Texas Wesleyan Law Review

Volume 11 | Issue 2 Article 20

3-1-2005

The Boundaries of Contract In A Global Economy; Cyberspace Contracting: Embracing Incomplete Contract Paradigm in the Wake of UCITA Experience

Saby Ghoshray

DOI: https://doi.org/10.37419/TWLR.V11.I2.19

THE BOUNDARIES OF CONTRACT IN A GLOBAL ECONOMY

CYBERSPACE CONTRACTING: EMBRACING INCOMPLETE CONTRACT PARADIGM IN THE WAKE OF UCITA EXPERIENCE

Saby Ghoshray†

I. INTRODUCTION

As we bask in the unprecedented advancement of the digital age, while seated at the precipice of a new millennium, we cannot but ponder over the legal ramifications of the burgeoning e-commerce that has become the norm rather than the exception. Like ancient times, commerce is facilitated by merchant agreements and contracts, and our very dear cyberspace is no exception. Traditional contracts are formed in real space involving live entities. On the other hand, in cyberspace contracts are formed via unknown, unseen players interacting in an environment cloaked under non-recognition. The last decade has seen a sudden explosion of commercial transactions involving automated agents. These transactions or business activities are being

† Dr. Saby Ghoshray is currently the Vice-President of Business Development and Compliance for the WorldCompliance Company and continues to publish and research in International Law and Corporate Governance issues. The present Article grew from the Author's presentation at the Common Law of Contracts Conference in Gloucester in June 2004. The Author wants to thank the speakers at the Conference who provided much food for thought, the Texas Wesleyan University School of Law for organizing the event, and the Texas Wesleyan Law Review for the invitation to participate.

consummated in cyberspace or in the Internet medium at transaction speeds much faster than the traditional pace of business. These business transactions, or "cyberspace contracting,"[1] are however, being guided by the existing legal framework or contracting paradigm designed for real space. As a result, the established concepts of commercial contracts are being challenged to a point hitherto unseen. These challenges primarily emerge from issues involving (i) overlapping jurisdiction,[2] (ii) complexity in enforcement, and (iii) lack of a robust legal framework,[3] among others.

On the flipside of the coin, the last decade alone has seen a maturation/evolution in "information law."[4] This information law has started to take shape as both legal scholars and practitioners more often draw guidance from existing models and statutes to develop a newer legal framework. This has generated a plethora of loopholes and unresolved conflicts leading to undesired situations.[5] Suppose for a mo-

1. In this Article, I am making a distinction between real space contracting and cyberspace contracting. This is because the laws in general are developed for a world where it is jurisdictionally segmented via both political and geographical barriers. However, advancement in computer networking and digital technology has made distance and political borders invisible to the users linked in a vast continuum in which business is being transacted. This virtual electronic space is termed as "cyberspace." To further business interests in this virtual space, entities forge contractual arrangements having legal consequences and this is going to be termed as "cyberspace contracting."

2. The idea of overlapping jurisdiction comes from the fact that all the actors involved in an Internet transaction have real-world existence, and thus are located in one or more legal jurisdictions. The digital equipment for networking and for computing transactions and for record keeping is also located in legal jurisdictions. However, it may become difficult to identify precisely which equipment was used when trying to assess *liquidated damage* if a particular case warrants. Similarly, if we are faced with a dispute or wrongdoing in the formation or consummation of a contract, the issues of the applicable law and the jurisdiction thereof might become difficult to determine. For more information on this issue, read CHRIS REED, INTERNET LAW: TEXT AND MATERIALS (2000).

3. As we will show in this article, the existing legal framework, such as, the traditional common law of contracts, and its more advanced variants, such as Article 2B of the Uniform Commercial Code, UNICITRAL Model Law, or electronic commerce, etc. have either ambiguity or weakness in dealing with the identification of a legal regime under which disputes can be addressed, or liquidated damages can be assessed. For further insight see Anne Wells Branscomb, *Jurisdictional Quandaries for Global Computer Networks*, *in* GLOBAL NETWORKS: COMPUTERS AND INTERNATIONAL COMMUNICATION 83, 92 (Linda M. Harasim ed., 1993). *See also* Dan L. Burk, *Application of United States Patent Law to Commercial Activity in Outer-Space*, 6 SANTA CLARA COMP. & HIGH TECH. L.J. 295, 316–17 (1991). The Model Law is *available at* http://www.uncitral.org/english/texts/electcom/ecommerceindex.htm (last visited Jan. 28, 2005) (on file with the Texas Wesleyan Law Review).

4. *See* Nicholas P. Miller & Carol S. Blumenthal, *Intellectual Property Issues*, *in* TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS 227, 227–28 (Anne W. Branscomb ed., 1986).

5. The unresolved conflicts and undesired situations have emerged due to the confusion as to which law applies to particular types of contracts and how the various competing legal regimes have attempted to influence judgment. *See* Mathew Burnstein, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J.

ment, a consumer orders cutlery knives from a vendor on the Internet, and after reviewing the online catalogue learns the seller's place of business is Azerbaijan. Upon receiving the shipment, the customer, to her dismay, finds the knives to be of inferior quality. As she e-mails the company for a refund on returning the product, she finds the vendor to be uncooperative. Upon further examination, the consumer realizes that although the place of business is listed in the former Soviet Republic, the products actually come from China, and the financial transaction was processed via a bank in the Cayman Islands. Ultimately, the customer is unhappy and begins exploring her options for remedy. Here, we are confronted with issues ranging from the enforceability of a contract under the law of the jurisdiction to the limit of the liquidated damage. Let us analyze this a little further. First and foremost, does ordering from the catalog create a contract, even though no intermediate confirmation took place? By clicking the mouse, does the customer become party to an enforceable contract? Because the parties involved in this transaction physically reside in two distinct geographical regions and are possibly governed by two different legal regimes, under what law and to what extent can the offending party be held liable for damages? And more importantly, a breach in one regime may not be the same in another regime, so how will any damages be assessed? The questions are plenty, confusions are abundant, and the search for answers becomes lost in the murky world of cyberspace contract regime, or the lack thereof. We will begin our dissection on these very issues by first discussing jurisdiction law and enforcement mechanisms. We need to understand the two existing modalities of contract enforcement, namely public enforcement of contracts, mainly through the court system, and private enforcement of contracts, the majority through the reputational mechanism.

II. JURISDICTION AND ENFORCEMENT

As transactional activity proliferates in the digital domain, contractual disputes become increasingly difficult to adjudicate. This is in

TRANSNAT'L L. 75, 83–87 (1996). In this context, several recent cases have only enhanced the confusion regarding jurisdictional issues. *See* CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1263 (6th Cir.) (holding that a Texan who entered a shareware agreement with CompuServe had sufficient contacts with Ohio, CompuServe's location, to establish personal jurisdiction). The court noted that the Texan entered an online agreement with CompuServe that had an Ohio choice of law provision and subsequently posted this program on a CompuServe server in Ohio via a local Texas access number. *See id.* at 1260–61; *see also* Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996); Maritz, Inc. v. Cybergold, 947 F. Supp. 1328 (E.D. Mo. 1996) (lowering the minimum contacts threshold by finding that advertising on the Internet constitutes sufficient contact with foreign states for the purpose of establishing jurisdiction, even if the advertiser is not making an effort to target specifically in that forum).

part driven by the ambiguity in identifying the jurisdiction in which to proceed and in part engineered by the difficulty in enforcement. Because cyberspace has no geographical boundaries,[6] identifying a jurisdiction to prosecute or selecting the law to apply will continue to be a daunting task, unless and until a universal legal regime is developed and all members of cyberspace agree to abide by it. Perhaps a look at the utility of digital commerce will further drive home the reality that cyberspace business transactions are here to stay, and not just to stay, but rather to flourish. Because physical distance is no longer an issue, purchasing goods from the other side of the world is functionally equivalent to purchasing them from a neighbor. When the commodity involves information goods and services, this purchase or transaction becomes even easier via online. This ease of transport and mode of information flow to facilitate it has made transactions by private individuals, spanned across disparate and disjointed geographical regions, very possible in cyberspace.[7]

Because public enforcement of contracts between parties can take place through the court system, enforcement is more difficult across multiple jurisdictions than in a single jurisdiction.[8] This is due to the artificial barriers created via cultural norms, languages, mutual trust, and last but not least, the cost involved in such operations. Moreover, as the physical lines of separation get overlapped, so do the limits of jurisdiction, as the authorities find it extremely difficult to identify what law the contracts are likely to fall under. As a result, public enforcement becomes very difficult. This leads us to believe that this will be a less viable method of law enforcement in the future.[9]

The advancement of technology in e-commerce has become a primary driving force for the proliferation of e-commerce. The technological marvels of public key encryption[10] make available a bigger,

6. For further discussion on this issue of jurisdictional quandary, see W. Scott Petty, *Which Court Has Jurisdiction Over Cyberspace?*, CYBERSPACE LAW., Jan. 1997, at 8.

7. For more information on this, see David Friedman, *A World of Strong Privacy: Promises and Perils of Encryption*, 13 SOC. PHIL. & POL'Y 212 (1996), *available at* http://www.davidfriedman.com/Academic/Strong_Privacy/Strong_Privacy.html (last visited Jan. 28, 2005) (on file with the Texas Wesleyan Law Review).

8. *See* REED, *supra* note 2.

9. For a detailed discussion on these issues, see Friedman, *supra* note 7.

10. A cryptographic system that uses two keys refers to a *public key* known to everyone and a *private* or *secret key* known only to the recipient of the message. When John Doe wants to send a secure message to Jane Doe, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key. Public key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet. They are extremely secure and relatively simple to use. The only difficulty with public key systems is that you need to know the recipient's public

more secure virtual world to people who can transact anonymously. This is made possible again due to technological advancement in which people are referenced by a very different identity than their real space counterpart. This cyberspace identity does not encroach in real space, thus it does not affect real-life reputation, making it easier for most people to transact.[11] This comfort of privacy draws more and more people to online activities on a daily basis, and is really the driving force behind the explosion in e-commerce activities.[12] How can we therefore sue someone, when we do not know who she is or on what continent she lives? In this context, public enforcement of contracts becomes not only difficult but also rather irrelevant.

If public enforcement of contracts is so difficult to achieve, does private enforcement have any chance to succeed? This depends on how we view the impact of reputational risk in real life because if the reputational mechanism becomes the primary driver for private enforcement of contract in cyberspace, then only enforcement will succeed. Let us examine the case of using the Better Business Bureau to control the behavior of local merchants. Suppose a local store in the neighborhood has cheated some of its customers by providing inferior product and refusing to exchange merchandise even though it promised to do so. Repeated complaints to the Better Business Bureau in this case can put a dent into the reputation of this business to the point of eventually losing some of its customers. In the absence of any other regulatory mechanism, it is this fear of losing reputation that sometimes ensures that the business stays honest. How does this scenario translate into online commercial activities? Let us take the example of *eBay*, a very successful online auction site, to illustrate the point. Whenever a seller or a buyer wants to complete the transaction that he or she may have won via the auction process, the individual has the capability to review the reputation of the counter-party. The *eBay* software allows its legitimate user to view from its database comments about other users. These comments are available, both in summary form and in text, to anyone bidding in an auction with that seller.[13] This is done by incrementally aggregating reputation of all

key to encrypt a message for him or her. What is needed, therefore, is a global registry of public keys, which is one of the promises of the new LDAP technology. Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. For this reason, it is sometimes called *Diffie-Hellman Encryption.* It is also called *asymmetric encryption* because it uses two keys instead of one key (*symmetric encryption*).

11. *See* Violina P. Rindova & Suresh Kotha, *Building Reputation on the Internet: Lessons from Amazon.com and Its Competitors* (revised Sept. 1999), *available at* http://us.badm.washington.edu/kotha/personal/pdf%20files/amr_final.pdf (last visited Jan. 25, 2005) (on file with the Texas Wesleyan Law Review).

12. *See* David Friedman, *Contracts in Cyberspace* (May 4, 2000), *available at* http://www.best.com/~ddfr (last visited Jan. 26, 2005) (on file with the Texas Wesleyan Law Review).

13. *See* http://www.ebay.com (last visited Jan. 23, 2005); *see also* Joseph O. Patterson, *A Matter of Trust: Reputation Management in Peer-to-Peer Networks*, *at* http://

eBay users by allowing each user to post comments on his or her counter-parties on a range of issues such as if the goods lived up to their description, if they were delivered promptly, and whether the buyer followed through with her commitment to complete the purchase.

Now the question comes to mind, is this a foolproof mechanism for private enforcement of a cyberspace contract? The answer depends on how much an individual's future activity can be predicted from his past behavior, as well as how much the individual's commercial activity depends on his online reputation. Reputational enforcement can work only if there is a cost attached to the person who engages in illicit behavior online.[14] For example, if someone is looking for a one-shot deal to retire, she can cheat her counter-party out of a huge sum and never again surface in cyberspace. Clearly, this person is not going to do more business online any time soon. Where is the enforcement now? How does the injured party proceed to recover his damages? Under which jurisdiction and under what law will the adjudication of guilt or innocence be given, and are there any consequential liquidated damages to be collected? So, we are back to the issue of public enforcement and the jurisdictional quagmire again.

III. CONTRACT FORMATION

Under the traditional view of contract law, formation of a contract requires at a minimum, the willingness of two parties to be bound by the terms of their agreement.[15] Contract formation consists of the dis-

csci.mrs.umn.edu/Personal/pub/Patterson/SeminarIIPaperDevelopment/sem2_draft.doc (last visited Jan. 28, 2005) (on file with the Texas Wesleyan Law Review).

14. *See* Stephen J. Choi, *Gatekeepers and the Internet: Rethinking the Regulation of Small Business Capital Formation*, 2 J. SMALL & EMERGING BUS. L. 27, 54 (1998).

15. Contracts are promises that the law will enforce. The law provides remedies if a promise is breached and recognizes the performance of a promise as a duty. Contracts arise when a duty does or may come into existence because of a promise made by one of the parties. To be legally binding as a contract, a promise must be exchanged for adequate consideration. Adequate consideration is a benefit or detriment which a party receives which reasonably and fairly induces them to make the promise/contract. For example, promises that are purely gifts are not considered enforceable because the personal satisfaction the grantor of the promise may receive from the act of giving is normally not considered adequate consideration. Certain promises that are not considered contracts may, in limited circumstances, be enforced if one party has relied to his detriment on the assurances of the other party. Contracts are mainly governed by state statutory, common (judge-made) law, and private law. Private law principally includes the terms of the agreement between the parties who are exchanging promises. This private law may override many of the rules otherwise established by state law. Statutory law may require some contracts be put in writing and executed with particular formalities. Otherwise, the parties may enter into a binding agreement without signing a formal written document. *See* RESTATEMENT (SECOND) OF CONTRACTS § 110 (1981). Most of the principles of the common law of contracts are outlined in the Restatement of The Law of Contracts published by the American Law Institute. *See* RESTATEMENT (SECOND) OF CONTRACTS (1981). The Uniform Commercial Code, whose original Articles have been adopted in nearly

tinct steps of presentation of an offer, and acceptance of the same. A contract is concluded when an offer is accepted. According to the Restatement (Second) of Contracts,[16] an offer is defined as, "the manifestation of willingness to enter into a bargain, so made as to justify another person in understanding that his assent to that bargain is invited and will conclude it."[17] In that sense, the offer is a statement by one party of his or her willingness to enter into a contract on stated terms, provided these terms are accepted by the party to whom the offer is addressed. However, the common law of contracts and contract law regimes in Europe sometimes bring in an added layer in the process of contract formation. An invitation to treat is simply an expression of willingness to enter into negotiations with an implicit desire to conclude the contract at a later time.[18] In this context, there is a fine line of distinction between the "offer" and the "invitation to treat" in such a way that the thin line revolves around the concept of intention. Simply stated, an invitation to treat is preceded by an offer. In this context, the traditional common law maintains that the display of goods constitutes an invitation to treat, and the offer is constituted when the customer presents the goods at the cash register.[19] This dichotomy between "invitation to treat" and "offer" can be a lethal bone of contention in e-commerce transactions or in cyberspace contracting, as will be evident in the following scenario.

---

every state, represents a body of statutory law that governs important categories of contracts. The main Articles that deal with the law of contracts are Article 1 (General Provisions), U.C.C. art. 1 (2004), and Article 2 (Sales), U.C.C. art. 2 (2004). Sections of Article 9 (Secured Transactions), U.C.C. art. 9 (2004), govern contracts assigning the rights to payment in security interest agreements. Contracts related to particular activities or business sectors may be highly regulated by state and/or federal law. *See* Cornell University Law School, Legal Information Institute, *Contracts: An Overview* ("In 1988, the United States joined the United Nations Convention on Contracts for the International Sale of Goods which now governs contracts within its scope."), *at* http://www.law.cornell.edu/topics/contracts.html (last visited Jan. 23, 2005) (on file with the Texas Wesleyan Law Review).

16. *See* RESTATEMENT (SECOND) OF CONTRACTS § 24 (1981).

17. The fundamental elements of the contractual bargaining process are the existence of an offer and the corresponding acceptance of that offer. These elements are not always easily identifiable as counter offers, cross offers, mere invitations to treat, and the like, and these are just some of the potential hindrances to an enforceable contract.

18. Much of the argument supporting the "invitation to treat" viewpoint evolved in the famous English case of *Grainger & Son v. Gough*, (1896) A.C. 325 (H.L.), and some of its predecessors, such as *Payne v. Cave*, 100 Eng. Rep. 502 (K.B. 1789) and *Harris v. Nickerson*, [1872–1873] 8 L.R.-Q.B. 286 (1873). These cases have set a number of variants on an invitation to treat, such as, pre-contractual negotiations, shop-display, and advertisement.

19. Some U.S. courts have decided that taking the goods off of the shelves is an acceptance of the shops offer to sell even though the customer could cancel his acceptance before payment if he wished. *See* Lasky v. Econ. Grocery Stores, 65 N.E.2d 305, 306 (Mass. 1946); Sheeskin v. Giant Food, Inc., 318 A.2d 874, 882–83 (Md. Ct. Spec. App. 1974).

A. *Flying on the Cheap*

Passengers could not imagine such a deal. In 2002, United Airlines was advertising a round-trip ticket from its Chicago hub to big city Bombay, India for a mere $99. This was the deal of a lifetime for many people who had found the typical $1000 or more tickets unaffordable. By the time word spread of this jackpot of a flying deal, over 50 people had booked tickets. And, just as tickets were being bought by the fortunate few, United Airlines realized there had been a printing error on its advertisement. The original advertisement for the trip to India was to be printed at $990. This was a bargain still, according to United Airlines, given that tickets from Chicago to India can run as high as $1500. Nonetheless, the jackpot was brought to a halt as United Airlines fixed their printing mistake and redistributed the advertisement for their intended $990 dollar price. Surprisingly, United Airlines kept the passengers happy by honoring the deal, although it resulted in a financial loss the company had to shoulder.

This case points to the confusion that can occur between an invitation to treat and an offer of acceptance.

B. *Channel Surfer's Delight*

The many couch potatoes that love to sit and watch television were amazed at the great price being offered by the Argos Grocery chain for purchase of a new color television. The internet advertisement promised a color television for the low-low price of £2.99—a great deal. Sure enough, a few hundred people placed orders via the internet for the new television. However, a problem soon arose because Argos did not honor the deal that was printed in the web advertisement. Their position was that the intended price for the television was for £299.[20] This was a significant difference from the price the consumers had expected to pay. This case did not end so happily as the United Airlines case, as it was ultimately settled out of court, and highlighted the company's position that this was an invitation to treat but not presentation. They also argued the customers must go through a validating process.[21]

These two cases highlight the problems in contract formation in cyberspace or potential pitfalls that can crop up as a result of not un-

20. Joshua Rozenberg, BBC, *Business: The Economy Argos—An Invitation to 'Treat,' available at* http://news.bbc.co.uk/1/hi/business/the_economy/441740.stm (last visited Jan. 23, 2005) (on file with the Texas Wesleyan Law Review).

21. "A proposal to supply goods or services at stated prices made by a professional supplier in a public advertisement or a catalogue, or by a display of goods, is presumed to be an offer to sell or supply at that price until the stock of goods, or the supplier's capacity to supply the service, is exhausted." The Commission on European Contract Law, *The Principles of European Contract Law*, art. 2.201(3) (1998), *available at* http://www.jus.uio.no/Im/eu.contract.principles.1998/doc.html#29 (last visited Mar. 4, 2005) (on file with the Texas Wesleyan Law Review).

derstanding the contract framework in cyberspace. In the framework of common law, an acceptance can be considered as an *absolute and unqualified* communication of informed consent to the terms proposed by the offeror. According to the Restatement (Second) of Contracts, a party can accept an offer in "any manner and by any medium reasonable under the circumstances." The original offer becomes null and void when a counter-offer is presented such that the terms of this offer deviate in form from that in the original offer.

In cyberspace contracting, the offer and acceptance are generally communicated via e-mails. It becomes more complicated when automated agents negotiate the contracts.

IV. PROBLEMS WITH ELECTRONIC AGENTS

The traditional contracts paradigm gets its most difficult test when electronic agents facilitate cyberspace contracting.[22] Use of electronic agents or automated means of contract negotiation or consummation is a recent phenomenon, more famously brought to light by *eBay v. Bidders' Edge, Inc.*[23] When a computer program or other digitally created automated entity is distributed in cyberspace for the sole purpose of exchanging information and negotiating agreements without review by an individual, the limits of contract law become exposed because traditional contract law is posited on the assumption that human cognition will be guiding the intentions required in the procedures, such as making an offer and accepting or rejecting that offer. When electronic agents are introduced into the fray, human cognitions and discretionary aspects are no longer guiding the core procedures required to conclude a valid contract. In the absence of such premise, a contract, if formed, becomes grounded on shaky fundamentals because the framework for contract formation is governed by the human characteristics of choice and obligation. That is, given a set of choices, an individual is able to decide a course of action of his or her own volition. This course of action could range from accepting a given offer to presenting a counter-offer, thereby negating the previous offer. Once an action engineered by human volition is consummated, the said individual can be held liable for events transpired, or actions gen-

22. *See* U.C.C. § 2B-102 (Draft, Aug. 1, 1998), University of Pennsylvania Law School, *at* http://www.law.upenn.edu/bll/ulc/ucc2b/2b898.pdf (last visited Jan. 28, 2005) (on file with the Texas Wesleyan Law Review). Article 2B defines "electronic agent" as "a computer program or other automated means used by a person to independently initiate or respond to electronic messages or performances on behalf of that person without review by an individual." *Id.* Such contracts would be enforceable "if the interaction results in the electronic agents' engaging in operations that confirm or indicate the existence of a contract." *Id.* § 2B-204(1). This rule would apply "even if no individual was aware of or reviewed the agent's actions or their results." *Id.* § 2B-204(4).

23. 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

erated, because these actions or events can be directly connected to the volition discussed earlier.

If we bring in the so-called intelligent machines or automated agents into the fray to initiate, negotiate, and consummate a contract, we are taking away the ingredients of human cognition, volition, and choice from the whole process. This presents a fundamental challenge in the way contract law is to be interpreted and applied. This is where the problem of attribution and authority in cyberspace contracting comes to the purview because contracting via electronic agents may mimic the form inherent in real space, and cyberspace contracting falls short in providing a substantive base.

V. Is The Current Contract Framework Adequate?

When traditional contract law seems to be at its wits end, Article 2B[24] of the Uniform Commercial Code (U.C.C.) is widely believed to provide model rules to govern transactions in the digital domain. For example, Article 2B helps in defining rules to govern electronic contracting and tries to bolster the fact that a contract in electronic form neither reduces its validity nor its enforceability. However, since the draft version of Article 2B was published in 1998, it has met with widespread criticism because of its inadequacy to handle complex issues emanating from cyberspace contracting. As a result, the contract law community joined hands with information law specialists to develop the draft version of the Uniform Computer Information Transaction Act (UCITA). UCITA is envisioned to be the all-encompassing comprehensive statute, covering a myriad of issues

24. The Preface to Article 2B begins with the following epigraph:

> The UCC has given parties in traditional sales of goods a well-understood legal framework to establish contract formation, terms, and enforcement rights. It is timely now to adapt this framework to the digital era and to the new information products and services that will increasingly drive Global Electronic Commerce . . . . Article 2B can be a strong first step toward a common legal framework for digital information and software licenses.

U.C.C. art. 2B Preface (Discussion Draft, Aug. 1, 1998), University of Pennsylvania Law School, *at* http://www.law.upenn.edu/bll/ulc/ucc2b/2b898.pdf (last visited Jan. 28, 2005) (on file with the Texas Wesleyan Law Review) (quoting Letter from CSPP (a coalition of eleven major manufacturing companies) dated Nov. 19, 1997) (alteration in original); *see also* Raymond T. Nimmer, *UCC Revisions: Article 2 in the Information Age*, 416 PLI Patents Copyrights Trademarks & Literary Prop. Course Handbook Series 1005, 1007 ("Article 2 of the [U.C.C.] comprises the basic and most influential contract law of our country."). *See generally* U.C.C. art. 2 (1995) (providing a standard set of commercial law rules). Article 2 of the U.C.C. has promoted the growth of larger and more national markets for the manufacturing economy. *See* Fred H. Miller, *The Uniform Commercial Code: Will the Experiment Continue?*, 43 Mercer L. Rev. 799, 808 (1991) (noting the U.C.C.'s "substantive excellence" and discussing its success in promoting national uniformity). In doing so, Article 2 has been supplemented by Article 2A, which sets forth rules for leases of goods. *See generally* U.C.C. art. 2A (1990) (providing standardized rules for leases of goods).

ranging from contract formation to remedy for breach. UCITA adopts the fairly settled principles of contract law for the sale of goods under UCC Article 2 and embeds in it the concept of the purchase and sale of intangible computer information as a commodity. Thus, the issue before us is to analyze how equipped Article 2B is in authenticating or validating the "attribution" procedure.[25]

A. *Attribution in E-Commerce*

One of the problems involving electronic agents in cyberspace contracting is attributing actions to parties. Thus, attribution procedure has become a thorny issue in e-commerce,[26] because in cyberspace, transactions could take place either between an individual and an electronic agent acting on behalf of an individual, or between two electronic agents acting respectively on behalf of two individuals. The actions taken by these electronic agents have definite consequences. Therefore, it is very important to understand the attribution mechanism governing proper attribution of the electronic agents. In this regard, current contract law sanctions consensual arrangements concerning legally viable attribution procedures.[27] The widespread explosion of e-commerce and the resulting proliferation of cyberspace

25. In those jurisdictions where the Uniform Computer Information Transactions Act (UCITA) is in effect, "licenses" for access to electronic information are specifically characterized as contracts and the formation of such contracts are thus validated via click-wrap and click-through mechanisms. *See* UNIF. COMPUTER INFO. TRANSACTIONS ACT §§ 102(a)(41), 112 cmt. 2 (amended 2002), *available at* http://www.law.upenn.edu/bll/ulc/ulc.htm#ucita. UCITA has been adopted wholly or partly in Maryland and in Virginia. Iowa, North Carolina, and West Virginia have adopted anti-UCITA "bomb shelter" legislation, which denies enforcement of contracts governed by UCITA against residents of those states. Sections 208 and 209 of UCITA permit the formation of contracts using shrink-wrap and click-through mechanisms, including mechanisms that require assent and payment for access before all terms are disclosed to the offeree. *Id.* §§ 208, 209. Sections 112 and 113 require that the offeree has an "opportunity to review" and to reject post-assent contract terms before such terms can be enforced, but the "opportunity to review" need not do more than bring the terms to the attention of a reasonable person. *Id.* §§ 112, 113.

26. Section 102 of UCITA describes "attribution procedure" as a procedure used to identify the person who sent an electronic message or to verify the integrity of its content. *Id.* § 102(a)(5). In general, an attribution procedure has substantive effect only if it was agreed to or adopted by the parties or established by applicable law. Agreement to or adoption of a procedure may occur directly between the two parties or through a third party. For example, the operator of a system that includes information provided by third parties may arrange with database providers and customers for use of a particular attribution procedure. Those arrangements establish an attribution procedure between the customers and the database providers. An attribution procedure may also be established by two parties in the expectation that a third party may rely on it. For example, a digital signature may be issued to an individual pursuant to an agreement between the issuer and the individual, but then accepted or relied on by another party in a separate transaction. Use of the signature is an attribution procedure in that transaction. Similarly, a group of member companies may establish attribution procedures intended to bind members in dealing with one another. Such arrangements are attribution procedures under this Act. *See id.* §§ 108, 212, 213.

27. *See id.*

contracting has given rise to a slew of pertinent questions. For example, in the event of doing business between two parties, there has not been any prior established attribution procedure or reference to electronic agents conducting business. If a dispute arises, after it has been discounted that one party transacted business via electronic agents, can the legal principles of attribution govern the issue? Or, can agency law be properly applied to connect the electronic agent with the respective entity and thus the liability resulting from the action of the electronic agent be properly ascribed to the entity in question? Is contemporary contract law equipped to handle situations like this?

Even though UCITA[28] is designed to handle stress developed in traditional contract law due to the proliferation of cyberspace contracting, it is still considered inadequate to handle the legal ramifications resulting from the actions of electronic agents. This is an area that needs further exploration. A quick review of relevant law shows that it is intended to empower the electronic agents with the power to "manifest assent" on behalf of an entity.[29] In order to manifest assent, several conditions must be satisfied, and prime among them, is that the engaging entity must exercise an opportunity to review.[30]

Reviewing the "to manifest assent" requirements of UCITA, we find that the electronic agent must have either the knowledge of the record, or the opportunity to review the same. The law further stipulates that the electronic agent must engage in "affirmative conduct or

28. UCITA is the first uniform contract law designed to deal specifically with the new information economy. Transactions in computer information involve different expectations, different industry practices, and different policies from transactions in goods. For example, in a sale of goods, the buyer *owns* what it buys and has exclusive rights in that subject matter (e.g., the toaster that has been purchased). In contrast, someone that acquires a copy of computer information may or may not own that copy, but in any case rarely obtains all rights associated with the information. *See* DSC Communications Corp. v. Pulse Communications, Inc., 170 F.3d 1354, 1360–62 (Fed. Cir. 1999). What rights are acquired or withheld depends on what the contract says. This point only is implicit in Article 2 for goods such as books; UCITA makes it explicit for the information economy where, unlike in the case of a book, the contract (license) is the product. *See, e.g.*, Specht v. Netscape Communications Corp., 306 F.3d 17, 29 n.13 (2d Cir. 2002); S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081, 1083–84 (9th Cir. 1989).

29. According to Section 112 of UCITA:

> (a) [How persons manifests assent.] A person manifests assent to a record or term if the person, acting with knowledge of, or after having an opportunity to review the record or term or a copy of it: (1) authenticates the record or term with intent to adopt or accept it; or (2) intentionally engages in conduct or makes statements with reason to know that the other party or its electronic agent may infer from the conduct or statement that the person assents to the record or term. (b) [How electronic agent manifests assent] An electronic agent manifests assent to a record or term if, after having an opportunity to review it, the electronic agent: (1) authenticates the record or term; or (2) engages in operations that in the circumstances indicate acceptance of the record or term.

UNIF. COMPUTER INFO. TRANSACTIONS ACT § 112 (2002).

30. *See id.*

operations" that will eventually lead to the formation of acceptance. How does the electronic agent then satisfy the condition of exercising an opportunity to review for the manifestation of assent? How does an electronic agent review the record?

First and foremost, for an electronic agent[31] to be able to review records,[32] the said record must be made available to the electronic agent. For a review to be proper, it must "enable a reasonably configured electronic agent to react." This is a much harder threshold to overcome. For example, if the record in question contains terms describing provisions to pay damages in the event of default or any breach of contract, the electronic agent must be able to understand. This would mean the electronic agent must contain highly intelligent mechanisms to identify and understand such contractual provisions. What if the electronic agent in question is limited via programming and still agrees to the terms and conditions? This clearly makes the

---

31. According to UCITA:

> "Electronic agent" means a computer program, or electronic or other automated means, used independently to initiate an action, or to respond to electronic messages or performances, on the person's behalf without review or action by an individual at the time of the action or response to the message or performance.

Id. § 102(a)(27). This term refers to an automated means for making or performing contracts. The agent must act independently in a manner relevant to creating or performing a contract. Mere use of a telephone or e-mail system is not use of an electronic agent. The automated system must have been selected, programmed, or otherwise intentionally used for that purpose by the person that is bound by its operations. The legal relationship between the person and the electronic agent is not equivalent to common law agency since the "agent" is not a human being. However, parties that use electronic agents are ordinarily bound by the results of their operations.

32. Section 113 of UCITA defines "Opportunity to Review" as follows:

> (a) [Manner of availability generally.] A person has an opportunity to review a record or term only if it is made available in a manner that ought to call it to the attention of a reasonable person and permit review. (b) [Manner of availability by electronic agent.] An electronic agent has an opportunity to review a record or term only if it is made available in a manner that would enable a reasonably configured electronic agent to react to the record or term. (c) [When right of return required.] If a record or term is available for review only after a person becomes obligated to pay or begins its performance, the person has an opportunity to review only if it has a right to a return if it rejects the record. However, a right to a return is not required if: (1) the record proposes a modification of contract or provides particulars of performance under Section 305; or (2) the primary performance is other than delivery or acceptance of a copy, the agreement is not a mass-market transaction, and the parties at the time of contracting had reason to know that a record or term would be presented after performance, use, or access to the information began. (d) [Right of return created.] The right to a return under this section may arise by law or agreement. (e) [Agreement for future transactions.] The effect of this section may be modified by an agreement setting out standards applicable to future transactions between the parties.

Id. § 113.

case for ambiguity in the current framework for cyberspace contracting.

The above limitations become more prominent when dealing with "authentication"[33] within the context of manifesting assent by the engaging party. Additionally, the issue of "conspicuous"[34] signal provides another major conflict in trying to use the current modalities in this context for contract formation in cyberspace. In order to respond to "conspicuous messages," the automated setup must have highly sophisticated programming or electronic configuration that is able to discern implicit terms with consequences and eventually form acceptance. This again calls into question the confusion contract law can create in guiding electronic transactions leading to legitimate contract formation.

The discussion has so far centered around transactions involving electronic agents on both sides of the fence. What happens when an electronic agent and a human being are facing each other in a negotiation to form a contract? Here again the UCITA comes to our rescue. It is clearly stipulated that if the human identifies the counter-party to be an electronic agent, the onus is on the human in so much as to dissuade from actions that, according to the human, will trigger the

33. The term "authenticate" in UCITA has replaced "signature" and "signed." A similar change in terminology is made in U.C.C. § 9-102(a)(7) (1999). In this Act, the term "sign" has the meaning used in U.C.C. § 1-201 (1995), except that it is not limited to authenticating writing. The definition is technologically neutral. This makes clear that qualifying electronic systems fulfill former paper-based requirements. This is consistent with the policies of the federal Electronic Signatures in Global and National Commerce Act that preclude discrimination against electronic records and signatures solely because they are electronic in character. Any "signature" under other law is an authentication under this Act. In addition, authentication includes qualifying use of any identifier, such as a personal identification number (PIN) or a typed or otherwise signed name. It can include actions or sounds such as encryption, voice and biological identification, and other technologically enabled acts if done with proper intent. *See* Parma Tile Mosaic & Marble Co. v. Estate of Short, 663 N.E.2d 663, 635 (N.Y. 1996) (holding that the intent requirement was not met). There is no requirement under this Act that the authenticated record be retained by a party, but that requirement may exist under other law. An authentication may be on, logically associated with, or linked to the record. With digital technology, the analogy between signing a record electronically and signing a paper is not precise. "Logically associated" makes it clear that the association between an authentication and a record need not be physical in nature. However, the association must support the inference that the authenticating party intends to adopt or accept the associated or referenced record. "Referring to" or "linked to" captures the traditional concept of incorporating a record or term by reference, as well as use of an electronic connection, such as an Internet hyperlink. An "authentication" may express various intended effects. What effects are intended are determined by the context and objective indicia associated with that context.

34. Conspicuous, with reference to a term, means so written, displayed, or presented that a reasonable person against whom it is to operate ought to have noticed it. A term in an electronic record intended to evoke a response by an electronic agent is conspicuous if an individual presents it in a form that would enable a reasonably configured electronic agent to take it into account or react to it without review of the record.

electronic agent to perform actions that will be contrary to the interest of the parties. This protection mechanism embedded in the framework not only insulates the party using the electronic agent from higher levels of liquidated damage in the event of breach but also puts up a higher threshold on the part of the human entity engaging in such conduct.

VI. CYBERSPACE CONTRACTING AND ELECTRONIC COMMUNICATION

As mentioned earlier, at common law a contract is consummated when an offer is accepted. This appears to be a simple rule, but many disputes on how to characterize and identify invitations to treat and offers and acceptances, have given rise to confusion in cyberspace contracting. Due to the large number of entities spanning wider and multiple jurisdictions in this era of increased automation, the issue of identifying offer and acceptance has become the crux of the problem.

According to the traditional model, "an offer is manifestation of assent to enter into a bargain made by the *offeror* to the *offeree*, conditional on the manifestation of assent in the form of some action (promise or performance) by the *offeree*." This dictates that the parties may make the offer or acceptance through words, conduct, or communication. The main distinction between the offer and acceptance is that the offer must make a promise of future performance, whereas "acceptance" must consist of agreeing to the terms and conditions of the offer. When contracting is transformed into the digital arena due to the burgeoning need for e-commerce, the basic fundamentals do not change. The problem stems from correctly identifying the "offer" and the "acceptance," and hence legitimizing a contract. In cyberspace contracting, the situation gets further complicated when two electronic agents begin the process of completing a contract. In a plain vanilla "click and agree" situation, we do not foresee any conflict unless a case of breach develops later on. The ambivalence comes from the situation where the electronic agents in question begin to change and modify performance terms triggering a series of electronic signals or messages that could be interpreted in various ways.[35]

In the cyberspace mode of contracting, parties rely on electronic methods of offer and acceptance. In the absence of Electronic Data Interchange (EDI)[36] trading partner agreements, the parties will be exposed to an open-ended electronic messaging framework to con-

35. For a detailed discussion on electronic signals, message transmissions by electronic agents and how they affect contract formation, see Jeff C. Dodd & James A. Hernandez, *Contracting in Cyberspace*, COMPUTER L. REV. & TECH. J., Summer 1998, at 1.

36. *See* UNCITRAL, Model Law on Electronic Commerce, Article 2B, *available at* http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm (last visited Jan. 26, 2005) (on file with the Texas Wesleyan Law Review). This defines an "electronic data

summate a contract. In this regard, UCITA went very thoroughly over the established provisions of Article 2B to facilitate the flourishing of electronic commerce in cyberspace. As a result, the proposed legal framework broadened the scope and scenario under which a contract can be formed.[37] Additionally, it explored various means by which two parties can complete a contract even though the terms of acceptance vary from the terms of offer.[38] Unfortunately, this is what I believe has opened the Pandora's box because the broadened scope allows the formation of contracts by simply receiving an electronic message without the benefit of thorough review. If the proposed legal framework under the Uniform Computer Information Transaction Act or any of its variants is to be accepted as a guide for cyberspace contracting, there could be cases where contract formation may precede agreement between parties.

---

interchange" as the electronic transfer from computer to computer of information using an agreed standard to structure information. *Id.*

37. UCITA's goal of providing a much-needed consistency in dealing with both real-space and cyberspace in contract formation is worth note here. UCITA Section 202(a) follows U.C.C. § 2-204 (1995), the Restatement (Second) of Contracts § 19 (1981), and common law in most states. *See* UNIF. COMPUTER INFO. TRANSACTIONS ACT § 202(a) (2002). A contract can be formed in any manner sufficient to show agreement: orally, in writing, by conduct, inaction, or otherwise. Of course, no contract is formed without intent to contract. This section does not impose a contractual relationship where none was intended. In determining whether or not conduct or words establish a contract, courts must look to the entire circumstances, including applicable usage of trade or course of dealing. Subsection (a) recognizes that an agreement can be formed by operations of electronic agents. This is important for electronic commerce and gives force to choices by a party to use an electronic agent for formation of a contract. The agent's operations bind the person who deployed the agent for that purpose.

38. Section 204 of UCITA provides a comprehensive guidance in dealing with situation where acceptance is associated with varying offers:

> An acceptance materially alters an offer if it contains a term that materially conflicts with or varies a term of the offer or that adds a material term not contained in the offer. [A] contract [is] formed by varying acceptance . . . [e]xcept as otherwise provided in Section 205, [when] a definite and seasonable expression of acceptance operates as an acceptance, even if the acceptance contains terms that vary from the terms of the offer, unless the acceptance materially alters the offer. [Additionally], [i]f an acceptance materially alters the offer, the following rules apply: (1) A contract is not formed unless: (A) a party agrees, such as by manifesting assent, to the other party's offer or acceptance; or (B) all the other circumstances, including the conduct of the parties, establish a contract. (2) If a contract is formed by the conduct of both parties, the terms of the contract are determined under Section 210. [Furthermore], [i]f an acceptance varies from but does not materially alter the offer, a contract is formed based on the terms of the offer. In addition, the following rules apply: (1) Terms in the acceptance, which conflict with terms in the offer are not part of the contract. (2) An additional nonmaterial term in the acceptance is a proposal for an additional term. Between merchants, the proposed additional term becomes part of the contract unless the offeror gives notice of objection before, or within a reasonable time after, it receives the proposed terms.

UNIF. COMPUTER INFO. TRANSACTIONS ACT § 204 (2002).

In the foregoing discussion, we merely highlighted causes of concern as cyberspace contracting slowly comes out of its infancy and becomes as forceful as real space contracting. Over the last decade, a lot of improvement has taken force in areas related to contract formation, construction, interpretation, and selecting jurisdiction. However, as our analysis reveals, the goal of providing a robust and consistent legal framework to enable e-commerce activity to flourish is far from being achieved. Simply focusing on the subset of contract formation, we find the general choice of law principles are far from being complete and comprehensive. Perhaps, the next evolution for cyberspace contracting should go via embracing the incomplete contract paradigm. This is because the framework of UCITA envisioned the spirit of self-enforcement. However, research suggests that the domain of self-enforcing contracts extends to isolated interactions between strangers.[39] This can exploit the insufficiency inherent in UCITA to populate the cyberspace with myriads of contracts without agreement between parties, leading to a clogged court system for years to come. On the other hand, intentionally incomplete contracts[40] are simple in form, clear in commitment, and structured to create opportunities for parties to fully exploit the contractual surplus domain of digital commerce in cyberspace.[41]

VII. CAN INCOMPLETE CONTRACT PARADIGM WORK IN CYBERSPACE?

Traditionally, a contract is viewed as incomplete if it contains gaps or deficiencies so severe that in the opinion of the courts, the performance of the terms of the agreement would be legally unenforceable.[42] This has been one of the drawbacks in dealing with deliberately incomplete contracts, as more often than not, the courts rule that the

39. *See* Robert E. Scott, *A Theory of Self-Enforcing Indefinite Agreements*, 103 COLUM. L. REV. 1641 (2003).

40. Omri Ben Sharar, *Agreeing To Disagree: Filling Gaps in Deliberately Incomplete Contracts* (2004), American Law & Economics Association 14th Annual Meeting, *available at* http://law.bepress.com/alea/14th/art36 (last visited Jan. 25, 2005) (on file with the Texas Wesleyan Law Review).

41. Contract surplus can be understood as the aggregate incremental gain achieved by the contracting parties, as the difference between the aggregate gain by the parties in the most efficient contractual condition arrived by the renegotiation of the contractual terms and that obtained in the least efficient contractual condition. This clearly illuminates the fact that in an interacting transactional world, negotiation and subsequent formation of optimal contract can yield a more profitable revenue scenario. *See* Aaron S. Edlin & Benjamin E. Hermalin, *Contract Renegotiation and Options in Agency Problems*, 16 J.L. ECON. & ORG. 395 (2000); *see also* Yeon-Koo Che & Donald B. Hausch, *Cooperative Investments and the Value of Contracting*, 89 AM. ECON. REV. 125 (1999).

42. The U.C.C. defines "contract" as "total legal obligation which results from the parties' agreement as affected by this Act." U.C.C. §1-201(11) (1995). Thus, a "contract" by definition cannot be incomplete. *See* RESTATEMENT (SECOND) OF CONTRACTS § 33(2) cmt. b (1981).

contract is too vague, or too indefinite to be enforced,[43] thereby effectively creating a contract/no contract boundary. However, if the court relaxes the boundary condition and allows the parties to enter into a contractual situation, whereby they could agree on some of the terms and leave some for future fulfillment via renegotiation, we could see the creation of contracts with a better chance of being enforceable.

Let us for a moment, shy away from the complete contract paradigm and assume the two entities agree to negotiate to take advantage of any ex-post contractual surplus.[44] For this to facilitate, we must be cognizant of three issues. First and foremost, the scenario presented requires the introduction of a "bargaining" model in the legal framework of contracting. Second, the legal framework must be able to handle modification of contractual terms by mutual consent via electronic messaging. Lastly, and perhaps the most important, the scope and limitation of the incomplete contracting model has to be incorporated in the proposed framework such that legal challenges and inquiries will retain the enforceability of such contracts.

VIII. CONCLUSION

As the commercial activity in cyberspace exploded over the last two decades, so did the legal disputes and development of both case law and substantive laws. However, the evolution of legal framework has not been able to keep up with the emergence of both the complexity and ambivalence found in cyberspace contracting. In this review, we questioned some of the current contract law rules, which are either evolving or becoming very slow to be adopted universally. Thus, the search for a universally acceptable, yet legally robust framework, is still on. Therefore, the objective of this essay is to propose a framework for cyberspace contracting that embeds the robustness of deliberately incomplete contracts into the fluid comprehensiveness of the proposed Uniform Computer Information Transactions Act. At the current stage of this amalgam, it is a stretch whether this will be a viable model or not. But, perhaps, we are emboldened by the illustrious history of contract law that encourages courts to search exhaustively to explore the contracting parties' actual intentions for creating and renegotiating the contract. And it is in this spirit of contract law that lies the support for our proposed model. Let's build on it.

43. *See* Varney v. Ditmars, 111 N.E. 822–26 (N.Y. 1916).
44. *See* Che & Hausch, *supra* note 41; Edlin & Hermalin, *supra* note 41.