or the

---

2. See Oliver J. Armas, Mexican Electronic Commerce Amendments to take effect on June 7, 2000, (last visited March 21, 2001), <http://www.thacherproffitt.com/ealert.ihhtml?id=274>. See also Sergio Rodríguez Castillo, Clients Bulletin / E-Commerce Amendments, (last visited March 21, 2001), <http://www.bmck.com/ecommerce/mexico-memo.doc>.

3. See C.C.D.F. [Civil Code for the Federal District] art. 1794, 1824, translated in THE MEXICAN CIVIL CODE 329, 334 (Michael Gordon trans., Oceana 1980) where it states that the two elements required for the existence of a contract under the Civil Code are (1) consent or the act of agreement by the parties regarding the contract; and (2) an object for the contract that may be either the act that the obligor must perform, or must not perform, or the thing to be given by the obligor under the contract terms.

electronic method used to get that consent, the agreement is considered to be valid. The amendment to the law went a bit farther as the procedures of the civil code were also modified to provide that an electronic message, an electronic exchange of information can be used as proof or as valid evidence in a court of law. But this is only to the extent that the information derived by this technology is attributable to such person and it was not modified by any other means.

There are some issues that I want just to put on the table for further consideration for our Mexican colleagues about the capacity of the parties. A necessary element of the agreement is authentication, that only parties who have sufficient capacity may have entered into the contract. For instance, what happens if the party does not have authority because he is under 18 years old? What happens when, in the case of a corporation, a party who does not have legal authority to bind the company is clicking the web page? Would the consent be enforceable or can the parties reject that transaction?

Regarding the form of the transaction or the writing issue, some amendments were also made to allow for transactions to be valid using electronic means, but only to the extent that one goes back to the applicable law for each transaction, and for each particular state where the written form may be required. Moreover, some time is required to satisfy the formality of going to a notary public to enter into that transaction. Although the amendment provides that in those events where the certification of the notary public is necessary, the notary public will record the transaction and will keep a copy of the electronic records. However, notary publics in Mexico, and in each particular state, have their own rules and their own proceedings. These procedures require that the parties sign the agreement in front of the notary public in order to make the transaction valid. So what happens with this principle? It is effectively forgotten and overwritten, so we need to look at each state and see how it has been incorporated into the law.

Another concern is that in this problem, Pedro was using a credit card that belonged to his brother. Thus, the question is whether Pedro can bind his brother to pay for the amount charged for the purchase of the books. Will this not represent a bias to the consent given by the parties?

Additionally, based on the amendments to the Act, a basic framework was provided for e-transactions, or transactions made using electronic means. However, the major flaw of this Act is that the digital signature was not regulated. While it was the first objective of the amendments, there were complications and the Secretary of Economy or the Ministry of Commerce, as it was called during 2000, decided to put these issues on hold and to keep reviewing it. Nevertheless, the Civil Code and the Commerce Code provide that a click on a web page may be a binding transaction with some conditions and may represent a valid transaction for the parties involved.

**GORDON:** When you state that the law says this, are you reading from the Civil Code for the Federal District or from the Commercial Code?

**SALDAÑA:** Actually, you have to look at the two at the same time because they are consistent and very good changes were made to certain sections of both. For instance, the part of the agreement called the "term of acceptance" is the period after you make an offer to somebody where the other party has the opportunity to give acceptance. The old rule states, and this applies for other kind of transactions, that if you are dealing with parties that are present, the acceptance needs to be given

immediately in order to make the agreement valid. However, if the parties are absent, one needs to allow three days for the party to agree. Then one also has to consider the time required for postal service. This is because the Civil Code is from the last century and if this is not applicable, the parties must agree on the appropriate additional terms to modify the time requirement. However, this does not apply to Internet transactions because the legislators were clever enough to clarify that a transaction made by the Internet is considered a transaction between present parties.

**GORDON:** Although we are discussing an international transaction, it might be worthwhile just for a moment to look at it in the context of some of the variations of a contract solely within Mexico because this helps to clarify the distinction between a civil contract and a commercial contract. As I think you have explained, there are thirty or thirty-two different civil codes in Mexico. These Civil Codes apply to the civil contract. Let us assume for a moment that Pedro bought some books in this same way over the Internet, not from a commercial dealer, but from a friend in Guanajuato. It would then seem that we have a civil contract that would come under the Guanajuato Civil Code. Then one must ask whether Guanajuato has updated its Code to cover e-commerce. But what if Pedro buys the books from a friend who is in the Federal District? Now it would seem that there is an issue regarding the Federal District Code, which has been updated. So, let us assume that the Guanajuato Code is not updated. In this example, he is buying it from a merchant. Clearly if there were two merchants involved, one would go to the Commerce Code, which is updated. But what if Pedro, as an individual, buys the books from a Mexico City merchant by means of e-commerce? Would the Civil Code of Guanajuato apply? Would the Commerce Code apply? Would the federal law apply? Are these problems that one would have to sort out domestically?

**SALDAÑA:** Those are very good questions because they bring out the issue of what law is applicable here in Mexico. Is the applicable law that of the domicile of the retailer, or of the domicile of the buyer, or of where the transaction is going to take effect? What if Pedro gave a different address and requested the delivery of these books in Ciudad Juárez, Chihuahua, and the books are never physically present in Guanajuato. This is another internal conflict that may have the same consequences as an international transaction, such as the one described in the problem. The Federal Code says that unless the parties agree otherwise, the rule for an electronic message is that the person who is releasing the information will apply its domicile and the person who is receiving the message will apply its domicile. So we only have an issue of two jurisdictions. Unfortunately, the Federal Code is silent about which of the two jurisdictions will prevail if there is not an express agreement between the parties.

**GORDON:** You mentioned that the Civil Code for the Federal District is for the Federal District and for matters throughout the Republic that are federal. To federalize this problem from the fact situation, Pedro is a professor here in Guanajuato and he has ordered the books from Germany. There is a question of whether the Civil Code of Guanajuato or the Civil Code of the Federal District applies because it is a federal matter. How is this resolved?

**P. HERNANDEZ:** I think the problem requires a clarification. When the amendment, the Electronic Data or the Electronic Act as it is called, was made applicable to the Civil Code for electronic agreements, its name was actually

changed to the Federal Civil Code. That is why there is a Federal Civil Code that reads almost the same as the Civil Code for the Federal District. Thus, there is a Federal Civil Code, which contains the Electronic Data Regulations, and then there is the Civil Code for the Federal District. It is no longer called the Federal District in application throughout the country for federal matters. What are left are multiple Civil Codes: one for the Federal District, one Federal Code, and then one for each state. Thus, the electronic provisions apply throughout the country.

**GORDON:** So your view then is that the Civil Code of Guanajuato would not apply?

**P. HERNANDEZ:** No. I would say that it would be a valid transaction because of the Federal Civil Code. That would be my interpretation.

**SALDAÑA:** I tend to disagree with that because the Federal Congress has authority to legislate over domestic issues like sales, regardless of the way the sales are made. Remember that a transaction made using electronic data is still a transaction. The use of electronic methods does not change the core or the nature of the transaction; it remains a sale among parties. Thus, there is a Constitutional question as to whether Congress has authority to regulate a practice that has been vested on each state and in the Federal District. Therefore, the Federal Code does not apply.

**P. HERNANDEZ:** I think this is a federal provision and the Federal Congress does have the authority to regulate federal issues. At the same time, the Commerce Code, which is also a federal application, was modified such that there is no incongruence between the two laws. Accordingly, an electronic provision and the electronic transmission that one enters into would be a mercantile act. This is because such a transaction does not have to be between two merchants to make it fall within the federal concept of a transaction.

**A. HERNANDEZ:** The fact that cyber-waves are being used, which is a federal matter because it falls under the rules of telecommunications, means that Congress has the authority to regulate. These problems also involve interstate commerce as they are understood in the U.S. But as it is a legal provision, it might be attacked for constitutionality. You might recall that the Federal Congress and local governments can enact laws governing the same matter. For example, the environmental legislation has shared responsibilities, meaning that certain areas are the responsibility of the federal government and certain areas are the responsibility of local governments. This is a case where perhaps the Guanajuato Civil Code might enact something, but the Federal Congress is not precluded from enacting laws that affect interstate commerce. This is especially true when the airwaves are being used. Thus, if it is unconstitutional, it is for the Supreme Court to decide.

**SALDAÑA:** I think that in all the states, when we talk about sales amongst absent people, the Civil Code does apply. Since the Internet uses the *vías generales de comunicación*, or "general means of communication," it does fall under federal authority. The Congress did change that provision in the Federal Civil Code, but that provision was just for transactions that involve e-business. While I agree that these changes were made at the same moment and in the same congressional act, the Act also created the Commercial Registry, which has nothing to do with e-business issues. In the United States, this debate is also occurring with regard to uniformity between the states so that there are the same rules across the board.

**GORDON:** In the United States, we have never been able to work out uniformity from state to state with regard to taxation, sales taxes on purchases, etc., and we are going to have to address uniformity again because of e-commerce. I have been hearing Mexicans debate this issue for a very long time as to what are federal matters. It is nice that in the United States we never have that kind of issue of what are states' rights and what are federal rights. I think that some of my colleagues here would like to disagree with me. I would like to have them perhaps comment on not only the U.S., but also how the U.S. view differs from the Mexican view.

**NORWOOD:** Let me give you a quick background. I come at this partly from an information technology background. This whole thing is put together and works because of Internet technology. We have to realize that e-commerce, or commercial activity on the Internet, is less than a decade old, so we are in a learning curve that is quite fast and we are going to have to try to stay with it. Obviously, a lot of the old laws that we have will work on the Internet by analogy. However, many other things will not. So we are going to feel our way along and see what happens.

To begin with, I would say that all of the participants in this problem have a high interest in all of these transactions being valid. The United States has an interest in it, the government of Germany has an interest in it, the government of Japan has an interest in it, Pedro has an interest in it, and Rhine.com and East all would like these transactions to work. There are problems with these transactions that are identified in these problems, and we should go through those, but I would start with that assumption that it is very important that we figure out ways in which these transactions can be made to work.

The Internet, as I said, is the foundation. The Internet does one thing well, and that is about it. It manages information. It communicates information, it stores information, and it allows you to retrieve information. It is all about information. Human commercial activity, to a large extent, is about information; but it is important to keep in mind that it is not exclusively about information. There are aspects of commercial activity that just cannot be replicated by reducing everything to some form of information. Now, the key problem with this transaction is with Rhine.com. It is hard to figure out why Pedro did not go directly to East and East did not go directly to Pedro and why they went through Rhine.com, other than it presents a nice problem. The whole purpose of Internet, according to theorists, is to get rid of this intermediary. However, in this problem, there is an intermediary: Rhine.com. Who needs them? They raise the price for Pedro, and he should just go directly to East and simply cut out Rhine.com.

Nevertheless, the problem with Internet activity or human activity is, as the common saying goes, when you are using the Internet, no one knows if you are a dog. In addition to that, no one knows if you are talking to a dog. The problem here is authentication. Who knows what is reliable, who knows what is authentic, who knows who is who? In other human activities we have a little more information about that, but not much.

The problem changes from a technology point of view. If we are going to have these transactions, we have to have some method for making a record that we know is authentic, reliable, stable and available in a non-fragile, usable system. There are a lot of people who are nervous about using the Internet because they think it is fragile, unstable, and insecure. Now, that is a generalized problem about the



Internet. But with this particular transaction and with any commercial transaction, we would like to know if the record is authentic, reliable and stable. We would like to know who is the person who has participated and initiated the transaction in this problem. We would like to know who he is and if he is authentic, as the person who really who did it. We would like to know that in fact he performed the transaction with deliberation. That is one of the attributes of a signature. When you sign something, it is like a ceremony. You pause, and you think about what you are signing. You may have never read what you are signing, but you sort of believe it is okay. You also want to know that what you are signing will remain what it is you are signing, and that nobody is going to change it in the stream of commerce, or that somebody is not going to come along and erase everything above your signature and put something different there. So what you sign and the stability of what you sign has become critical.

When you sign, it can be very important for transactions that occur later on, and so you have to have some date stamp, or a time stamp, to make sure that you know exactly when the commitment was made. For jurisdictional purposes, it allows one to know where the commitments are made. However, that can be very difficult sometimes because there are servers recording all this data in Kansas City and participants in Germany and in Mexico City. So where this took place can be tricky. But we need to know where Pedro was at the time he signed.

The answers to these problems are three fold. The first answer is code. That is, drafting or writing software that handles these issues and that assures these authentications. The problem with code is that it is built on bits and bytes that are like atoms, meaning that they are everywhere. Not only are they everywhere, but they are available to everybody, which means that bits and bytes can enter into the stream of commerce from all sorts of strange sources and all sorts of places, which leads to some other aspects called cyber crime and viruses. But there is code and a lot of solutions to these problems are based on code. Writing the proper code with the digital signature is largely based on encryption, or private key, public key code. The second answer is regulation. The regulations right now coming out of the United States, I would argue, are generally based on promoting commerce. The third answer is self-regulation. This includes self-help kind of concepts, and there is a lot of strength in people promoting those as the answer.

So in terms of the question we are left with, which was whether we have some standard or general approach to this from country to country, the answer, at least within the United States, is moving rapidly toward cyberspace in interstate commerce. The federal government will be the one that basically has to regulate, if regulation is at all required. There will be very little opportunity for states have any input, especially where commerce is concerned.

**SPANOGLE:** The U.S. approach to this has been on a dual-track basis, as far as electronic contract formation is concerned. There are three issues under the Uniform Commercial Code. One issue is the Statute of Frauds. The second issue is the requirement of assent and the third is the definition of a signature. One answer is that the federal government has enacted what is called the E-SIGN Act.<sup>4</sup>

---

4. See Electronic Signatures In Global and National Commerce Subchapter I—Electronic Records and Signatures In Commerce, 15 USCA §7001 et seq. (approved 12-18-01).

The Federal E-SIGN Act is a fairly simple piece of legislation at its core. It provides that a court cannot deny enforcement of a contract solely because it exists through an electronic record or is in electronic form.

But then the devil is always in the details. The details are usually in the definitions, and the definition of "record" is "information stored in an electronic medium, which is retrievable in perceivable form." It was always arguable under the UCC that if an e-mail was printed out, there was a writing. Although that argument was never put to the test, it is a pretty good argument. If you never downloaded the e-mail, under the UCC there probably was not a writing. The E-SIGN Act says that the e-mail never has to be downloaded; however, one does have to be able to bring it up on a screen so that people can perceive it, and that is an interesting distinction. The E-SIGN Act applies to all contracts in interstate commerce and in international commerce. It does not, however, apply, as it could have, to all contracts that use interstate communication devices. Almost any contract on the Internet would have been covered by that latter language, so the E-SIGN Act contains a narrower definition than it really had to. What the Federal Congress wanted to do was to push the states to enact enabling legislation. If you then look at what the states have been doing, they are enacting such legislation. The National Conference of Commissioners on Uniform State Laws (NCCUSL), who drafted the UCC, has drafted the Uniform Electronic Transactions Act (UETA).<sup>5</sup> The E-SIGN Act states that it is applicable to all contracts in interstate commerce, unless the applicable law is the law of a state that has enacted the UETA as promulgated by the Uniform Commissioners in 1999. A problem with this is that the Uniform Commissioners can never go back and change their minds about any of the provisions in UETA unless they get federal congressional permission to do so, because no state is going to put its exemption from preemption in jeopardy.

The state-enacted UETA repeats many of the provisions of the federal E-SIGN Act. Thus, UETA starts out by establishing that one cannot deny effective enforcement of a record solely because it is in electronic form. It then goes one step further, as only a state law can, and states that a record in electronic format satisfies the writing requirement in any state statute. The federal law could not do that. Federal law could state what satisfies state law, but only what would grant standing to let them into court. However, UETA, as state law, can say what is sufficient to satisfy the requirements of state law. The definitions of record and electronic record are the same thing as in the E-SIGN Act, so the two statutes track each other.

The concept of signature raises many of the same problems, but not always the same answers. The UCC says that any symbol adopted by a party with an intent to authenticate is acceptable as a signature. That symbol can be a sixteen or sixty-four-digit algorithm, so those folks in the industry of e-commerce simply approved that. But there is still the problem of the requirement of a signed writing: does the signature need to be in writing or can it be in this other form? The E-SIGN Act solves that issue and so does the UETA. Both of these Acts establish that a

---

5. The National Conference of Commissioners on Uniform State Laws also have drafted the Uniform Computer Information Transactions Act, but the UCITA has been enacted in only one state because it is a much more controversial piece of legislation. See also <http://www.etaonline.com/index.html>.

signature in electronic form is acceptable. The state act goes further and says that it satisfies the writing requirement. However, note that the statutes require that the symbol be adopted by the purported signer. One of the issues for litigation is whether, when I click something on a web page, I have adopted that click as my "symbol," intending to authenticate my actions. Or, is this an unintentional or mistaken act on my part; or the dog or cat playing on the keys? There are a myriad fact-based problems and hypotheticals that must be worked out in this area. However, the statutes have at least given you a criterion.

For a German contract, you have a whole different set of problems. The German Civil Code, at least until it was amended recently, provided that the only signatures admissible in court were hand-written ones. Facsimile machines were out. Signature stamps were out. They did not like symbols. The implication of the requirement of hand-written signatures was that a person was required to write his or her name and not a symbol. Recently, however, the Germans have adopted two pieces of legislation, one of which takes into account that the 21st century has come and that electronic signatures must be considered as an option. There is also an E.U. Directive that provides that there will be regulation as to what will be permissible as a signature. This analysis now gets into admissibility in court, but it is hard to talk about one without the other.

In most contracts, when the person on the other end of the transaction provides a name, there is a contract, and there is little reason to worry about it. There is a possibility of fraud, and sellers adjust their price just a little bit for that possibility, but they do not hesitate to "make that deal." Particularly in mass volume transactions, sellers do not take a whole lot of time and trouble to authenticate who the buyer is at the other end of the line. However, there are the transactions that involve shipping \$10 million worth of diamonds, industrial or otherwise, off to a purported buyer. In that case, a seller really does want to know who the person is at the other end of the line. Thus, those in technology have created something called public key encryption (PKI), which is a wonderful set of technical gizmos using third parties to certify that my sixty-four-digit algorithm really is me, and to change it for each transaction to ensure security. PKI is necessary in the \$10 million transaction.

The problem with PKI arises when a legislature starts defining what types of authentication a court will be permitted to accept. One option is to mandate PKI, and maintain that it has to be through a certification authority that is licensed by a state. Thus, there is a three-tier division of digital signature legislation between (1) statutes that require PKI with licensed authorities; (2) statutes that require PKI with no government interference, just mercantile influence; and (3) statutes that have no requirements but allow courts to make determinations based on the facts. Most catalogue transactions operate on the latter, which is based on the faith that most people are who they represent themselves to be.

When you look at the E.U. directive, there are ten substantive provisions. Nine and a half of those ten provisions talk about how to do public key encryption, how to set up certification authorities with licenses and how to supervise those licensees.

This is all fine for the \$10 million transaction but not particularly helpful for the \$10 transaction. Then, one-half of one article talks about all other forms of electronic signatures, and provides that a court may not discriminate against a signature simply because it is in electronic form. What is missing from that E.U.

Directive is any criterion for authentication of any signature other than one using PKI technology. Thus, here is an attempt to regulate by saying "we are going to hold you to the highest possible standard."

Such legislation imposes an enormous cost on most e-commerce transactions, the usual mass marketing and B2C transactions. The legislation also imposes even on the people who are selling \$10 million worth of diamonds, providing that they too need to be regulated and that their method of self-regulation, by choosing a non-licensed certification authority, is not acceptable. PKI legislation also usually gives a monopoly to a certain type of person who can obtain a license from the state to run the certification authority.

There are both types of digital signature legislation in the United States. Utah supports the use of public key encryption because they had a lot of technology experts who knew all about PKI technology. On the other hand, California, which is not interested in public key encryption, but also has a lot of technology experts, enacted legislation that permits signature authentication by bio-metrics—retinal scans, voice recognition, etc. Then, there are states in between, like Illinois, which allow parties to use whatever technical system is appropriate to the kind of transaction they are doing. That middle standard was built into the UNCITRAL Model Law on Electronic Commerce.<sup>6</sup> I would assume that is what you have in your Mexican Federal Statute, the standard that was built into UNCITRAL.

But at least note the tension here. The regulators say "we know how to do this and we want to have a really high standard." By contrast, the merchants are saying, "let us make these kinds of decisions as to how far you push it. We do not want to give a monopoly to the state-licensed PKI certification authorities because somebody in two years is going to come along with software that makes all of that inefficient, costly and obsolete." That is the tension in the legislative arena.

**GORDON:** Let us look at the fax situation. The writing, signature, intent and authentication are all at issue under Mexican law such that it is curious what the result would be with a fax. Maybe we do not have enough facts, but how would one answer under Mexican law on the first contract, if there is a contract, between Pedro and Rhine.com?

**SALDAÑA:** Based on the e-commerce act or whatever we want to call it, the Congress regulates that particular item. Thus, in the Federal Civil Code and in the Commerce Code, there are the same kind of rules, which basically state that acceptance given by electronic methods or means, optical or any other technological means, will be considered an acceptable way to give or to demonstrate consent. What this means is that the rules for acceptance were modified in regard to absent parties. Recall the rule that requires that acceptance be given immediately when you are making an offer to somebody who is present has been modified. The same rule now applies when you are making an offer by telephone or by any other electronic method, optical or any other technological means. In other words, you no longer have to wait three days to accept the offer.

There are other issues with regard to the technology and standards compared to those used in Utah, California, or Illinois. With respect to those standards, we

---

6. See UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, (visited March 21, 2001), <http://www.uncitral.org/english/texts/electcom/ml-ec.htm>

realize that the Mexican laws are using very clumsy language because the statutes provide that as long as the information generated is communicated in integral form, it is attributable to those persons who have the intention to be obligated, and it is accessible for further consultation.

**GORDON:** I can understand that we perhaps have eliminated the writing and the signature here, but how can we say that Pedro intended to be bound in this case because it seemed to me that he intended his brother to pay the price and he had no intention whatsoever of being obligated on the contract. How would Mexican law handle that?

**SALDAÑA:** That is a very important point. Let us assume for a moment that Pedro has the approval of his brother to use his card. Then the facts state that this electronic exchange of information is attributable to the persons who want to be obligated by this transaction. However, the amendment does not elaborate on what occurs when one is acting on behalf of someone or when one represents another party.

**GORDON:** Pedro gave only his mailing address in addition to the credit card information. There does not appear to be any attempt by Rhine.com to authenticate, nor does there appear to be any attempt to prove that Pedro was Pedro. How would Mexican law deal with authentication and attribution?

**SALDAÑA:** The way it is treated in both main bodies that regulate this area, which are the Federal Civil Code and the Commercial Code, is that agreements made between parties using telegraph, electronic methods, optical methods or any other technology, legally exist once the acceptance to the proposal has been delivered. The Mexican law does not yet cover these complications or intricacies of codification or authentication. There was a big assumption that as long as the information was given or obtained and may be replicated further on, the operation is valid. As previously stated, authentication was left out of the e-commerce Act at the last minute by the Mexican Congress.

**GORDON:** Would U.S. law give us as clear an explanation as under Mexican law?

**SPANOGLE:** Interestingly enough, the E-SIGN Act contains absolutely nothing about attribution, so what you get is whatever the state law is. The UETA does provide what would be normal U.S. agency law, with no additions for e-commerce. There is attribution if there is an act of a person, which can be shown in any manner. It can be the act of a person, the act of a person's employee who is acting within authority, or the act of a person's computer if it is programmed so to act. That takes care of East and Rhine.com and the contract formed by machine. Incidentally, the two businesses probably have a trading partner agreement to iron out these problems anyway. This is a fair example of actual, apparent and ostensible agency issues, and there is no new point of contention.

The new point of contention arises under the Uniform Computer Information Transactions Act (UCITA)<sup>7</sup> and the UNCITRAL Model Law. It is the question of whether an act done by a third party is attributable to you if there was an agreed-upon procedure between the parties, including you, and a third party used that

---

7. See What is UCITA: A Commercial Code for the Information Age, (last visited March 21, 2001), <http://www.ucitaonline.com/slhpwiu.html>.

procedure without authorization. This problem arises if the security procedure was used by the janitor, who is an unauthorized employee; or even if it arose from the cat on the keys, or if a hacker did it. Do you have a presumption? And the sensitive issue is whether this is a conclusive presumption or is it a rebuttable presumption.

The second issue in this area is whether unauthorized use of a security procedure is attributable to the identified principal if the principal gave the signature methodology to some third person without actual authority to use it. Again, should the issue be determined by a presumption and, if so, should it be a rebuttable presumption or a conclusive presumption?

The background for those questions goes back to banking law. Many employers who issue paychecks use facsimile machines to sign them, and the bank can either say "yes, we will accept that as a signature" or no. In the contract with the bank, they will almost always say "well, all right, you can use a facsimile machine if you want to, but you have to realize that, if someone else breaks the lock on it or you forget to lock it up one night and the janitor rolls out an extra \$50,000 worth of paychecks for himself, you must pay them because that is going to be your signature."

Applying the same concepts to e-commerce, if you agreed on a security procedure, if you set up one of these public key encryption algorithms, and somebody uses it without authorization, are you stuck with the unauthorized transaction? With the public key encryption, that probably makes sense, but with lesser things it probably does not. Again, a statute where one size fits all and there is strict liability is probably not terribly appropriate. Although, if you give the benefits by law to a party, they will want to use it, and the bank would like to say "you are liable on all unauthorized transactions using your credit card number, even though somebody just guessed it or took it off of a slip you discarded." However, that is not the law in the U.S.

**ROGERS:** Could I just ask if the hypothetical could be modified slightly to illustrate something? Let us suppose that this is Pedro S.A. de C.V. It is a legal entity, a corporation, and he is ordering \$10 million worth of books, and there is a public key encryption system in place, and he is ordering from Rhine.com, GMVH, who is also incorporated. These are all legal entities. How does the question of corporate authority for entering into these contracts get addressed in a public key encryption system?

**SALDANA:** Basically, under the Mexican regulations, there is a presumption that the data message is received from the issuer of the message, if the message has been sent using identification methods, just like *claves* or *contraseñas*, which means special encryption, or any special number or special name that both parties have agreed. Moreover, bear in mind that this is using an information system that has been programmed by the issuer of the message, or on his name, in order to operate automatically.

**SPANOGLE:** That is only for agreed-upon security measures. That means that the parties to the transaction have an umbrella agreement or a trading partner agreement between them. It does not work very well in an open system, so be aware of where this is applicable and where it is not. Also, there is probably a different treatment in the order to East and the order to Rhine.com if Mexican law does not apply. German law will basically say that since you have established a public key encryption identification, certification authorities will rely upon it, and

under the E.U. Directive and the German legislation, you are bound. American law will require you to look at the contract you have with East and determine whether it agreed to the use of public key encryption. Also, you would have to examine who did, in fact, use the PKI methodology and whether you have any defense. If there is a trading partner agreement, then you have got to look at the words and the presumptions that were set up in that contract.

**ROGERS:** Let us assume that in each country involved there is a certification authority, and under the trading partner agreement, each company has agreed that its order will be carried out through an electronic ordering system, and those orders will be made effective by any authorized officer of the company. How does the determination of whether the person who clicks the order is an authorized officer effect the contract?

**SPANOGLE:** That is where the second half of what I was talking about from UNCITRAL, which I suspect is also in the Mexican law, does come out. If you do not control the public key encryption algorithm or how to access it on the computer, then it is effectively over. It is the same as if you do not control the facsimile machine; then it is effectively over. And so the second part of that says it is attributable if somebody got it from you, usually through your negligence or with your consent, even if they are not authorized. Only the guys who are authorized better know how to get to that part of the computer.

**GORDON:** Let us move on. Which traditional system, the civil law tradition, which would include Mexico and Germany, or a common law tradition in the United States, is posed with a more difficult problem in terms of admissibility of evidence when we move into e-commerce?

**SALDAÑA:** Well, I guess, again, we have sort of two kinds of rules here. First, in the last amendment, they permitted the use of electronic data as valid evidence, which is important. I think it will be a cornerstone for these kinds of transactions. However, if you look at the Mexican law for the protection of consumers, the burden of proof is on the merchant's side and not on the buyer's side. So if there is any problem about legality or about authority to bind the other party, you can go to that particular provision in the amendment and start claiming several rights with regard to the particular language that covers the whole country. There is a particular legal body that applies through all Mexico in all of the states.

**GORDON:** Do Mexican discovery rules adequately reach the kind of evidence that might be necessary to prove the existence of a contract plus authentication, etc.?

**SALDAÑA:** They used an approach that benefits the business side of transactions. They again made a presumption that if there is any information exchanged using electronic means, it will be considered attributable to the persons who are considered to be obliged if and only if that information will be accessed for further consultation and it is not modifiable.

**SPANOGLE:** At least at common law, and I suspect at civil law as well, the real question is how the data has been stored. You have to be able to introduce evidence as to how it was stored. Then the other side can start figuring out ways in which, however you stored it, it could have been tampered with. If they can prove that you could have tampered with it or that somebody else could have tampered with it, the judge is entitled to say, "I do not think I am going to give this any weight." So you must think about storage security and the messages must be reproducible.

UNCITRAL was hampered in the development of a Model Law by the U.S. best evidence rule.<sup>8</sup> I do not think there is any comparable civil law doctrine. Some specific rules in both types of legal systems require originals. Additionally, there are rules that require notarization, and that is more likely to be a civil law difficulty. This might lead to the point where you may require a certification authority acting in the capacity as a notary, and these issues are fairly easily solvable. Both the UNCITRAL Model Law and the E-SIGN Law say almost nothing about this. UETA Articles 12 and 13 deal with it without many problems, and UNCITRAL Article 9 deals with it, and that is all fairly straightforward. But if there is no legislation like UETA or the UNCITRAL Model Law, some judges will simply say "I have no reason to trust any of this, good bye and good luck." That is one reason for having facilitating legislation in this area.

**SALDAÑA:** Let me again repeat very clearly what are the three requirements that the procedure law requires in order to make this electronic information acceptable in a court of law. First, where there is a method that generated the information or someone who received the information or filed the information, it is "trustable." Second, when it is feasible to impute to any of the persons who are deemed to be obligated by the content of the information, then we get to the issue of Pedro and his brother. Third, the information is or may be accessed for further consultation. If you complied with all the three requirements at the same time, that kind of information may be used in a court of law.

**GORDON:** Let us turn to number two, the question of jurisdiction, where and what law? Looking at the first contract, Pedro and Rhine.com, what would Mexican law say in regard to the appropriate form and what is the applicable law?

**SALDAÑA:** The Mexican law did not spend too much time on the E-Commerce Act with regard to this type of issue. It simply states that when the issuer of the message and the recipient of the message interact with each other, the message has been released from the place of the domicile of the issuer. This is also true in the case where the consequence of the recipient is the same as the domicile of the recipient. There was no elaboration as to the conflict that may apply in the particular rules and that might be applicable for both. I mean, for the reseller and the buyer, and for an international transaction, the conflict goes deeper.

**GORDON:** Do you think on the facts in this case that if Rhine.com were to go into a Mexican court demanding payment from Pedro, disregarding the brother issue and assuming Pedro used his own credit card, that a Mexican court would retain jurisdiction of the matter? Would they possibly then apply German law?

**SALDAÑA:** I think on that particular question that if Pedro rejected payment or rejected the goods, the only real possibility that Rhine.com may have in order to enforce an agreement would be under Mexican law. This is because Mexico is the place where the acts will have a legal effect on the one hand. On the other hand, since the buyer is here, and the reseller is giving up the jurisdiction, that he may claim this based on his domicile and I do not understand why a Mexican court would reject the jurisdiction under those grounds. And consider the reforms that

---

8. See *Gordon v. United States*, 344 U.S. 414 at 421 (1953) where it states that the "best evidence" rule rests on the fact that a document is a more reliable, complete and accurate source of information as to its contents and meaning than anyone's description and this is no less true as to the extent and circumstances of a contradiction.



were made to the code that allowed an electronic agreement to be valid if it is not signed.

**GORDON:** It sounds like a good time for a country to adopt *forum non conveniens* if they have not already, not that there is not available an adequate forum, but we certainly do not want to get involved. What if Pedro were a Texas resident now? So this is a question of U.S. versus German law.

**SPANOGLE:** Well, it depends as always on whether you are in a German court or you are in an American court. If you are in a German court, the Treaty of Rome says to apply the law of the place of business of the person who is performing the characteristic performance. So, in the sale between Rhine.com and the consumer, that would be German law, and in the case of East selling to Rhine.com, that would be U.S. law. If you go to a Texas court, it is relatively certain that they will take a look at UCC §1-105 and apply American law. This was the "imperial clause" deliberately designed by the original drafters of the UCC to make sure that it was used as much as possible before it actually became adopted in forty-nine states.

There is an interesting question that you are about to skip over that I am going to bring up anyway. What American law would you apply? Suppose, for example, that the book is not shipped in hard copy but instead is made available as information over the net, which Pedro can download on his computer and print. Is that a sale of goods? Courts have gone different ways on that under the UCC, so you have an interesting split of opinion. If UCITA ever becomes enacted throughout the United States, it would resolve debate as to whether this was sale of information, rather than a sale of goods.

A different issue arises if this is still a sale from East to Rhine.com, which is in Germany, to Pedro who is in Mexico. Is it thought of as a sale of goods under the U.N. Convention on Contracts for the International Sale of Goods (CISG)? My reading of the four applicable cases under CISG so far would indicate that it is.<sup>9</sup> Each of these countries is a contracting state to the CISG, and both sales would fulfill all the requirements of Article 1, Paragraph (1)(a). In these sales, you would not apply as American law the UCC. Instead, you would apply as American law the CISG. Further, you would not apply as German law the German Commercial Code; rather you would apply the CISG. One of the fortunate things about CISG is that it does not require a writing. So you have just escaped the Statute of Frauds.

**GORDON:** But it does require other things, and it is kind of interesting because the CISG being international law having then been implanted as domestic law does not have this developing body of electronic commerce overlay. In Mexico, there is the E-Commerce Act so we maybe saved one problem with the CISG. However, we may have some other problems that are serious and that were not considered. How do we resolve those?

**SPANOGLE:** Well, in the United States you have the E-SIGN Act. In Germany you have the German Electronics Law and the E.U. Directive, and in Mexico, if I understand it right, you have a new federal law here. All of these laws basically say that a signature in electronic form, for instance, can still be valid. That is the problem that would be left. UNCITRAL, which I believe Mexico adopted

---

9. See RALPH H. FOLSOM et al. HORNBOOK ON INTERNATIONAL BUSINESS TRANSACTIONS (2nd ed., West Group 2001) at §1.6.

faithfully, and UETA both say that machine-to-machine contracts are valid, and that a machine can generate assent, so in all of these cases the contract should be enforceable.

**SALDAÑA:** That is the case, and you are exactly right.

**GORDON:** Let us look at our privacy issue, which is always interesting and we all have, I think, personal situations where we think our privacy perhaps has been invaded by the gathering of information about ourselves. Rhine.com has been sending daily reports to its parent, Rivers.com, in the United States and they are gathering information, as it is typically done. That information talks about individuals who are interested in different subjects. So, Pedro now finds himself on all sorts of mailing lists. He opens up his e-mail and begins to find offers to go to the World Cup and all sorts of things. We all have very different fundamental views of privacy. I have polled my students in international business when we do this problem as to whether they would prefer to have a European model privacy law or a U.S. privacy law, and they uniformly prefer the European view. Of course, it depends on how you phrase the question to them. But let us look at some of the privacy issues here. Rivers.com wants to know whether it can continue its practice of disseminating information in view of the European Union Privacy Directive. It is necessary to determine whether the United States has made adequate changes to satisfy the European Union or whether it continues to be a country that would violate the policy of the E.U. guidelines. There was an act, but it was one that was fairly encompassing, and intended to cover every possible act of human conduct. I think it did not have any e-commerce in it, and I think that exemplifies the attitude of many civil law tradition nations, to regulate conduct. Our attitude has been more, I think, to fix things through legislation when things are broken. How does this difference in attitude affect the development of legislation in our different countries? How does it affect it on an international level? It would seem to me that while I know this is not true, but it would just seem to me that we should question why we should be bothering to participate in all of this because it goes against our philosophy to try and draft a code that covers all parts of our conduct.

**NORWOOD:** Let me start by asking a question: who owns the Internet? Of course, the answer is that no one owns it. The Internet is basically a set of software tools that are made available to anybody who wants to enter into the Internet. The only centralized force needed to make the Internet happen is a company now called ICAN, and that is a company that manages all of the Internet addresses, which means all of the dot coms, dot biz, dot org, etc., then some that are followed by country codes, they are issued to .mx for Mexico, for example. One central authority controls all of those domain names, which is necessary because otherwise the addressing systems just would not work. That authority is now a for-profit business called ICAN. Anyway, because no one owns the Internet, the question is, who do you regulate and how do you regulate what is going on? Well, it also is constructed with Internet service providers (ISP's). These are gateway people. These are people that you contact in order to have domain name, to have dot com or dot org. You contact them and you have free access to anywhere on the Internet, which people try to limit by code, but then the question is whether you going to regulate the users. Are you going to regulate the carriers, the ISPs, the people that allow this traffic to go on, and to what extent are you going to regulate them? Who can you regulate? Can you regulate people outside of your country? Can people

outside of your country regulate you? And these are sort of the threshold issues of regulation, which was the philosophy of the people that invented it. Let us let it go, see where it goes, and sort of that is where we are now.

**SALDAÑA:** I do not think there is anything to add on that experience on the Mexican side. I just know that ICAN in Mexico has been sued by some cyber squatters which claim to use some names like BMW, which means Buenos y Malos Web and they sued them for damages after ICAN canceled the registration of that domain name. Also Yahoo de Mexico and Banorte have sued squatters. You have these stories of people who are trying to take advantage of those kinds of rights in cyberspace.

**SPANOGLE:** Let me again distinguish between statutes that facilitate transactions and those that regulate. Most regulatory statutes seem to cause more problems than they solve. On a commercial level, we have talked about a couple things, like the public key encryption as an attempt to regulate. Businessmen like to use the law to leverage themselves, to get an advantage. That is part of the job of lobbying. One example is Article 16 in UETA where a business with a solid monopoly on one methodology persuaded the drafters of legislation to provide that it was the only permissible methodology. In many respects, UCITA is comparable. Here is a law written for Microsoft, and it seems to be a wonderful Microsoft protection device which, if enacted by states, can be used to control many aspects of e-commerce not only from coast to coast but, depending upon events in the Hague, perhaps globally. It does not state that it is a regulatory statute. So, watch out. This kind of regulation comes in all sorts of flavors, and you may not know what is in front of you. Some apparent facilitation is really regulation in disguise.

**NORWOOD:** Let me, on the regulation front, just add that there are interesting places where regulation can sneak up on the Internet and all of a sudden have a huge impact. An example is the North American Free Trade Agreement. NAFTA has a provision in it for international practice of law, which means that the practice of law now may well become multi-jurisdictional, whether you have a license where you are practicing or not, as long as you have a license somewhere, in cyberspace. NAFTA never really contemplated the practice of law on the Internet, but yet some clever lawyers are going to figure out: I want to do multi-jurisdictional practice so I can sit in my home in my bathrobe and practice law anywhere in the world. Well, anywhere in the NAFTA world. So I am sure that the WTO probably has some similar opportunities. There are going to be opportunities that arise and Internet users are going to quickly take advantage of them in the commercial sphere. The other thing I would just mention is that the biggest threat to the Internet is crime: cyber-crime of all kinds. Basically anything that damages data, disrupts data, or harms computers. Viruses we are all well aware of. And these are going to involve not only some good detective work and some good security devices, but also some international agreements on bringing criminals to justice. The Internet is pretty fragile; it is pretty vulnerable to really smart people, and even not-so-smart people. I think Scotland Yard, for example, recently made a public prediction that within ten years, half of the crimes that they work on will be solved using their computers, but half the crimes that they have to solve will be committed using computers.

**GORDON:** Thank you. If we had done this five years ago, I think we would have spent most of our time identifying issues. Those issues seem to be much clearer to us now, and our governments have enacted a good deal of legislation in

an attempt to address them. But one thing that certainly has been absent is any body of case law from any of our nations. Perhaps if we look at this in another five years, we will begin to sort out some of the issues that we talked about today but did not come to any clear conclusions.

### **BIOGRAPHICAL SUMMARIES**

Professor Michael W. Gordon is the Chesterfield Smith Professor of Law at the University of Florida College of Law where he teaches international business transactions, international trade law, international litigation, and the law of NAFTA, S.W. 2d Avenue at S.W. 25th St., Gainesville, FL 32611. Telephone: 352-392-2211. Fax: 352-392-8727.

Prof. Gordon has held the Centennial Professorship at the London School of Economics, the James S. Stone Chair at Alabama, the Alverson Chair at George Washington, and also has been a visiting professor at Duke, Konstanz, Frankfurt, Escuela Libre de Derecho (Mexico), Universidad de Costa Rica and King's College (London). He has lectured in the United States for the Council on Foreign Relations and abroad for the Department of State. Prof. Gordon has consulted for ten foreign governments, held Fulbright professorships in Mexico, Guatemala and Germany, and been a Scholar in Residence at Bellagio. He has authored or co-authored more than thirty books and numerous chapters and articles. His books are principally on international business law, comparative law, Mexican law, and on the NAFTA. Professor Gordon was appointed by the Clinton administration to the dispute resolution panel rosters of both the World Trade Organization and the North American Free Trade Agreement, and has served on two NAFTA Chapter 19 panels. He received his B.S. and Juris Doctor degrees from the University of Connecticut, his M.A. degree from Trinity College, Ireland, the Diplome de Droit Compare from the University of Strasbourg, and Maestria en Derecho from the Universidad Iberoamericana, Mexico. He was admitted to the Connecticut Bar in 1963.

Prof. J. Michael Norwood is a Professor of Law at the University of New Mexico School of Law, 1117 Stanford NE, Albuquerque, New Mexico, 87131-1431. Telephone: 505-277-6553. E-mail: Norwood@law.unm.edu

Professor Norwood's interest in computer technology includes both computer applications and the law that governs the use of computers, especially Internet law. He was the inaugural research scholar at the Centre for Computer Technology and Law at the University of Strathclyde in Glasgow, Scotland in 1992. He is currently a member of Board of Directors of the Center for Computer Aided Legal Instruction (CALI), and he is CALI's immediate past president. Professor Norwood received the J.D. degree from the University of New Mexico School of Law in 1970 and was admitted to the Bar of the State of New Mexico the same year.

Lic. Roger Saldaña is a corporate counsel of Cemex e-business division CxNetworks, Lic. Saldaña is currently living in Miami, Florida and working for a CxNetworks subsidiary NEORIS at 703 Waterford Way, Suite 700, Miami, FL 33156. Lic. Saldaña has specialized in international business transactions, in areas such as mergers and acquisitions, intellectual property, consulting, software agreements, taxation and general corporate matters. Before joining CxNetworks, he was in-house counsel of Cydsa, SA in Monterrey from 1995-2000. During 1994-1995 Lic. Saldaña was an associate of Fried, Frank, Harris, Shriver & Jacobson in

New York. Prior to that he was Chief of the Double Taxation Department of Mexico's Treasury Department (*Secretaria de Hacienda y Credito Publico*) in Mexico, D.F. Lic. Saldaña received his law degree from the Universidad de Monterrey in 1989 and was admitted to the Mexican Bar in 1990. In 1994 Roger obtained a Masters in Law degree (LLM) from Harvard University and a diploma from Harvard's International Tax Program (ITP), Harvard's ITP awarded Lic. Saldaña a certificate for research and writing for his paper regarding Transfer Pricing Issues. Lic. Saldaña was an OAS and CONACYT Scholar.

Prof. John Andrew Spanogle is William Wallace Kirkpatrick Professor of Law, George Washington University School of Law, 2000 H St., NW, Washington, D.C. Telephone: 202-994-7015. E-mail: [aspanogle@main.nlc.gwu.edu](mailto:aspanogle@main.nlc.gwu.edu). Professor Spanogle's primary teaching and research interest is in the field of international business transactions. His casebook on International Business Transactions (West Publishing Co. 4th Ed. 1999) (with R. Folsom and M. Gordon) is the most widely-adopted coursebook in that field. He and his co-authors have also published a Treatise and Nutshell books in that field and in International Trade and Investment. From 1982 to 1989, Professor Spanogle was a member of the U.S. delegation to UNCITRAL (United Nations Commission on International Trade Law) and was the Chief of Delegation to UNCITRAL's Working Group on Payments Systems. During that time, the Working Group completed the drafting of the U.N. Convention on International Bills of Exchange and Promissory Notes (1988), and then began drafting Model Rules for International Credit Transfers. Since 1991, he has been an Advisor to the World Bank and USAID on creating the legal infrastructure to permit secured transactions. In 1996, the Polish Government enacted a Registered Pledge Law on which Professor Spanogle had worked for five years. His other primary interest is in U.S. domestic commercial law, a field he first explored as Research Assistant to Professor Karl Llewellyn, the principal draftsman of the Uniform Commercial Code. His newest interest is in the law of Ecommerce, both domestic U.S. and, comparative and international. He will be, a co-author of a casebook on this subject to be published by West in 2002. Prof. Spanogle graduated from Princeton University in 1957 and the University of Chicago School of Law in 1960.