E-COMMERCE PROVISIONS IN THE UCITA AND UETA

This July, the National Conference of Commissioners on Uniform State Laws will vote on the Uniform Computer Information Transactions Act (UCITA) and the Uniform Electronic Transactions Act (UETA). UCITA is a broad statute, intended to govern all aspects of contracts that involve software, digitally stored information (such as movies, music and books on CDs), and (if so specified in the contract) goods that are bundled with software (such as computers). UETA applies to a broader set of transactions, but only with the limited objective of facilitating electronic contracting.

Both bills have electronic commerce provisions; these provisions sometimes conflict.

This article probes the differences between UCITA and UETA, primarily in terms of issues of concern to customers' advocates. The timing of this article is difficult—at the time of writing, the conference drafts of UCITA and UETA were not yet available. I've based these comments on the February draft of UCITA, the March draft of UETA, and committee meeting notes from both.

Here are the issues:

1. What is an electronic signature? Under what circumstances is an electronic "mark" a signature, and what does the presence of such a mark signify?
2. What about consumer-protective rules that require written agreement to some terms?
3. What if one person fraudulently makes the electronic signature of another?
4. Is the customer entitled to a downloadable or printable or printed copy of an electronically made agreement?
5. What rules will apply to receipt of legal notices?
6. What about mistakes made by a customer?
7. What about choice of law and choice of forum?

I ordered these nine issues in a logical sequence rather than in priority order. I would most like to draw your attention to receipt of notices.

1. What is an electronic signature?

You can affix your name or mark to a document for many different reasons. For example, when you send an e-mail message and type your name at the bottom,

(A) you might merely be identifying yourself as the author of the message, or

(B) you might be agreeing to a contract, or

(C) you might be sending a message back, saying "This is what I received." If I send you a message and you return it to me, and if both copies match, then you know that I received what you sent, without error.

UCITA 102(b)(4) recognizes that any of these are possible by defining "Authenticate" as "to sign, or otherwise to execute or adopt a symbol or sound, or to use encryption or another process with respect to a record, with intent of the authenticating person to: (A) identify that person; (B) adopt or accept the terms or a particular term of a record … or (C) confirm the content of the information in a record. However, it then (UCITA 119 (c)) adds a presumption, that "Unless the circumstances indicate otherwise, authentication is deemed to have been done with the intent to: (1) establish a person's identity; (2) establish that person's adoption or acceptance of the authenticated

record, term, or contract; and (3) confirm the content of the record or term as of the time of the authentication.

Such a presumption can create a trap for the unwary. To limit its effect, I advise clients include a routine disclaimer with their e-mail, such as “Nothing in this message should be interpreted as a digital or electronic signature that can be used to authenticate a contract or other legal document.” Unfortunately, not everyone consults counsel for advice on how to send e-mail.

UETA uses the words “electronic signature" instead of “authenticate.” In section 102(8), it defines an electronic signature as an “electronic sound, symbol or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.”

In contrast with UCITA, UETA does not create a presumption for electronic signatures. Instead of creating a new rule, it refers back to existing signature rules in section 108(b). “The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties’ agreement, if any, and otherwise as provided by law.”

I think UETA’s approach is preferable. Let the underlying rules be the same for ink signatures and electronic ones.

2. What about consumer-protective rules that require written agreement to some terms?

Several consumer protection laws have required that specific terms be signed by a consumer. The policy underlying these laws is to reduce the probability of unfair practices. This requirement goes beyond simple conspicuousness by ensuring that by the consumer not only actually sees the term but also sees that it has been specially brought to the consumer's attention. Neither UCITA nor UETA attempt to preserve the policy underlying this signature requirement.

Here is UCITA 105 (d) “Except as otherwise provided in subsection (e), if this article conflicts with a consumer protection statute or regulation of this State in effect on the effective date of this article, the conflicting statute or regulation prevails.”

UCITA 105 (e) “If a law of this State in effect on the effective date of this article applies to a transaction governed by this article, the following rules apply: (1) A requirement that a term, waiver, notice, or disclaimer be in a writing is satisfied by a record. (2) A requirement that a writing or a term be signed is satisfied by an authentication. (3) A requirement that a term be conspicuous or the like is satisfied by a term that is conspicuous in accordance with this article. (4) A requirement of consent or agreement to a term is satisfied by an action that manifests assent to a term in accordance with this article.”

UCITA explicitly overrides the signature requirements of state consumer protection laws. Additionally, terms can be “conspicuous” under UCITA even though they (and the rest of the contract) cannot be seen by the customer until after the customer pays for the product and takes it away.

UETA (section 106) is not so precise as UCITA, but it probably has the same effect.

It would be helpful to have comments in UCITA and UETA instructing courts to be sensitive to the consumer protection policy underlying a signature requirement. A court should listen sympathetically to the argument that an electronic signature was not obtained under circumstances that could be reasonably expected to provide comparable notice to the consumer as those involved in the written signature. This should be a proper basis for a finding of unconscionability.

3. Fraudulent electronic signature?

What happens if someone pretends to be you and enters into contracts in your name?

Under UCITA section 116, your liability can be unlimited if you use a security procedure (such as a digital signature) and a criminal gains access to the method that you use for identification.

For example, consider a digital signature system. You would obtain two encryption keys from a Certificate Authority. One of the keys is a “private key” which you keep private. The other is the public

key, which everyone has access to. You can "sign" a document by encrypting all or part of it with your private key. Only your public key can decrypt this message. If someone sends me an encrypted message and I can decrypt it (make it intelligible to a human) with your public key, then the message was almost certainly encrypted with your private key.

Suppose that someone gains access to your private key without your knowledge. There are several ways that this can happen in the normal course of business. Here are a few examples:

- Your disk drive is scanned when you report a defect electronically or register your software electronically.
- Your drive is copied by your maintenance staff or by a computer repair technician.
- Your drive is copied to a remote web site that takes advantage of the latest security flaw in your internet browser.
- A virus or other program that you installed on your computer contains a scanner that tracks what you type on your keyboard. It captures the password that you use to access your encryption key file and sends your file and password to a remote site.

This person now impersonates you, orders merchandise in your name, signs electronic purchase orders in your name, and has the merchandise delivered electronically or to a postbox. Your risk is unlimited.

First consider the case in which the criminal impersonates you in a transaction with someone with whom you already do business using your digital signature. Under UCITA 116(c), if an attribution procedure exists between the parties with respect to the electronic record, and (116(c)(2)) if the parties agree to, or otherwise adopt an attribution procedure to verify the person from which an electronic record comes, the record is attributable to the person identified by the procedure, if the party relying on that attribution satisfies the burden of establishing that (116(c)(2)(iii)) the attribution procedure indicated that the electronic record was that of the person to which attribution is sought.

If your encryption key is used, the requirement of 116(c)(2)(iii) is satisfied and you are liable.

UCITA allows you to escape liability if you can prove, under 116(c)(3), "that the electronic record was not caused directly or indirectly by a person: (i) entrusted at any time with the right or duty to act for the person with respect to such electronic records or attribution procedure; (ii) who obtained access to transmitting facilities of the person; or (iii) who obtained, from a source controlled by the person, information facilitating breach of the attribution procedure."

To fit within UCITA's savings clause, you will first have to find out who used your key and how they obtained it. Otherwise, you won't be able to prove that the criminal did *not* obtain the key in one of the listed ways. If the crime is unsolved, you lose. Having jumped through this hoop, you next have to prove that the criminal never obtained access to your transmitting facilities—but I think that the thief obtained access to your facilities in all of the examples that I mentioned above.

Next, consider the case in which the criminal impersonates you in a transaction with a new vendor. Under UCITA 116(e), you are still liable if you "failed to exercise reasonable care." UCITA lays out no standards for "reasonable care." What standards are the courts going to apply? How much knowledge of electronic security procedures will be imputed to consumers and small businesspeople?

In contrast, UETA makes no presumptions. Section 108 says that "An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be proved in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable." This looks better than UCITA, but we would be better served by regulations that impose a significant portion of the risk on the business entities who specified which security procedures will be used in the first place.

The risk of loss provides a significant incentive to create better security procedures, but this has to be applied to the people who have the power to create or specify use of those procedures. Laws that shift risks to consumers create moral hazards for sellers and security system providers. We should either limit consumer liability or provide consumers with a wider range of options for increasing their own security. For additional discussion and recommendations, see Jane Kaufman Winn & Carl Ellison "Regulating the Use of Electronic Authentication Procedures by US Consumers in the Global Electronic Marketplace" at

www.ftc.gov/bcp/icpw/comments/revwin~1.htm and Cem Kaner, “The Insecurity of the Digital Signature,” at www.badsoftware.com/digsig.htm.

4. Is the customer entitled to a copy of an agreement?

One of the remarkable debates in the Article 2B/UCITA meetings concerned the customer’s right to keep a copy of a contract that she had just entered into. The most recent example of this debate came in the drafting committee meeting on February 26-28, 1999. One of the software publishers’ lobbyists argued emphatically that it should be enough to show the customer the contract once, and that the publisher should not be required to allow the customer to print or download the contract.

Despite repeated discussion of the issue over the past three years, there is no requirement in UCITA that a customer be allowed to print or download a contract that she has supposedly “agreed” to.

There is such a requirement in section 107 of UETA. For example, in 107(c), “An electronic record may not be sent, communicated or transmitted by an information processing system that inhibits the ability to print or download the information in the electronic record.” And in 107(d), “The effect of this section may not be varied by agreement..”

5. What rules apply to receipt of legal notices?

UCITA 102(b)(40) (II) defines "Receive” to mean “in the case of an electronic notification, to come into existence in an information processing system in a form capable of being processed by or perceived from a system of that type, if the recipient uses, or otherwise has designated or holds out that system as a place for receipt of such notices.”

First, suppose that your e-mail address is yourname@aol.com. And suppose that when you purchased software over the web, your nonnegotiable, visible-only-after-the-sale click-wrap contract specified in the fine print that all legal notices could be sent to you by e-mail to yourname@aol.com.

- A message sent to you is deemed to have been received by you as soon as it hits aol.com. If you don’t make a practice of regularly checking your e-mail (as many, many users don’t), then this notice may well have its effect long before you become aware of it.
- A message sent to you is deemed to have been received by you as soon as it hits aol.com even if it is subsequently lost by AOL or lost during transmission to you or deleted by standard spam-filtering software it at your machine without you ever seeing it because the message looks so much like unsolicited commercial e-mail.

Next, suppose that the click-wrap contract specifies that legal notices can be sent to you by e-mail to yourname@vendor.com, where vendor.com is a system controlled by the vendor. You might not even realize that you have to log onto the vendor’s e-mail system to retrieve mail intended for you.

Next, suppose that the contract specifies that notices will be published on the vendor’s web site. This satisfies the literal definition in UCITA and this example was raised in detail in a brief by the Motion Picture Association a year ago, without causing a narrowing or refining of the definition. In this case, you have to check the vendor's web site for notices. If this doesn’t sound oppressive, think about the person or company who has downloaded images, software, or published information content from a few hundred web sites. Imagine having to check for legal notices at a few hundred web sites every few days.

I provide several other examples in a letter to the Federal Trade Commission, at www.ftc.gov/bcp/icpw/comments/kaner.htm.

UETA 114 (b) has similar problems: “Unless otherwise agreed between the sender and the recipient, an electronic record is received when it enters an information processing system (1) that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent; (2) in a form capable of being processed by that system; and (3) from which the recipient is able to retrieve the electronic record.”

At least in UETA, there is the requirement that the recipient be able to retrieve the record.

Because many people do not check e-mail with the same regularity that they check physical mail, we are pushing the law ahead of practice with these provisions.

Additionally, because there are many ways for mail to be lost between receipt at an internet service provider (such as AOL) and your local computer's in-box, we are subjecting you to a random risk that you will be deemed to have received a message that you have never seen. This is within the definition of receipt. Unlike the mailbox rule, the fact that you never actually received the message is not a defense.

I urge NCCUSL to recognize that society is not as far down the technology curve as the computer law hotshots among us. For now, let us adopt a rule that (at least for mass-market transactions) says that a message is electronically received when a recipient acknowledges having received it. If someone wants to take advantage of a mailbox rule, they can use traditional mail instead. We can create an electronic variation of the mailbox rule in a few years, when technology and social practices stabilize.

6. Mistakes made by the customer?

The web is an unfamiliar medium and people make a lot of mistakes using it.

Dr. Jakob Nielsen, one of the world's most influential experts on web site usability, gave a keynote address at the 12th International Software Quality Week on May 28, 1999. Dr. Nielsen pointed out that in his research, only about 20% of internet users were able to successfully fill out and submit a web-based form and that in a "study of 15 large commercial sites users could only find information 42% of the time even though they were taken to the correct home page before they were given the test tasks." (Quoted from Jakob Nielsen's *Failure of Corporate Websites,/www.useit.com/alertbox/981018.html.* See also Jared Spool et al., *Web Site Usability : A Designer's Guide*, Academic Press / Morgan Kaufmann, 1998.)

UCITA section 2B-118 provides a defense only to consumers if the consumer made an error when interacting with an information system that did not provide a "reasonable method to detect and correct or avoid the error."

Why is this defense available only to consumers? People will make these mistakes whether they are acting as consumers, professionals (such as lawyers or teachers), or businesses.

UETA section 109(2) provides the defense to all individuals but only when interacting with a system that "did not provide an opportunity for the prevention or correction of the error." Note that the opportunity need only exist under UETA, whereas under UCITA it must also be a reasonable opportunity.

The error defense should be available to all parties who interact with an information system that does not provide a reasonable method to detect and correct or avoid the error.

7. Choice of law and forum?

UCITA sections 107 and 108 give the vendor the power to choose the applicable law and forum. I say that this is vendor's choice because in a mass-market or consumer transaction, the terms are non-negotiable and these particular terms can be presented inconspicuously and after the sale.

The often repeated justification for including such clauses in UCITA is that they are essential for electronic commerce. It is instructive that such terms are not included in UETA.

The rules governing choice of law and forum belong in Article 1, not UCITA.

Closing notes

UCITA is controversial. It is supported by software publishers and computer manufacturers (who will be able to opt their contracts into UCITA) and opposed by (among many others) software developers (several professional societies have expressed opposition to UCITA and none have expressed support for it), consumers, large business customers, librarians, and most other copyright industries (including trade associations and professional societies representing broadcasters, motion picture studios, music publishers, newspaper and magazine publishers, photographers, the recording industry, cable television, and writers).

In contrast, UETA is much less controversial.

I attended almost all of the Article 2B (UCITA) drafting committee meetings and a few of the UETA meetings. A colleague who is co-authoring an engineering text with me attended several other UETA meetings and we discussed them in detail. Based on this experience, I can say that the e-commerce provisions in UETA were much more carefully scrutinized that UCITA's. In the differences noted above (and in the many other e-commerce differences between UETA and UCITA), I don't see any reason in principle for the two laws to differ.

The Article 2 drafting committee decided to conform itself to the UETA. I think that UCITA should do the same.