Contracting In Cyberspace

by

Jeff C. Dodd and James A. Hernandez*

I. INTRODUCTION

Many authors have written about the travails and techniques of “cyberspace contracting.” This commentary masks a simple fact: the issues relating to contracting in cyberspace relate more to method than substance. The substance of a contract—the arrangement of the parties—is not affected much by whether the parties form the contract through electronic means instead of through more traditional methods. The manner of contracting may sometimes affect the degree to which courts will recognize the arrangement, but the arrangement itself is not much influenced.

Of course, information law generally or “cyberspace law,” does concern itself with substance. For example, whether software licenses are forced into a sale of goods model is an issue of great consequence, and substantive outcomes turn upon the resolution of that issue. But here we address a thin slice of cyberspace law: how can parties create enforceable contracts in electronic commerce? Making this the central question of “cyberspace contracting” illuminates the broad range of this thin slice; it affects all types of contracts, whether they call for the sales of goods, licenses of software, or any other transaction with respect to an item of commercial exchange. It treats only the formation of contracts, not the substance.

This question certainly is neither without significance nor without its difficulties. Wrestling with cyberspace contracting issues has meant bending traditional legal notions around the new technologies for making contracts. These issues, of course, are numerous and diverse. For example, if a chemical company’s computers “speak” to a buyer’s computers with respect to an order for chemicals, is the completed order valid, though no human directly intervened in that particular instance of the contracting process? If a person orders books electronically from the web site of Amazon.com, for example, does that method of ordering create an enforceable contract, though no writing or even verbal confirmation completes the transaction, no signature is present and the order exceeds $500? These issues do not directly implicate the web of contractual rights and duties; rather, these issues relate only to contract formation in a variety of electronic settings.

As one may suspect, the law imperfectly addresses these problems. To date, given the absence of clear legislative or judicial guidance, a form of “cyberspace law merchant” has developed to govern cyberspace contracting. Indeed, the development of the cyberspace law merchant parallels the emergence of the law merchant in

* Copyright © 1997-1998 by Jeff C. Dodd and James A. Hernandez. Mr. Dodd is a partner, and Mr. Hernandez is an associate, at Mayor, Day, Caldwell & Keeton, L.L.P.

1. U.C.C. § 2-201 (1995) (stating that “a contract for the sale of goods for the price of $500 or more is not enforceable . . . unless there is some writing sufficient to evidence that a contract for sale has been made . . .”).
Contracting in Cyberspace

Europe during the late Middle Ages. The economy of the Middle Ages was local and agrarian, but in the eleventh, twelfth and thirteenth centuries, leaps in agricultural production, population growth and technological innovations, combined with the dramatic expansion of cities, accompanied the rise of a merchant class throughout Europe. These merchants increasingly traded across traditional boundaries, tying city to the countryside, nations to other nations. The law merchant developed to address the needs for certainty and stability in commercial relationships that spanned across the traditional boundaries. In doing so, the law merchant drew heavily from the notoriously unsystematic, though highly refined principles of Roman civil law, Roman (and Mediterranean) customs of maritime trade, canonical law, as well as the customs and practices of merchants. Collections of these rules were occasionally published, especially by Italian cities, though these collections were at first episodic and not comprehensive. As transnational commerce increased, so did the uniformity of the mercantile law.

The law merchant followed in the wake of the commercial practices for which it was fashioned to regulate, and in turn formed those commercial practices themselves; the commercial law of cyberspace, including contracting principles, evolved from the customs of those engaged in cyberspace transactions. The dramatic changes in medieval social conditions powered the rise of merchant commerce and mercantile law; the developments in technology during the past fifteen years have enabled any business to engage in cyberspace commerce, forcing the development of commercial cyberspace law. The law merchant borrowed from a variety of legal and non-legal sources, melding them into an increasingly uniform law to respond to the exigencies and practices of merchants; the emerging law of cyberspace samples heavily from a variety of legal and customary sources. Much of what a lawyer now says about “cyberspace contracts” is little more than a set of conjectures about what the courts will or should do. These conjectures are based on the lawyer’s experience with the practices and customs of electronic commerce mixed with borrowed ideas from other laws (e.g., Article 2 of the Uniform Commercial Code) that seem to relate, even if loosely, to these commercial transactions.

Cyberspace law has started to take some shape as lawyers and merchants increasingly look to the same models and structures for guidance. Proposed statutes dealing directly with cyberspace contracting issues are working their way through the process of uniform and legislative law making. A few of these statutory laws have already made it through the gauntlet.

Although this unsystematic growth through practice has led to a motley collection of legal standards governing cyberspace contracting, most of the issues that these standards purport to deal with relate to only five root problems:

(a) Authority. When is the contract “my” contract? What electronic “actions” will be attributed to me? Can electronic machines be agents and bind contracting parties?

(b) Methods of Formation. How are offers and acceptances electronically formed? Is a contract formed? When is it formed?

---

(c) **Authentication.** If electronic signals are exchanged, without more, will this exchange be treated as the functional equivalent of writing? If I send certain electronic signals, will they be the equivalent to my “signature”? How can I make sure that my signals will not be wrongfully used—i.e., stolen—by another?

(d) **Payment.** If one side of the bargain involves payment, can payment be effectively and securely made electronically?

(e) **Jurisdiction.** What law governs the formation and enforceability of the substance of the electronic contract? Where can the parties to the electronic contract be sued?

This paper addresses these issues in the order listed above. In the course of discussing these remaining sets of problems, we advance not only our conjectures about the current state of cyberspace contract law, but also cover some of the current and developing legislation that addresses these problems. This article examines current contracting practices, most prominently electronic data interchange agreements, touching upon the five root issues of cyberspace contracting.

**II. CONTRACT FORMATION**

**A. Overview**

As any first year law student knows, there is nothing magical about forming a contract: at a minimum, two parties agree to be bound by the terms of their agreement. Under the traditional view, the minuet of offer and acceptance forge the contract through a formalized bargaining process. An offer is no more than a “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.”

A party can accept such an offer in “any manner and by any medium reasonable under the circumstances”, unless the offer stipulates that the other party must accept in a particular manner. Determining what constitutes a reasonable response involves considerations of the speed and reliability of the medium, a prior course of dealing between the parties, and trade usage.

Most cyberspace transactions do not differ inherently from the “real world” counterparts envisioned by traditional contract law principles. Thus, regardless of the transaction’s form, the formation of cyberspace contracts, like their real world analogues, can—and should—be analyzed by focusing on the core elements that comprise the particular contract in question and by applying traditional contract law principles.

However, technology has effaced some of the traditional indicia of contract, such as a clear human manifestation of intent, or a pen and ink signature at the end of a paper document. Where technology precludes strict adhesion to contract law, lawyers usually advise their clients to mimic the traditional indicia of a contract. For instance, “point and click agreements”, where a user must assent to the terms of an online system agreement by clicking on the “YES” icon or the “I AGREE” icon, are cyberspace analogues to traditional transactions in which consumers must sign a

---


6. See U.C.C. § 2-206(1)(a) (1995). See also Restatement (Second) Of Contracts § 65 (1981) (indicating more generally that acceptance can be in any manner customary at the time and place).
Contracting in Cyberspace

receipt or invoice to manifest assent. Similarly, online conduct, such as downloading software or other content, does not differ inherently from real world assent by performance.

From one perspective, therefore, the art of cyberspace contracting involves searching for areas lacking indicia of traditional contracting and fashioning surrogates for such indicia. The efforts to make the new methods resemble judicially-accepted methods create a legal fiction.

[T]he fiction represents the pathology of the law. When all goes well and established legal rules encompass neatly the social life they are intended to regulate, there is little occasion for fictions. There is also little occasion for philosophizing, for the law then proceeds with a transparent simplicity suggesting no need for reflective scrutiny. Only in illness, we are told, does the body reveal its complexity. Only when legal reasoning falters and reaches out clumsily for help do we realize what a complex undertaking the law is.7

Three of the four core problems of cyberspace contracting discussed in this paper bring Fuller’s observation especially to mind: authority, method and authentication. Historically, in the absence of established legal rules, practitioners have resorted to a picture of traditional paper-based contracting to respond to cyberspace contracting problems. In essence, cyberspace-contracting practice is based on a fiction that electronic commerce is paper commerce.8

B. Attribution and Authority: The Problem of Electronic Agents

Perhaps one of the most troubling areas in the cyberspace contracting environment arises when an “electronic agent” concludes a contract. This occurs when “a computer program or other electronic automated means [is] used, selected, or programmed by a person to initiate or respond on behalf of that person to electronic messages or performances without review by an individual.”9 Electronic agents do not find easy analogues in traditional contract law. Contract law assumes that human discretion will factor into decisions to make an offer and to accept or reject that offer.10 However, contracting parties can fairly discern those choices from the actions of the other contracting parties. Stated otherwise, an individual can be held accountable for her promises or actions because those promises or actions are the product of her volition;11 this leads the other parties to expect that she will keep her promise, regardless of her subjective intentions.12 These two conceptions—promise as obligation rooted in human choice and promise as reflection of objective manifestations of choice—are not necessarily incompatible in the electronic model of contract formation. Just as the advent of “intelligent weaponry” has diminished the fabric of the law and morality of warfare, the emergence of “intelligent machines

7. LON L. FULLER, LEGAL FICTIONS, viii (1967).
11. See id. at 61-62.
12. See 1 E. ALLEN FARNSWORTH, CONTRACTS § 3.6 (1990).
that make and respond to orders with little or no human discretion has shaken the
foundations of contract law. The objective manifestations of contract may be present,
but the direct operation of human choice is not.

As a practical matter, those who rely on electronic agents in contracting
currently do so under the aegis of “electronic data interchange” (“EDI”) or “trading
partner” agreements. The function of EDI agreements is much broader than sorting
through agency issues; indeed, many do not appoint or sanction the use of electronic
agents as such. Rather, these agreements generally focus on a broad range of issues
associated with electronic trading, including the acceptance of certain messages in
certain formats as sufficient to create contracts. For example, when a retailer and a
wholesaler network for EDI transactions, the retailer’s inventory system automatically
evaluates when particular items should be ordered and, perhaps after some review or
intervention by an employee, the system transmits an electronic order to the
wholesaler. The trading partner agreement defines how the retailer must structure his
“messages” to qualify as orders sufficient to create a contract.

In setting the message standard, the trading partner agreements also explicitly
set forth the procedures that the parties must follow to attribute these electronic
messages to the parties. So, trading partner agreements invariably touch upon
authority. Nonetheless, trading partner agreements often will not explicitly identify
whether the originator or receiver in the electronic transaction may be an electronic
agent. This means that the party relying upon a message communication may be
unaware of the fact that an electronic agent participated in the other party’s
communications. In such cases, the objective theory of contracts should aid the party
who relied on these manifestations of assent. Because the messages result directly
from a prior contract, courts should enforce contracts formed on the basis of
“messages” complying with the attribution procedures embraced by the parties.

Article 2B would confirm this result, since Article 2B would sanction
consensual arrangements concerning commercially reasonable “attribution
procedures.” Attribution procedures are for “verifying that an electronic
authentication, record, message, or performance is that of the respective party or is for
detecting changes or errors in content.” Reliance upon the attribution procedure in
good faith provides the receiving party the benefit of a presumption that the message
or performance came from the sender. Suppose, however, that the trading partner agreement contains no attribution
procedure or reference to electronic agents, and one party knows an electronic agent is
acting on behalf of the other party. Should that knowledge change the result? This
squarely puts the issue of whether the actions of an electronic agent generally should
be attributed to the programming party as a matter of agency law. It is not clear that
agency law, in the absence of an agreement or statute, would recognize the power of
computers to bind, though they may be programmed to take actions. That is not to
say that a court should not attribute the actions of an electronic agent to its principal;
we think it fair to do so. The fact that an offer or acceptance was completely
automatic should not necessarily indicate that the parties did not intend to create a
binding contract. We emphatically believe that a company that creates an entirely

13. See UNCITRAL, MODEL LAW ON ELECTRONIC COMMERCE, Article 2(B) [hereinafter “UNCITRAL, MODEL LAW”] (defining an “electrical data interchange” as the electronic transfer from computer to computer of information using an agreed standard to structure the information).
15. Id. § 2B-116(a)(2).
automated system to make or accept offers should be bound by the objective indicia of the intent created by the responses issued through its programming. However, prudence dictates caution in the absence of legislation or case law.

Fortunately, proposed uniform legislation would validate actions of electronic agents even without explicit agreement among the parties. Thus, the UNICITRAL, Model Law on Electronic Commerce would expressly treat a “data message” as that of the originator if “it was sent . . . by an information system programmed by or on behalf of the originator to operate automatically.” The April 15, 1998 draft of Article 2B adopts this approach. Among other actions, an electronic agent may form a contract for a party by recognizing “the existence of a contract.” Also, Section 2B-118 flatly states that operations “of an electronic agent constitute the authentication or manifestation of assent of a party if the party used, selected, or programmed, the electronic agent for the purpose of achieving results of that type.” The proposed Uniform Electronic Transactions Act, now set in motion by the National Conference of Commissioners on Uniform State Laws, follows Article 2B’s lead. Section 202 provides that “an electronic record is attributable to a person,” if among other things, “it was in fact the action of that person, a person authorized by it or the person’s electronic agent.”

Section 401 more explicitly states that, subject to certain exceptions, “[a] person is bound by the terms and agreements resulting from the operations of its electronic agent even if no individual was aware of or reviewed the electronic agent’s actions or the resulting terms and agreements.” Neither Article 2B nor the proposed Uniform Electronic Transactions Act would require an agreement affirmatively empowering the agent. Thus, an electronic agent’s power rests on the fiction that such agents do not differ from human agents; the principal has delegated actual authority through detailed instructions comprising the programs.

Article 2B remains deeply conflicted regarding the actions that an electronic agent may perform in an “automated transaction,” absent an agreement about the agent’s authority. This ambivalence about the role of electronic agents pervades Article 2B. For example, Article 2B clearly invests electronic agents with the power to “manifest assent” on behalf of a party. As part of manifesting assent, an electronic agent may exercise a party’s “opportunity to review” a record or term. Though space does not permit a detailed discussion of the signal importance of “manifest assent” in Article 2B, this concept essentially has three basic functions. First, in some cases, a party must manifest assent to a particular record in order for it to bind that party. Thus, a party’s release of its intellectual property rights must come in a record to which that party has manifested assent. In a commercial setting, a party manifesting assent to a standard form record is generally bound by that standard

19. ARTICLE 2B—April 15, 1998 Draft § 2B-119(a). See also id. § 2B-116(a) (a message or performance received is attributed to the sender if it was sent by the sender’s electronic agent).
21. Id. § 401(b)(4).
22. Id. § 2B-102(a)(4) (defining “automated transaction” as “a contract formed by electronic means or electronic messages in which the acts or messages of one or both parties will not be reviewed by an individual as an ordinary step in forming the contract.”).
23. Id. § 2B-111.
24. Id. § 2B-112; See also UNIFORM ELECTRONIC TRANSACTIONS ACT—March 23, 1998 Draft § 107(a).
25. Id. § 2B-206.
Second, in some cases a party must manifest assent to a particular term in order for that term to become part of the contract. Thus, in a mass-market license setting, a party adopts the terms of a license only if the party manifests assent, or otherwise agrees, “before or in connection with the initial performance or use of or access to the information or informational property rights.” Third, manifest assent can serve as a signature substitute for certain purposes.

Although Article 2B would allow the electronic agent to supply the manifest assent without the express sanction of an agreement, it also seems to require a form of judgment or discretion. Thus, for a manifestation of assent to occur, the “person or electronic agent” must (1) have “knowledge of [the record], or . . . the opportunity to review, the record; (2) have “an opportunity to decline to engage in the conduct”; and (3) engage in “affirmative conduct or operations that the record conspicuously provides or the circumstances . . . clearly indicate will constitute acceptance” of the record or term. Note how these actions imply some judgment. Article 2B does not define actual knowledge, much less attribute knowledge to programs. We believe that the term “actual knowledge” refers to the sort of knowledge endemic to human beings.

This leaves an electronic agent with one method of satisfying the first of the three conditions of manifest assent: it must exercise an opportunity to review. For this to happen, the record or term must be “made available” to the electronic agent “in a manner that . . . would enable a reasonably configured electronic agent to react.” Mere availability for authentication does not appear to suffice; the program must have the ability to react. Suppose a term included in a record sent to an electronic agent requires the principal of the agent to pay “liquidated damages” in the event of breach, and to bring suits exclusively in a designated judicial forum. Note that the current draft of Article 2B does not require the parties to make these terms conspicuous or to separately agree to the terms. Authentication of the record will suffice. However, while a party may program an electronic agent to do much, it will require a sophisticated program to process the import of those terms. Has the record been made available in a manner to allow reaction if the electronic agent cannot detect such terms? Should a party transmitting those terms not have the ability to rely on the authentication of the record when it does not know of limitations in the electronic agent’s programming, and the electronic agent creates a message evidently agreeing to the record? The words of Article 2B seem, on the one hand, to accord some allowances for the program that cannot react. On the other hand, the Article appears to allow a party to rely on the electronic agents of another. In sum, Article 2B is ambivalent.

This becomes even more evident when we consider the rare occasion of “conspicuousness” in Article 2B records. For example, a party can show the third element of manifesting assent—authentication—by taking actions “that the record conspicuously provides, or the circumstances . . . clearly indicate, will constitute acceptance” of the record or term. How does an electronic agent measure

26. Id. § 2B-207.
27. ARTICLE 2B—APRIL 15, 1998 DRAFT §§ 2B-102(a)(30), (31) (defining “mass market license” and “mass market transaction”).
29. Id. § 2B-111(a). See also UNIFORM ELECTRONIC TRANSACTIONS ACT—MARCH 23, 1998 DRAFT § 107(a).
30. Id. § 2B-112(g).
32. Id. § 2B-111(a).
 conspicuous warnings or detect circumstances indicating that certain actions constitute acceptance? Both of these activities seem to import discretion. Interestingly, however, Article 2B would impose on the person who employs an electronic agent to act reasonably in configuring it to take into account “conspicuous” messages. Once again, Article 2B seems torn: it allows programs to manifest assent, but it requires some individual responses implying judgment. It then makes the party using the electronic agent anticipate when something conspicuous might appear in someone else’s incoming form.

Article 2B’s hesitancy about the capacity of electronic agents becomes apparent when it treats situations where electronic agents face humans. Where two electronic agents operate in a manner that signifies agreement, the agents form an agreement. In situations involving an electronic agent and a human, the agreement is construed against the human if he “has reason to know that [he] is dealing with an electronic agent and takes actions that the individual knows or should know will cause the agent to perform, provide benefits, or permit use of the information . . . that is the subject of the contract, or are clearly indicated as constituting acceptance regardless of other expressions or actions by the individual to which the electronic agent cannot react.”

More importantly, the contract terms involving an electronic agent on one side and an individual on the other “do not include terms provided by the individual in a manner to which the electronic agent could not react.” In such cases, Article 2B protects the party using electronic agents from humans who may take advantage of the pre-programmed limitations of the agent. Article 2B also presumes that electronic agents can appropriately respond to gradations in circumstance, various manners of making specific terms conspicuous, and various warnings calling particular terms into account.

We certainly do not criticize Article 2B’s approach to electronic agents. Rational choice is the touchstone for the validity of contracts; imputing rationality to programs that a party intends to employ raises difficult questions. The fiction allowing Article 2B, the UNCITRAL Model Law, and trading partner agreements to treat programs as if they were human agents breaks down if the programs are put to the challenge of acting as true agents as normally conceived. Even retail clerks shoulder the responsibility for responding to the unusual requests of humans. As agents, the law charges them with various duties corresponding to the notion that they are expected to exercise some judgment. For this reason, we believe that those who employ electronic agents in the future will continue to do what they currently do, even after the enactment of Article 2B: either limit the other side’s choices to a menu composed by the electronic agent’s principal or ensure the existence of an agreement governing electronic transactions and the permissible bounds of agency.

33. Id. § 2B-102(a)(8).
34. Id. § 2B-204(2).
35. Id. § 2B-204(3). See also Uniform Electronic Transactions Act—March 23, 1998 Draft § 401(b)(2).
C. Methods of Formation

1. Offer and Acceptance

The “orthodox catechism” of contract law envisions a contract as evolving from a bargaining process in which both parties assent to a sufficiently defined and binding agreement. Parties manifest assent through offer and acceptance. As Professor Farnsworth states, 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.” Parties may make the offer and the acceptance through words or conduct; however, the offer must somehow make a promise, whereas the acceptance need only assent to the terms of the offer. Acceptance becomes a promise through the action of the offer. So a party may show her acceptance by either promise or performance, though the offeror may in theory dictate the form that the acceptance may take.

Contracting in the electronic world does not usually disturb this traditional model. Most common difficulties, which may seem trifling, involve the manner of proving the offer and acceptance. For example, suppose a party sends a printed order that requires acceptance by parcel post. If the accepting party confirms the order via e-mail, is the contract formed? In the past, courts have found assent even when the parties have employed different technologies to send their assents. Courts have also found assent when the parties have specified that a response must come in a form different from the one actually used. Thus, courts have held that acceptance of a telegraphed offer by a mailed acceptance was reasonable.

Of course, much of this becomes irrelevant if performance occurs. Depending on the circumstances and on any prior agreement by the parties, acceptance of an offer often occurs through performance of the requested service or shipment. This is especially true in the electronic world where the performance entails electronic communication of digital information. Both Article 2 and the Restatement (Second) of Contracts validate acceptance by performance. Moreover, Article 2 broadly provides that an offer to buy goods “for prompt or current shipment shall be construed as inviting acceptance either by a prompt promise to ship or by the prompt or current shipment of . . . goods . . . .”

By contracting, parties can eliminate most of the troubles lingering with electronic methods of offer and acceptance. EDI trading partner agreements do just that. When parties have entered into a trading partner agreement before the

---

37. Farnsworth, supra note 12, § 3.2.
38. Id. § 3.1.
39. Id. § 3.3.
40. Id. §§ 3.10, 3.11, 3.12.
41. Id. § 3.12. See also U.C.C. § 2-206(1)(a); Restatement (Second) Of Contracts §§ 62, 65.
42. See Farnsworth, supra note 12, § 3.13.
43. U.C.C. § 2-206(1)(b). The emphasis is on prompt action. An offeror not notified of acceptance within a reasonable time may treat the offer as having lapsed by acting before delivery of the goods. Similarly, “[w]here beginning performance is a reasonable mode of acceptance, an offeror who is not notified of acceptance within a reasonable time may treat the offer as having lapsed before acceptance.” Id. § 2-206(2). The Restatement (Second) Of Contracts indicates that if an offer invites acceptance by performance, the contract requires no notice of acceptance given to the offeror (buyer). Restatement (Second) Of Contracts § 54.
transaction, they invariably establish the means of transacting business and concluding an offer and acceptance. Among other provisions that govern message formats, data segments, system requirements and maintenance, the trading partner agreements will explicitly approve electronic messages accessible to the receiving party of the message. Additionally, the agreements will provide that “valid and enforceable obligations may be created by the communication of messages in compliance” with the agreement. A contract will form when “the message sent as acceptance of an offer has been received in accordance with” the agreement.\footnote{44. \textit{UN/EC Working Party on the Facilitation of International Trade Procedures, Commercial Use of Interchange Agreements for Electronic Data Interchange}, at § 4.1 (Jan. 1996) [hereinafter \textit{Model Interchange Agreement}].}

Certainly the open-ended principles of contract law would have eventually embraced, if they have not already embraced, the idea of an electronic response, especially as the use of e-mail systems increased. In any case, proposed or emerging uniform laws now in process will eliminate any question about the sufficiency of electronic messages in creating contracts. Proposed revisions to Article 2 and proposed Article 2B would broadly validate the use of “records”—which includes information stored in electronic media—as sufficient to prove offers and acceptances, regardless of whether both parties used electronic messages.\footnote{45. \textit{Id.} § 4.3.} Indeed, as proposed Section 2B-203 states, “[u]nless otherwise unambiguously indicated by the language of the offer or the circumstances, [a]n offer to make a contract invites acceptance in any manner and by any medium reasonable under the circumstances . . . ,”\footnote{46. Article 2B defines “record” as “information [that is] inscribed on a tangible medium or stored in an electronic or other medium and retrievable in perceivable form.” \textit{Article 2B—April 15, 1998 Draft} § 2B-102(a)(38). \textit{Accord Uniform Electronic Transactions Act—March 23, 1998 Draft} § 102(16).} including by electronic record. This section provides even more explicitly that a “record or authentication may not be denied legal effect, validity, or enforceability solely on the ground that it is in electronic form.”\footnote{47. \textit{See U.C.C., Revised Article 2, Sales} §§ 2-201, 2-203, 2-205, 2-207 (ALI Discussion Draft, March 1, 1998); \textit{Article 2B—April 15, 1998 Draft} §§ 2B-201, 2B-202, 2B-203, 2B-204, 2B-205.} So, if an offeror specifically states the method or mode of acceptance, he must be very, very specific.\footnote{48. \textit{Article 2B—April 15, 1998 Draft} § 2B-203(a)(1).} Thus, legal fictions have developed so that parties may treat electronic messages the same as paper messages.

\footnote{49. \textit{Id.} § 2B-113. \textit{See also Uniform Electronic Transactions Act—March 23, 1998 Draft} § 201 (“A record may not be denied legal effect, validity or enforceability solely because it is an electronic record.”).}

\footnote{50. Indeed, acceptance with standard forms loaded with terms varying from the terms of the offer may nevertheless create a contract; Article 2B has a complex of rules to sort out what goes into the contract and what does not. \textit{See Article 2B—April 15, 1998 Draft} §§ 2B-202, 2B-203, 2B-207, 2B-208, 2B-209. But, as with Article 2, this liberal approach of allowing contracts to be formed, and acceptances to come in a variety of forms, tends to create some difficulties. \textit{See Farnsworth, supra note 12, § 3.14.} Article 2B and Article 2 handle these difficulties in basically the same way. For example, if acceptance comes by way of performance, and a prompt promise to perform, or actual performance or notice of performance is not forthcoming promptly, the offeror may after a reasonable time “treat the offer as having lapsed without acceptance.” \textit{Article 2B—April 15, 1998 Draft} § 2B-203(a)(3); U.C.C. § 2-206.}
Yet, treating electronic messages and paper communications as functional equivalents still creates some predicaments. Article 2B’s treatment of the formation of contracts refers to electronic messages that signify an offer or an acceptance, rather than messages intended as an offer or acceptance. This permits the formation of a contract even when a party’s computer merely receives an electronic message, and neither party knew of or reviewed the initial response, reply, information, or acceptance of the contract.\footnote{Id. §§ 2B-203, 2B-204.} This establishes a preference for finding a contract when the parties may not have been in agreement. Electronic messages are more susceptible to scrambling and transmission than transactions conducted by traditional methods.

The current draft of Article 2B includes several provisions designed to address these commonplace problems in electronic contracting. Thus, Section 2B-116 allocates error risk by generally attributing messages to the putative actor if the message resulted from acts of “a third person that obtained access [to] numbers, codes, computer programs, or the like from a source under the control” of the alleged actor “that failed to exercise reasonable care.”\footnote{ARTICLE 2B—APRIL 15, 1998, DRAFT § 2B-116(c)(3). See also UNIFORM ELECTRONIC TRANSACTIONS ACT—MARCH 23, 1998 DRAFT § 402.} This is a fault-based standard. Also, the risk of error or appropriation will remain with a party, even when that party was not at fault, if the other party concludes, in good faith and in accordance with “a commercially reasonable attribution procedure for identifying a person,” that the action was taken by the apparent sender or its agent.\footnote{ARTICLE 2B—APRIL 15, 1998, DRAFT § 2B-116(a)(2).}

Attribution procedures may take a variety of forms. Article 2B defines an attribution procedure as “a procedure established by law, regulation, agreement, or adopted by the parties, for the purpose of verifying that an electronic authentication, record, message, or performance is that of the respective party or for detecting changes or errors in content.”\footnote{Id. § 2B-102 (a)(2).} The possibility exists that an attribution procedure under Article 2B may be as simple as a PIN number. The point here is that electronic offers and acceptances do not necessarily replicate their more traditional counterparts; therefore, the fiction treating them as functional equivalents would lead to incongruent results. Article 2B created special rules to address the unique forms of pestilence that beset electronic transactions.

2. Timing of a Contract—The Mailbox Rule

In addition to considerations regarding the making of offers and acceptances, cyberspace contracting presents unique problems regarding when the offer, the acceptance, or a rejection of the offer becomes effective. Once again, the fiction of treating electronic messages as paper messages is imperfect.

In most situations, this question has little relevance since disputes generally arise after the parties show some reliance or exchange some value. In some cases, however, the significance relates to the ability of either party to refuse to perform without breach of contract, by revoking either the offer or the acceptance before creation of the contract.\footnote{See FARNSWORTH, supra note 12, § 3.16 (“[a]fter the offeror has conferred a power of acceptance on the offeree by making an offer, that power can be terminated in any of the following ways: (1) revocation of the offer by the offeror, (2) death or incapacity of the offeror, (3) lapse of the offer, or (4) rejection of the offer by the offeree”).}
In the United States, the majority rule with respect to an offer's revocation is that the revocation will be effective only when received by the other party. Generally, receipt occurs "when the writing comes into the possession of the person addressed, or of some person authorized by him to receive it for him, or when it is deposited in some place which he has authorized as the place for this or similar communications to be deposited for him." A different rule applies when the offeror attempts to revoke the offer after the offeree has already dispatched an acceptance. The general rule in this situation, known as the mailbox rule, is that unless an offer provides otherwise, an acceptance is effective when sent. In face-to-face communications, this rule presents no problems since there is no time lapse between the sending of the acceptance and its "receipt" by the other party (i.e., dispatch is instantaneous with receipt). A much different situation exists, however, in the case of offers and acceptances exchanged by parties separated by significant physical distance. As such, the mailbox rule "curtail[s] the offeror's freedom to revoke by ending it at the earliest feasible time."

Should the mailbox rule govern in a cyberspace contracting environment? Arguably there are similarities between e-mail and "snail-mail," but certainly not with respect to speed of delivery. We believe that a better analogy may be telephonic communications. According to Section 64 of the Restatement (Second) of Contracts, in cases involving technology such as a "telephone or other medium of substantially instantaneous two-way communication", the same principles applicable to face-to-face communications should apply with respect to the timing of acceptances. Acceptance through an electronic message in an online environment should not be treated as a paper message, but rather as a face-to-face or telephonic message and thus be effective upon receipt. The underlying rationale is that parties in direct communication will immediately perceive and be able to clarify "ambiguities and misunderstandings." In the cyberspace world, where communications can occur in real time, presumably contracting parties could clarify any garbled messages that occur when background sound or interference inhibits communication. We certainly acknowledge, however, that the logic for applying "in person" rules breaks down

---

56. See id. § 3.17 ("An offer can be withdrawn if notice of withdrawal reaches the offeree no later than the offer does. . . . The revocation is not effective . . . until it is received by the offeree.").
57. RESTATEMENT (SECOND) OF CONTRACTS § 68. See also U.C.C. § 1-201(26) ("[a] person 'receives' a notice . . . when (a) it comes to his attention; or (b) it is duly delivered at the place of business through which the contract was made or at any other place held out by him as the place for receipt of such communications.").
58. See RESTATEMENT (SECOND) OF CONTRACTS § 63 ("Unless the offer provides otherwise . . . an acceptance made in a manner and by a medium invited by an offer is operative and completes the manifestation of mutual assent as soon as put out of the offeree’s possession, without regard to whether it ever reaches the offeror . . . ").
59. See FARNSWORTH, supra note 12, § 3.22.
60. The term used by Internet surfers when referring to mail delivered by the Post Office.
61. See also FARNSWORTH, supra note 12, § 3.22 (stating that the mailbox rule does not apply to “substantially instantaneous means of communication, such as the telephone, telex and electronic mail.”).
62. RESTATEMENT (SECOND) OF CONTRACTS § 64.
63. See Reporter’s Memorandum accompanying UNIFORM ELECTRONIC TRANSACTIONS ACT—MARCH 23, 1998 DRAFT, § 402, Reporter’s Note 34 (“Subsection (e) rejects the mailbox rule and provides that electronic records are effective on receipt. This is consistent with . . . Article 2B.”).
Proposed Article 2B and the proposed Uniform Electronic Transactions Act emphatically reject the mailbox rule for electronic transactions. As the current draft of Article 2B formulates the electronic communication rule, if “an electronic message initiated by a party or an electronic agent evokes an electronic message in response, a contract exists when a response signifying acceptance is received.” This is generally true even if no individual is aware of the receipt.

D. Authentication: Writing and Signature Requirements

1. Overview

We now move to a discussion about the Statute of Frauds, which exists in one form or another throughout the United States. Generally, the Statute of Frauds operates to preclude the enforceability of “certain classes of contracts, unless there is a note or memorandum thereof in writing signed by the party to be charged or his authorized agent.” The Statute of Frauds concerns contracts for the sale of land, contracts that cannot by their terms be performed within a year, contracts to guarantee the debt of another, and contracts for the sale of goods priced at $500 or more. For contracts dealing with the sale of goods, U.C.C. § 2-201(1) provides that any such contract “for the price of $500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker.”

The “signed writing” requirements of the Statute of Frauds serve a number of useful functions, most notably cautionary, approval, efficiency and evidentiary functions. Signed writings serve a cautionary function by conveying to the signer the legal significance of entering into a legally binding agreement. The approval

64. See STUCKEY, INTERNET AND ONLINE LAW § 1.02[4][c] at n. 108.
65. See ARTICLE 2B—April 15, 1998 DRAFT § 2B-120, Reporter’s Notes 1; UNIFORM ELECTRONIC TRANSACTIONS ACT—MARCH 23, 1998 DRAFT § 402(e).
66. ARTICLE 2B—APRIL 15, 1998 DRAFT § 2B-120(a)(1). “[I]f the response consists of furnishing the information or access to the information,” the contract is formed “when the information or notice of access is received or use is enabled, unless the originating message required acceptance in a different manner.” Id. The Uniform Electronic Transactions Act sets out a hierarchy of rules to determine receipt. Unless otherwise agreed, receipt occurs when “the electronic record enters an information processing system from which the recipient is able to retrieve electronic records in a form capable of being processed by that system, and the recipient uses or has designated that system for the purpose of receiving such electronic records or information. An electronic record is also received when the recipient acquires knowledge of it.” UNIFORM ELECTRONIC TRANSACTIONS ACT—MARCH 23, 1998 DRAFT § 402(e).
68. Id. See FARNSWORTH, supra note 12, §§ 6.2-6.6. See also TEXAS BUSINESS AND COMMERCE CODE (listing the types of contracts that must be in writing).
69. U.C.C. § 2-201(1).
70. See THE AMERICAN BAR ASSOCIATION DIGITAL SIGNATURE GUIDELINES [hereinafter, the “ABA GUIDELINES”] at 4.
71. See FARNSWORTH, supra note 12, § 6.1 (commenting on the “suretyship provision” of the traditional Statute of Frauds; Professor Farnsworth notes that in such contexts, the statute “performs an important cautionary function, . . . by bringing home . . . the significance of the promise and preventing ill-considered and impulsive promises.”). See also ABA GUIDELINES at
function relates to the fact that in certain situations “defined by law or custom, a signature expresses the signer’s approval or authorization of the writing, or the signer’s intention that it have legal effect.” 72 The efficiency function relates to the sense of “clarity and finality”73 that the act of signing an agreement conveys with respect to the transaction and “may lessen the subsequent need to inquire beyond the face of a document.” 74 Perhaps the most important of the four general functions is the evidentiary function. 75 A signed writing serves an evidentiary function by providing proof that the parties actually entered into the contract in question and also by identifying the parties to the contract. For example, when a document is executed in a “distinctive manner,” the agreement as executed becomes attributable to the parties signing it, with the identification of the parties providing a means of authenticating the agreement. 76

Statutes of frauds, especially under the U.C.C., often do not apply to contract disputes since U.C.C. rules apply only to executory agreements, while common law rules generally apply only to contracts of a particular type or duration. If the parties use written confirming memoranda or purchase order acknowledgments mailed after receipt of an electronic offer, even electronic transactions will satisfy the writing requirement, independent of issues regarding the sufficiency of electronic records or codes. 77 Nonetheless, in the cyberspace context, the potential problems inherent in authenticating and identifying the parties to an online contract are evident. The online world is ethereal. Anyone who has ever entered a “chat room” on America Online knows the difficulty of verifying the identities of the chat room participants. Online transactions frequently involve people who have never met in person or even talked with one another over the phone. In all likelihood, most parties to online transactions will never meet. 78 As purely electronic contracting has become more commonplace and as more types of transactions are consummated online, the enforceability of these types of agreements has become and will continue to be an issue. This requires thoughtful determinations as to whether electronic messages satisfy the writing and signature requirements of the Statute of Frauds. 79

2. Writing

What might satisfy the writing requirement in an electronic contracting environment? Judges have struggled with somewhat comparable situations, where “new” forms of communication appear, such as when telexes or telegrams were new forms of communication. 80 What about less tangible “writings”? Some courts have

4 (noting that the act of executing a contract “calls to the signer’s attention the legal significance of the signer’s act” thereby helping to prevent “inconsiderate engagements.”).
72. ABA GUIDELINES at 4.
73. Id.
74. Id.
75. See Farnsworth, supra note 12, § 6.1 (noting that the original purpose of the Statute of Frauds “was evidentiary, providing some proof that the alleged agreement was actually made . . .”).
76. ABA GUIDELINES at 4.
77. Id.
79. Id.
80. See Hidca Petroleum Corp. v. Tampimex Oil Int’l, Ltd., 740 S.W.2d 838 (Tex. App.—Houston [1st Dist.] 1987, no writ) (telex sufficient); compare Houston Contracting Co. v.
Jeff C. Dodd and James A. Hernandez


held that tape recordings constitute writings.\(^81\) Other courts have assumed, without expressly addressing the issue, that faxes may also constitute writings.\(^82\) In situations not involving a Statute of Frauds analysis, courts have found that data stored on computer disks constituted writings.\(^83\)

Section 1-201(46) of the U.C.C. is also illustrative. It defines “written” and “writing” to include “printing, typewriting or any other intentional reduction to tangible form.”\(^84\) Given this definition, it is useful to envision an “electronic contracting spectrum” when analyzing related Statute of Frauds issues. Cyberspace transactions, like their real world counterparts, are not all alike. Some are electronic transmissions that can be recorded in a tangible form while others represent electronic impulses coursing through the Internet.\(^85\) For example, e-mail, saved on a hard disk or in hard copy format (i.e., electronic contracting that can be “reduced to a tangible form”) comprise one end of the spectrum while real time chats, in which two online users strike up a bargain, comprise the other. Thus, if a record of the transaction is maintained, it seems the writing requirement would be satisfied, although this is not entirely free from doubt.\(^86\) As such, computer systems routinely yielding printed output, whether at the receiving point or in a functional acknowledgement returned after receipt, should satisfy the writing concept. Additionally, if the online transmission originated from a written document, that writing itself may be sufficient.

But what happens to purely electronic transmissions that do not begin or result in printed or other tangible manifestations? Based on the U.C.C. definition of a writing, the answer depends on how records of the transaction are retained and whether a court can be convinced that storage of the electronic records is tantamount to reducing the message to “tangible form.”\(^87\) E-mail, online chats and bulletin board dialogues that are not stored or printed would probably not satisfy the writing

Chase Manhattan Bank, 539 F. Supp. 247 (S.D.N.Y. 1982) (telex not signed). See also Farnsworth, supra note 12, § 6.7 (listing the following as writings that have satisfied the Statute of Frauds: “a letter, a telegram or telex, a receipt, an invoice, a check, a penciled price list, the minutes of a meeting, another contract, and a will.”).

81. See Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212, 1228 (D. Colo. 1972) (oral agreement for sale of corporation recorded on tape held to be a contract “reduced to tangible form”; but see Roos v. Aloi, 487 N.Y.S.2d 637, 642-43 (Sup. Ct. 1985) (tape recording that “memorialized” oral agreement among shareholders did not constitute a “writing” so as to remove agreement from Statute of Frauds). At least one noted commentator has stated that the status of tape recordings is not yet clear. See Farnsworth, supra note 12, § 6.7.

82. See Bazak Int’l Corp. v. Mast Indus., Inc., 535 N.E.2d 633, 638-39 (1989) (annotated purchase order forms signed by buyer and sent to seller via telecopier held to be within “merchant’s exception” satisfying statutory writing requirement under U.C.C. § 2-201 without express discussion of transmission via telecopy); American Multimedia, Inc. v. Dalton Packaging, Inc., 540 N.Y.S.2d 410, 411 (Sup. Ct. 1989) (under federal arbitration statute analysis, a faxed purchase order was also assumed without discussion to be a writing).

83. See People v. Avila, 770 P.2d 1330, 1332 (Colo. Ct. App. 1988) (a computer disk was “written instrument” within meaning of forgery statute); Clyburn v. Allstate Ins. Co., 826 F. Supp. 955, 956-67 (D.S.C. 1993) (in breach of contract suit brought by insured against insurer, “written notice” required to be given to insured’s agent under South Carolina law before cancellation would be effective and could be accomplished through digital computer).

84. U.C.C. § 1-201(46) (emphasis added).


86. Id. at 10.

87. Id. at 28.
requirement. Similarly, transactions in which the sending and receiving computers maintain only a momentary record of each separate transaction, prior to dispatching transaction information into a general database, would probably not satisfy the writing requirement.

Because laws validating electronic messages as the functional equivalents of paper contracts have lagged, parties have adopted protocols for handling their transactions by contract. EDI agreements provide one example of such contracts. EDI agreements (or trading partner agreements) have become fairly standardized over time, especially in their core provisions mandating that, “[w]ithout regard to the absence of any writings and written signatures . . . the records of [m]essages maintained by the parties shall be admissible and may be used as evidence of the information contained therein.” Many forms require separate logs of all transactions. For example, one form of a standard EDI interchange agreement developed in the United Kingdom requires that each party maintain a “data log” including all messages sent and received, without modification. According to Professor Nimmer, “[o]rdinary rules of evidence indicate that, properly verified, such a log would be admissible evidence of the transactions.”

88. See Smedinghoff, supra note 85, at 10 (advising readers to always maintain a record of the electronic transaction).
89. Id. at 10. See also SELLING PRODUCTS ONLINE, a copy of which is available from the authors, at 28-29 (“[w]here the messages at both ends of the contracting chain yield information fully integrated into the database of the relevant computer and not discernible as a discrete offer or acceptance, however, the tangibility requirement is not met.”).
90. These agreements, however, must address such fairly ticklish issues. As a paper issued by UN/ECE Working Party on the Facilitation of International Trade Procedures pointed out, [O]nce a company decides it will use EDI, it will require agreement with its trading partners on at least the following issues, the priorities of which will vary based upon the specific needs of that company:

a) selection of EDI messages, message standards and methods of communication;
b) responsibilities for ensuring that the equipment, software and services are operated and maintained effectively;
c) procedures for making any systems changes which may impair the ability of the trading partners to communicate;
d) security procedures and services;
e) the points at which EDI messages have legal effect;
f) the roles and contracts of any third party service providers;
g) procedures for dealing with technical errors;
h) the needs (if any) for confidentiality;
i) liabilities in the event of any delay or failure to meet agreed EDI communications requirements;
j) the laws governing the interchange of EDI messages and the arrangements of the parties; and
k) methods for resolving any possible disputes.

MODEL INTERCHANGE AGREEMENT, supra note 7, at 4.
91. Id. § 4.2. This form hedges the broad validation with a phrase, “to the extent permitted by law.” Sometimes that qualifier is deleted from agreements.
92. Smedinghoff, supra note 85, at 10.
93. See SELLING PRODUCTS ONLINE, supra note 89, at 29 (citing EDIA Ass’n, STANDARD ELECTRONIC DATA INTERCHANGE AGREEMENT 7.1 (2d ed. 1990)).
94. Id.
should be an easy one for the courts to reach. After all, the EDI agreement itself is a writing. Certainly, writings identified as agreements in accordance with the parties’ adopted procedures should suffice.

The trick will be validating electronic impulses without a tangible writing or log that both parties, prior to the agreement, acknowledge will suffice. While, especially under the U.C.C., a strong case can be made that a retained electronic record satisfies writing requirements, the interpretation needed to achieve that result yields uncertainty.95

Proposed Article 2B and the proposed Uniform Electronic Transactions Act replace the concept of a “writing” with the concept of a “record.” Both broadly validate electronic records, providing that a “record . . . may not be denied legal effect, validity, or enforceability solely on the ground that it is in electronic form.”96 Under both pieces of proposed legislation, the record does not have to be tangible as long as it is stored in a medium from which it can be retrieved in “perceivable form.”97 This concept comes from copyright law, which does not require that a work be fixed in a tangible medium of expression to be protected by a copyright.98 Article 2B will not require the parties to agree that records will suffice as evidence of these arrangements in advance. Rather, as a matter of law, “a record authenticated by the party against which enforcement is sought is sufficient to indicate that a contract has been made,”99 and will also satisfy the writing requirement. “Authentication,” the functional equivalent of a signature, thus becomes the key concept in the Statute of Frauds analysis under Article 2B.

3. The Signature Requirement

This requirement100 sets the stage for the discussion of a convergence between law and technology that has developed to facilitate electronic commerce on the Internet by providing reliable security for online transactions. It also provides a technological surrogate for traditional paper-based signatures. The Statute of Frauds has always required a signed writing for contracts that fall within its purview to be enforceable. However, a gradual eroding of the statute over time, as well as a broad

95. Id.
96. Article 2B—April 15, 1998 Draft § 2B-113; accord Uniform Electronic Transactions Act—March 23, 1998 Draft § 201 (“A record may not be denied legal effect, validity, or enforceability solely because it is an electronic record. If a rule of law requires a record to be in writing, or provides consequences if it is not, an electronic record satisfies that rule. In any transaction, a person may establish reasonable requirements regarding the type of records acceptable to it.”).
97. See Article 2B—April 15, 1998 Draft § 2B-102(a)(38); accord Uniform Electronic Transactions Act—March 23, 1998 Draft § 102(16); see also UNCITRAL, Model Law dealing with electronic data interchange, which uses the concept of “data message.” Data message is defined in the model law as “information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy.” UNCITRAL, Model Law, Article 2(a).
98. See Selling Products Online, supra note 89, at 29.
100. In addition to a “signed writing,” part performance removes the “bar of the statute, at least to some extent” in certain exceptional situations. Farnsworth, supra note 12, § 6.9. Further, the equitable doctrine of estoppel can operate as an exception to the Statute of Frauds. See Fred M. Greguras et al., Electronic Commerce: Online Contract Issues, 452 PLI/PAT 11 (1996).
concept of “signed,” has led to a variety of things being deemed signatures that at first blush might not appear to be so. For example, courts have held that typed, stamped, and printed symbols, as well as trademarks and printed letterhead, satisfy the signature requirement.

The test for determining whether a party has signed a writing is “whether the other party reasonably believes that the asserted signer’s intention is to authenticate the writing as the asserted signer’s own.” In accordance with this liberal test, the U.C.C. defines “signed” to include “any symbol executed or adopted by a party with present intention to authenticate a writing.” Though the signature test set forth above and the U.C.C. definition clearly suggest that something other than a pen and ink signature at the end of a document will satisfy the signature requirement in a cyberspace contracting environment, some courts have been reluctant to find that adequate authentication has occurred with respect to certain non-paper based documents. Nevertheless, as a legal requirement, the use of electronic transmissions should not result per se in a determination that no signature exists.

Article 2B proposes to move away from the idea of “signature” and focus instead on “authentication.” Article 2B would expressly allow use of encryption

101. See FARNSWORTH, supra note 12, § 6.8 (noting “[t]he requirement that the writing be signed has not been applied with rigor.”).
102. See Bains v. Piper, Jaffray & Hopwood, Inc., 497 N.W.2d 263 (Minn. App. 1993) (holding, inter alia, that the letterhead of a computer generated confirmation notice satisfied the Statute of Frauds).
103. FARNSWORTH, supra note 12, § 6.8.
104. Id. § 6.8 (noting further that “[i]f this test is satisfied, initials or any other symbols will suffice.”).
105. U.C.C. § 1-201(39).
107. Further, U.C.C. Article 5, which governs letters of credit, provides persuasive guidance with respect to the means by which a cyberspace signature could satisfy the Statute of Frauds. U.C.C. § 5-104(2) states that a “telegram may be a sufficient signed writing if it identifies its sender by an authorized authentication [that] . . . may be in code . . . .” Other persuasive guidance can be found in the ABA Model Agreement, which sets forth the following with respect to the signature requirement:

Each party shall adopt as its signature an electronic identification consisting of symbol(s) or code(s) which are to be affixed to or contained in each Document transmitted by such party (Signatures). Each party agrees that any Signature of such party affixed to or contained in any transmitted Documents shall be sufficient to verify such party originated such Document. Neither party shall disclose to any unauthorized person the Signatures of the other party. See SELLING PRODUCTS ONLINE, supra note 89, at 31 citing ABA MODEL AGREEMENT § 1.5. See also STANDARD INTERCHANGE AGREEMENT § 4.1 (providing that “all Messages must identify the sender . . . and must include a means of verifying the authenticity of the Message either through techniques used in the Message itself or by some other means provided for in the Adopted Protocol.”). Id.
technology and similar electronic methods to create “digital signatures” as a means of document authentication, thereby satisfying the writing requirement. Indeed, all that must be shown is an act animated with “intent to identify.” Thus, authenticate means “to sign, execute or adopt a symbol or sound, or encrypt or process a record in whole or part, with intent by the authenticating person to: (A) identify that person; (B) adopt or accept a record or term that contains the authentication or to which a record containing the authentication refers; or (C) attest to the integrity of a record or term that contains the authentication or to which a record containing the authentication refers.” Article 2B further provides that a record or message is authenticated “as a matter of law” if the party complied with a commercially reasonable attribution procedure. “Otherwise, authentication may be proven in any manner, including by showing that a procedure existed by which a party . . . must have engaged in conduct or operations that authenticated the record or term in order to proceed further in the use it made of the information or informational property rights.”

Authentication under Article 2B is very broad. As discussed in Section 5, some states have enacted or proposed “digital signature legislation” that allows authentication by electronic means only if certain procedures are followed. Article 2B would find authentication as long as the authenticating act demonstrates that the party wished to make the record her own. Thus, a signature, a specific type of action requiring a formal intention to be bound, is replaced with a much broader concept. Under traditional contract law, deeds could bind, but a signature was unique. Now that uniqueness has been diluted to some extent.

As broad as the concept of authentication is, it is not as broad as the “manifests assent” concept. Authentication requires action that imparts identification, an act that intimately identifies the person to the record or action taken. The idea of manifesting assent is broader. It includes authentication, as well as other “affirmative conduct or operations that the record conspicuously provides, or the circumstances including the terms of the record clearly indicate, will constitute acceptance, and the person or electronic agent had an opportunity to decline to engage in the conduct or operations.” This is not an identification of a person to act but rather a form of acceptance. Subtle yet significant differences lurk here. As the Reporter’s notes to the definition of “manifests assent” make clear, the “point and click” method of indicating assent to a record or action would be sufficient indicia of a manifestation of assent. Just as the Statute of Frauds today renders arrangements with assent and agreement unenforceable if a signed writing is not present, Article 2B’s Statute of Frauds requires authentication, not mere assent. Authentication is an action that uniquely identifies the person to the deed or record, not just an action that shows assent to the record.

111. Id. § 2B-111(a)(2).
112. Id. § 2B-111, Reporter’s Notes, Illustration 1.

4. Encryption Technology: How Digital Signatures Work

As the Article 2B Reporter notes, “[e]ncryption and other technologically enabled acts are today used to achieve the effects associated with a traditional, written signature.” A digital signature, among other authenticating acts, will work under Article 2B. Current legislation or legislation now in progress has or will affirmatively approve the use of digital signatures. On August 1, 1996, the Science and Technology Section of the American Bar Association published the much-anticipated “Digital Signature Guidelines” (hereinafter, the “ABA Guidelines”). The ABA Guidelines defines a digital signature as:

A transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer’s public key can accurately determine (1) whether the transformation was created using the private key that corresponds to the signer’s public key, and (2) whether the initial message has been altered since the transformation was made.

Digital signature technology developed from an applied mathematics concept known as cryptography. Cryptography is concerned with “transforming messages into seemingly unintelligible forms and back again.” The first step involved in digitally signing a document is the creation of a public-private key pair. The sender uses the “private key” to transform the message into a seemingly unintelligible form; the recipient uses the “public key” to verify the sender’s digital signature by restoring the message to its original form. Generally, the sender should keep the private key confidential, while the public key should be posted where the recipient can access it, such as in an online database or repository.

113. The discussion that follows relies heavily on the ABA GUIDELINES, supra note 70, at 8-16.
114. ARTICLE 2B—APRIL 15, 1998 DRAFT § 2B-102(a), Reporter’s Note 3.
115. The Reporter noted that Article 2B is intended to be technology neutral as to what will be authentication:

Statutes in some states give special recognition to ‘digital signatures’ that rely on a specific encryption technology and a certification or licensing system. The procedures set out in those statutes qualify as authentication for Article 2B. The Article 2B concept is broader, however, and recognizes that technology and commercial practice constantly change and provide many different ways of achieving an authentication.

Id. § 2B-102(a), Reporter’s Note 3.
116. ABA GUIDELINES, supra note 70, § 1.11; see also Smedinghoff, supra note 88, at 20 (stating that “[a] digital signature is not a digitized image of a handwritten signature or a typed signature such as ‘/s/john doe’ . . . . but rather “an electronic substitute for a manual signature . . . . that is created by running an electronic communication through a one-way hash function and then encrypting the resulting message digest with the sender’s private key. It is an unintelligible string of alphanumeric characters.”)
117. See ABA GUIDELINES, supra note 70, at 8.
118. See id. at 8. Computer hardware and software utilizing the public-private key pair are generally referred to as an “asymmetric cryptosystem.”
119. See id. at 8-9. If the asymmetric cryptosystem has been properly designed, it is “computationally infeasible” to derive the private key from knowledge of the public key” despite the fact that the public and private keys are mathematically related.
120. Smedinghoff, supra note 87, at 21.
The digital signature is created when the sender determines the message to be signed and through the use of an algorithm in the sender’s software, known as a hash function, creates a digest of the message. The digest, known as a “hash result,” is equivalent to a fingerprint for the message because it is unique to the message.

Using the sender’s private key, the sender’s software can then convert the hash result into a digital signature unique to both the message and the private key. The sender can then attach the digitally signed hash result and transmit it with the message. Upon receipt of the message, the recipient’s software can compute a new hash result of the original message by using the same hash function used to create the digital signature. Using the public key, the recipient can verify whether the sender created the digital signature using the sender’s private key, since the sender’s public key will only verify a digital signature created by the sender’s private key. Additionally, the new hash result can be compared to the original hash result. If it is identical, then the digitally signed message will be the same as the received message. If the message has been altered in any way, a different hash result will be produced. Thus, the process described above can verify both the message’s authenticity (i.e., it was digitally signed by the sender) and its integrity (i.e., it has not been altered). If the sender’s private key has not been “compromised”, the process can also prevent the sender from denying that it sent the message (known as non-repudiation).

The concept of a “trusted third party” has developed as a means to associate the sender with its public-private key pair. The process described above relies on the critical assumption that the public-private key pair actually belonged to the sender.

The benefits of authenticity and non-repudiation would be lost if the public key used to verify the digital signature belonged to an imposter who created the public-private key pair. One way to counter this problem is by having a trusted third party or “certification authority” verify the identity of the sender. After all, the public-private key pair is merely a set of numbers with no “intrinsic association” with any particular person. The certification authority concept assures the recipient that “a certain public key corresponds to a private key and that the private key belongs to an identified person.” Using a range of procedures to identify the sender, such as credit card identification for routine consumer transactions to producing proof of identification for more complex transactions, the certification authority will issue a digital certificate confirming that the sender identified in the certificate corresponds to a particular public-private key pair.

A number of commercial certification authorities have entered the electronic commerce marketplace and established hierarchies and validation procedures for digital certificates. For example, one commercial certification authority, Verisign, Inc., has established four classes of digital certificates. Class 1 certificates, used primarily for Web browsing and personal e-mail, are issued to individuals only and “confirm that a user’s name and E-mail address form an unambiguous subject within the Verisign repository . . . and establish continuity in the sequence of communication

---

121. ABA GUIDELINES, supra note 70, at 10.
122. See id. at 11.
123. See Smedinghoff, supra note 85, at 22.
124. See id. at 22.
125. See ABA GUIDELINES, supra note 70, at 23.
126. Smedinghoff, supra note 85, at 23.
127. The certificate authority will also create its own public-private key pair to insure the authenticity and integrity of the digital certificate. See Tomlinson, supra note 78, at B12.
128. Id. at B12.
by providing assurances that follow-up communications are from the same user."129

Class 2 certificates, used primarily for “intraorganizational and interorganizational E-
mail, small low-risk transactions, personal E-mail, password replacement, software
validation and online subscription services,” are also issued only to individuals.

These certificates confirm that “the application information provided by the
subscriber does not conflict with information in well-recognized consumer
databases.”130 Class 2 certificates provide “a reasonable but not foolproof assurance”
of a user’s identity by comparing the user’s “name, address and other personal
information on the certificate application against widely referenced databases."131

Class 3 certificates, used primarily for electronic commerce, including electronic
banking, EDI, software validation and membership-based online services, provide
assurance of identity by requiring personal appearance before an independent
validating authority such as a notary public.132 Individuals and private and public
sector organizations may purchase a Class 3 certificate. For organizations, the
certification authority validates the existence and name of the organization, conducts
a review of its authorization records, and makes independent callbacks.133 Class 4
certificates require a significant degree of “independent research and validation” and
currently are not available.134

5. Pending Legislation

Although the ABA Guidelines establish a legal and institutional framework for
applying digital signature technology to electronic commerce, digital signatures are
not yet uniformly recognized throughout the United States. Nevertheless, the impetus
provided by the four year project that culminated in the ABA Guidelines has
influenced a number of states to pass or propose digital signature legislation in efforts
to legitimize the use of electronic contracting technology in online commerce.135

Utah has enacted the most comprehensive legislation to date.136 Passed in 1995
and amended in 1996, the Utah Digital Signature Act (“Utah Act”) was the first
legislation of its kind enacted in the United States. It sets forth a comprehensive
effort to “facilitate commerce by means of reliable electronic messages.”137 Modeled
after the ABA Guidelines, the Utah Act, in addition to setting forth a comprehensive
regulatory regime complete with a licensing mechanism for certification authorities,

129. See VERISIGN TM CERTIFICATION PRACTICE STATEMENT IN SUPPORT OF VERISIGN’S
PUBLIC CERTIFICATION SERVICES CLASS 1-3 DIGITAL IDS SM CERTIFICATES VERSION 1.1,
§ 2.2.1 (1996).
130. See id. § 2.2.2.
131. Id.
132. See id. § 2.2.3.
133. See Tomlinson, supra note 78, at B12.
134. See id.
135. Prior to the publishing of the final version of the ABA GUIDELINES in August 1996, a
draft version was widely distributed, and both the final version and the draft version have been
influential in promoting the development of a legal and institutional framework for electronic
commerce on both a national and international level. See RICHARD L. FIELD, DIGITAL
SIGNATURES: VERIFYING INTERNET BUSINESS TRANSACTIONS, 17th Annual Institute on
137. Id. § 46-3-102.
establishes a technology specific approach. This approach specifies the use of asymmetric cryptosystems (a “public key/private key” system) as part of its definition of digital signature. Specifically, under Utah’s (and the ABA’s) per se rules, the use of a digital signature in conjunction with a licensed certification authority results in the signature and text of an electronic message being deemed to constitute a signature, a writing, an original of the document, and an acknowledged writing or signature under applicable law. Choosing the public-private key infrastructure as the “approved” digital signature form seems safe, for it is generally thought that this method provides security and confidentiality for electronic transactions.

Specificity has its advantages. One chief advantage of a technology specific statute is that it sets forth a “bright line test” for achieving the benefits of compliance. In theory, commerce is enhanced because compliance yields certain legal results; the parties to the transaction benefit from that same certainty if their transactions comport with the requirements of the Utah Act.

Other states and the proposed Uniform Electronic Transactions Act take different approaches in that they do not specify any particular technology. Naturally, there are policy concerns about whether state legislatures are adequately informed about this issue and whether the specification of one particular technology now could impede the development of future technologies. Thus, the proposed Uniform Electronic Transactions Act, following Article 2B’s lead, adopts a “technology neutral” approach by broadly defining the term “electronic signature” and then by providing that if “a rule of law requires a signature, or provides consequences in the absence of a signature, that rule of law is satisfied with respect to an electronic record if the electronic record includes an electronic signature.”

Some states, such as Georgia and Texas, have gone the minimalist route by proposing legislation that would establish the legal sufficiency of electronic records, while deferring a more comprehensive regulatory effort until the movement toward electronic commerce has been studied in greater detail. The advantage of this technology neutral approach

---

139. The Utah Act defines a digital signature as the “transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer’s public key can accurately determine whether: (a) the transformation was created using the private key that corresponds to the signer’s public key; and (b) the message has been altered since the transformation was made.” § 46-3-103(10).
140. Similar to the ABA GUIDELINES, the Utah Act establishes a system of licensed certification authorities that can issue, control and certify keys for the public key encryption system adopted by the Utah Act. The principle role of the certification authority is to issue and maintain the security and accuracy of the public-private key system.
141. UTAH ACT §§ 46-3-401 to 46-3-405.
142. UNIFORM ELECTRONIC TRANSACTIONS ACT—MARCH 23, 1998 DRAFT § 301. “Electronic signature” is defined as “any signature in electronic form, attached to or logically associated with an electronic record.” Id. § 102(a)(8). “Signature” is defined, similar to Article 2B’s definition of “authenticate,” as “any symbol, sound, process, or encryption of a record in whole or in part, executed or adopted by a person or the person’s electronic agent with intent to: (A) identify that person; (B) adopt or accept a term or a record; or (C) establish the informational integrity of a record or term that contains the signature or to which a record containing the signature refers.” Id. § 102(a)(20).
Contracting in Cyberspace

(i.e., one that does not specify any particular technology), as opposed to the technology-specific regime established by the Utah Act, is the flexibility that technological neutrality provides, particularly in light of the rapidity with which technology changes.

As an example of the minimalist approach, the draft Georgia Electronic Records and Signatures Act ("Georgia Act"), rather than establishing an ABA Guideline-type regulatory framework, proposes to create an "Electronic Commerce Study Committee" to look further into issues raised by electronic records and signatures.\footnote{Georgia Act.} Additionally, the Georgia Act broadly defines the term "electronic signature"\footnote{Georgia Act.} in a technologically neutral manner to mean:

an electronic record or digital method executed or adopted by a party with the intent to be bound by or to authenticate a record, which is unique to the person using it, is capable of verification, is under the sole control of the person using it, and is linked to data in such a manner that if the data are changed the electronic signature is invalidated.\footnote{Georgia Act.}

Texas appears to have taken the minimalist approach one step further. Two bills on electronic contracting were introduced in 1997 before the 75th session of the Texas Legislature. One of the bills,\footnote{House Bill 306.} H.B. 984, was enacted and is similar to the Georgia Act in that it recognizes the legitimacy of electronic contracting, but does not establish a comprehensive regulatory framework along the lines of the ABA Guidelines. It amends Section 2.108 of the Texas Business and Commerce Code to read as follows:

[a] written electronic communication sent from within or received in this state in connection with a transaction governed by this chapter is considered signed if a digital signature is transmitted with the communication.\footnote{Section 1, Texas H.B. 984.}
Furthermore, the bill rather broadly defines a digital signature as “an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature.”

A detailed review and analysis of the various digital signature laws that have been proposed or enacted is beyond the scope of this paper. Rather, the foregoing discussion is intended to highlight the fact that lawmakers considering digital signature legislation specifically, and electronic contracting legislation generally, will have important policy decisions to confront. In addition to the policy choice between “technology-specific” and “technology-neutral” approaches, other cyberspace contracting policy issues that lawmakers undoubtedly will face in the near future include: the desirability of uniformity among the laws of the various states as well as international law, the desirability of consumer protection mechanisms, allocation of liability among the parties to an electronic transaction, the scope of liability that a certification authority should be exposed to, and state regulatory and quality control issues relating to the licensing of certification authorities.

E. Conclusion

Regardless of which policy choices are made, refinements in digital encryption technology address one of the difficulties with the fiction with which we began Part II. To impart some order to cyberspace contracting, lawyers and cyberspace merchants grasped for pen and ink analogues, resorting to the fiction that electronic commerce is paper commerce. Though useful, this fiction does not cure all of the myriad difficulties that arise in cyberspace contracting.

The law has formulated few fixes to make the fiction work. An example of this is the problem of electronic agents. While traditional commerce transpires in faceless encounters through agents, until recently the law did not need to face the prospect of agents that were nothing more than a set of instructions. Our notions of agency imply human judgment. The fix here is to acknowledge the electronic agency, and to attempt to limit the range of its action. Similarly, while the method of forming contracts may still occur through offer and acceptance, the method of forming contracts electronically requires the assistance of a few special rules, such as a


149. Id.
150. For a comprehensive online summary of digital signature legislation see <http://www.mbc.com/legis/>.
151. Rumors have circulated that Congress is considering digital signature legislation in order to insure uniformity. See MASSACHUSETTS CONDUCTS POLL ON FEDERAL/STATE DIGITAL SIGNATURE ISSUES, BUREAU OF NATIONAL AFFAIRS ELECTRONIC INFORMATION POLICY & LAW REPORT, 534-535 (May 23, 1997)[hereinafter “Digital Signature Poll”] available at <http://www.magnet.state.ma.us/itd/legal/survey1.html> (noting that in response to such rumors, the Information Technology Division of the Commonwealth of Massachusetts is “conducting an informal survey on how future policies and laws for digital and electronic signatures should evolve.”).
152. For example, should certification authorities be licensed to insure quality control? If so, should licensing be done at the state level? Do states possess the technological and budgetary means to oversee a licensing and registration infrastructure for certification authorities or should this be done through an accreditation process?
reversal of the mailbox rule. Thus, the fiction works for most authority and method of formation problems.

However, the fiction is under great pressure when it comes to authentication issues. If the matter involved merely tinkering with the Statute of Frauds to make electronic contracts the equivalents of written contracts, the difficulties would be small. After all, the Statute of Frauds has proven to be porous. However, the problem is far deeper. The specter of frauds and the possibility of forgery and deceit plague all commerce. Nonetheless, while someone can forge a signature, one can prove that one’s hand did or did not adopt a writing. A signature is uniquely a reflection of human intention. Nothing makes electronic signatures that personal or unique. They are nothing but a series of electronic signals. Great pains have been taken to formulate methods for fashioning unique sequences of signals that will reduce some of the risks of misappropriation. In some cases, that means making the digital signatures unique to a but to a particular situation, not to an “individual”, albeit in a way that identifies the actor uniquely to the situation.

Agreements have handled many of the authentication problems. Parties accede to procedures for identification, and presumably the trust that prompts them to contract in the first place allows them to accept electronic messages. Contracting dispels, or at least reduces, concerns about accepting electronic messages. Not until digital signatures become the functional equivalent of human signatures do the issues of authentication become stark.

III. PAYMENT SYSTEMS

Online payments from consumer to merchant and from merchant to merchant can occur in many forms, including credit cards, electronic checks, digital cash and electronic funds transfers. The use of credit cards to make online payments is already common, and various types of credit card payment systems have developed. The first “early” method – transmission of credit card information by buyer to seller over an “unsecure” server – became less frequent when modern Web browsers became equipped to handle transmission of encrypted information over secure servers. The security risks associated with transmission of credit card information over the Internet are obvious. Buyer is concerned about the integrity of an online vendor who may have no physical place of business. Similarly, seller is concerned that buyer is really an authorized user of the credit card. Both parties are concerned with nonrefutability, i.e., that neither party will deny engaging in the transaction.

Due to such security risks, two more reliable forms of credit card payment systems have evolved, each relying on variations of the digital signature technology discussed above. Secure credit card payment relies on public-key cryptography to encode sensitive data such as credit card numbers. The payment transmission is then digitally signed to insure its authenticity. The other payment system, registry credit card payment, combines digital signature technology with the concept of a “trusted third party” to facilitate the online payment process. Under this approach, a group of sellers affiliates with a third party who is responsible for servicing credit card payments. Buyers then register their credit card information with the trusted third party and receive an identification number for making purchases. In light of certain inherent limitations associated with credit card use, such as the lack of anonymity, payment limits, and the impracticality of using credit cards for low-value transactions, these systems offer a valuable alternative for online commerce.

---

153. Contrast with the concept of “manifests assent.”
transactions, and payment limits, credit cards may not be the preferred payment method for certain transactions, including very small or very large transactions.

As a result, electronic checks and digital cash have developed as alternate methods of effectuating electronic payments, particularly with respect to small-scale consumer-related and merchant-to-merchant transactions. Electronic checks function much the same way as their real world counterparts: the check authorizes the transfer of account balances from the account against which the check is drawn to the account to which it is deposited. The key difference is that the check and all information included on it would exist in an electronic format and could be transmitted electronically via e-mail or other network protocols to initiate payment. Also, like paper checks, electronic checks do not guarantee that the account contains sufficient funds; if the account contains insufficient funds, the electronic check, like its real world counterpart, will bounce.

Digital cash is the ideal method of electronic payment for low-value transactions. The nominal associated transaction costs make digital cash well suited for such transactions. Banks usually issue digital cash, digitally signed with the issuing bank’s private key and represented by an electronic token of some sort that can be downloaded from a user’s bank account and stored on a “smart card” or in a cyber-wallet. One of the key advantages to digital cash is that it can be anonymous, meaning that—like paper money—consumers can spend it in a generally untraceable manner. Digital cash also facilitates non-merchant commerce since none of the parties to the transaction needs to register with a credit card issuer.

However, none of the payment systems described above seems particularly well suited for large-scale trading partner type transactions. Each has its own limitations: credit cards may have spending limits, electronic checks do not provide a guarantee of payment, and digital cash is better suited for small-scale transactions. Perhaps the

155. Id.
156. Id.
157. Id. § 7.5.1.
158. Id. § 7.5.2.
159. Id. At least two alternative registry credit card payment systems have been developed, one by First Virtual Holdings, Inc. and the other by CyberCash, Inc. Under the First Virtual approach, buyer’s credit card information is stored on a secure computer system and is never transmitted over the Internet. Rather, when buyer wants to make an electronic purchase he or she merely supplies the identification number issued by First Virtual to seller, who then transmits the information to First Virtual in order to initiate the payment process. Somewhat differently, under the CyberCash approach, buyers use free software supplied by CyberCash to encrypt their own credit card information. Buyer then transmits this encrypted information to seller when buyer decides to make a purchase. Seller in turn transmits the information to CyberCash to initiate the payment process. Id.
160. Id. § 7.6.
161. Id.
162. Digital cash is simply an electronic way to store value that is the electronic equivalent of money. Id. § 7.7.
163. SMEDINGHOFF, supra note 154, § 7.7.
164. Id. Some forms of digital cash may include information about the identity of the person who originally withdrew it from the bank account, thereby making it “identifiable.” Id.
165. Id. § 7.7.
166. This is not to say, however, that these methods could not be successfully implemented in an online trading partner situation. Rather, each of these methods seems better suited for consumer transactions and lower-scale merchant-to-merchant transactions.
most practical method of online payment for trading partners is “financial EDI,” a combination of electronic funds transfers (“EFTs”) and EDI.\textsuperscript{167} Two essential components comprise financial EDI: (1) a payment of funds electronically destined for the seller’s bank, and (2) an electronic remittance of information associated with the payment, electronically destined for processing with seller’s accounts receivable information.\textsuperscript{168} The buyer can transmit remittance information electronically by combining it with a payment order so that the information transfers through the funds-transfer system to seller’s bank; or, the buyer can transmit remittance information separately, either directly from buyer to seller, or from buyer through a third-party intermediary to seller.\textsuperscript{169} However, many EDI transactions do not follow the foregoing paradigm. Rather, EDI transactions between established trading partners commonly consummate in the same manner as non-electronic transactions between regular trading partners: the seller provides the product or service on credit, sends invoices on a regular basis, and the buyer pays by check or wire transfer.\textsuperscript{170} The financial EDI paradigm can be useful, though, in situations in which the parties to the transaction have had few prior commercial dealings.

A brief discussion of electronic funds transfers facilitates a full understanding of the financial EDI paradigm. EFT involves the electronic movement of funds from one bank account to another pursuant to electronically communicated payment instructions.\textsuperscript{171} Generally, two types of electronic funds transfers exist: (1) credit transfers, which occur when a buyer instructs its bank to transfer funds to the seller’s bank, and (2) debit transfers, which occur when a seller instructs its bank to collect funds for it by debiting the buyer’s bank account.\textsuperscript{172} A typical credit transfer involves the following participants: (1) the originator of the payment, (2) the originator’s bank, (3) a funds-transfer system, (4) the beneficiary of the payment, and (5) the beneficiary’s bank. The originator initiates a credit transfer by sending a payment order to the originator’s bank, instructing the bank to pay the beneficiary by depositing funds into the beneficiary’s bank account.

Various funds-transfer systems for effecting electronic payments exist in the United States. Perhaps the most popular is the Automated Clearing House (“ACH”), a nationwide electronic payments system used by thousands of financial institutions and corporations and millions of consumers. It is the primary system used for consumer debit transfers. The Federal Reserve Banks own and operate Fedwire, another funds-transfer system. The twelve New York money center banks comprising the New York Clearing House Association own and operate the Clearing House Interbank Payments System (“CHIPS”), used primarily for processing international funds transfers among its members. Finally, there is the Society for Worldwide Interbank Financial Telecommunications (“S.W.I.F.T.”), a messaging system operated by a consortium of over 1700 banks in more than 80 countries. S.W.I.F.T. is a communications system that facilitates the communication of payment orders and other messages among its members. It is important to note the key difference between S.W.I.F.T. and the other funds transfer systems discussed above. S.W.I.F.T.
is not a settlement system: after payment orders have been communicated to member
banks, settlements are executed through Fedwire, CHIPS, or other means.

IV. CHOICE OF LAW AND JURISDICTION

A.  Overview

Conflict of law and jurisdictional principles arose precisely because persons of
different states dealt across national boundaries. Recalling that we began this paper
with a comparison of the law merchant to cyberspace law merchant. We noted that the
lex mercatoria became a sort of transnational law. Commercial courts and their
merchants operated with a general set of principles, somewhat loosely defined, and
sought to enforce as principles in whatever court they found themselves. They
needed to know that their contracts and arrangements would be given effect wherever
they traded. The need in cyberspace commerce is no less; and perhaps is more acute
because of the access now available to all types of merchants, large and small, across
national boundaries on an instantaneous or near instantaneous basis. Almost any
business literally can now trade anywhere.

This recent virtual ubiquity raises just as many jurisdictional problems as it does
dChoice of law problems. Personal jurisdiction has long been conceived of in
geographic terms. Personal jurisdiction is “the power of a court over the person of the
defendant,” and this power has long been found dependent upon actual physical
presence in a jurisdiction or “doing business in that jurisdiction.” Something must
happen in a geographical area that the court could point to as justifying its exercise of
power over the person. Now it is not so clear where this “something” occurs. A
person can create a web page in the United States, never set foot in France, and never
send anything to France, but nonetheless run afoul of a French law requiring works
appearing in France to appear in the French language.175 The technological wizardry
that allows the linking of web pages may very well bring the host of a web page
“into” a jurisdiction merely because his page links to another page.

B.  Choice of Law Issues

Unfortunately, general choices of law principles are in a mess. Different courts
and different states employ different rules. Various choice of law scholars advance
starkly different theories that would lead to dramatically different results. In certain
areas, legislators have tailored specific rules to govern discrete, narrow sets of
transactions and activities. Fortunately for our purposes here, we need to delve into
only the choice of law issues relating to consensual contractual arrangements. Even
then, however, the number of principles that one can invoke in a cyberspace
contracting situation is numerous.

175. In one recent incident, the Georgia Institute of Technology maintained a web page that
contained information concerning the school’s French programs. Two private associations in
France filed a complaint against a school in France with which Georgia Tech was affiliated,
based on the school’s failure to display a French translation. See <http://gtl.georgiatech-
metz.fr/>.

According to Professor Brilmayer, choices of law theories attempt to answer one deviously simple, but complex question: on what basis does a court choose one state’s law over another?

Choice of law theory vacillates erratically between two different answers to this question of proper prospective. One tradition is unabashedly *a priori*; it locates the source of choice of law principles in some normative system external to and more important than the authority of any particular state. . . . The other, internal tradition avoids the problem of authoritative source by treating the choice of law issue as turning on the forum state’s local law. . . . It asks merely whether the authoritative laws of the forum state . . . purport to apply to the case at hand.176

The law merchant would choose an external choice of law perspective.177 As evidenced by current uniform acts and statutes and the common modes of contracting cyberspace merchants have adopted in the absence of uniform laws, the groping towards a somewhat loosely structured set of laws transcending the laws of any given state becomes apparent.

In any event, none of the choice of law approaches currently in vogue is completely immune to the external or internal theories, but rather they mix the two in an uneasy balance. The *Restatement (First) Conflicts of Law* tips the balance towards the external approach, while the *Restatement (Second) Conflicts of Law* tips the balance toward the internal approach. According to recent studies, portions of one or the other of the *Restatements* apply in thirty-nine or more states.178 This section discusses the different approaches of these two Restatements, the choice of law provisions in the Uniform Commercial Code and Article 2B.

1. Restatement Approaches

a. *Restatement (First) Conflicts of Law*

The *Restatement (First) Conflicts of Law* embraces a “vested rights” theory in combination with a general external law approach, with a minor view of the internal theory. The concept behind the *Restatement (First) Conflicts of Law* was the division of law into individual states’ laws and general common law. Under general common law, events and interests gave rise to legal rights and, through the application of general legal rules, they transformed into various specific obligations between parties. “Upon the occurrence of such events . . . the legal rights of the parties then vested.”179 Once vested, the issue became *where* they vested. The *Restatement* embraced a “last act doctrine.”180 Under this doctrine, the rights vested at the place where the last act occurred that was necessary to complete the cause of action.”181 Where the rights

176. BRILMAYER, supra note 173, at 2.
177. Indeed, judges enforcing or recognizing the law merchant in the early centuries of this millennium referred to the law merchant as a law that applied as a form of natural law, that overrode contrary local law, at least to the extent of merchant transactions. HAROLD J. BERMAN, LAW AND REVOLUTION, 333 (1983).
179. BRILMAYER, supra note 173, at 19.
180. Id. at 21.
181. Id.
vested, various events and relationships coalesced to create an obligation in a particular geographic state; the laws of that particular state applied, and the other states were bound to respect the choice of that state’s laws.\(^{182}\)

Accordingly, the *Restatement (First)* set out a number of rules to determine where rights vested. For contractual validity issues (consideration and capacity), the vesting depended upon the location where the parties made the contract.\(^{183}\) The parties formed the contract where “the principal event necessary to make the contract occur[red],”\(^{184}\) which varied according to the type of contract involved and whether the contracting occurred face to face or over long distances. The *Restatement (First)* enshrined the mailbox rule, with the promise becoming effective upon dispatch.\(^{185}\)

In dealing with performance issues, the *Restatement (First)* made the touchstone the place where performance occurred or was supposed to occur.\(^{186}\) Florida conflict of law principles would govern a contract “formed” between two parties face to face in Florida; however, if performance under the contract occurred in Texas, Texas law would apply as to the performance issues. Obviously, much mischief and confusion can occur under the *Restatement (First)* approach, for validity blends into performance. Deciphering these issues becomes extremely difficult.

b. *Restatement (Second) Conflicts of Law*

The *Restatement (Second)* mixes the internal and external theories discussed above, with an emphasis on the internal theory. It takes the vantage point of the forum deciding the dispute, with the court looking outwardly to determine which state may have a greater interest in resolving the controversy.\(^{187}\) This approach allows a court deciding the dispute to look at the interests of the involved states and to take into account considerations such as interstate harmony and predictability.\(^{188}\)

However, the *Restatement (Second)* relates back to the *Restatement (First)* by articulating specific rules for specific categories of law, and specific types of events or arrangements. Within these categories and types, the *Restatement (Second)* sets up presumptions that would apply in the absence of some compelling reason to look to the more general interest calculus. For example, service arrangements are governed “by the local law of the state where the contract requires that the services, or a major portion of the services be rendered, unless . . . some other state has a more significant relationship.”\(^{189}\) In those instances, the court will apply the local law of the other state.

One can see a blend of the old and the new: the place of performance is presumptively valid, but a court may choose instead to rely on general interest analysis. In cyberspace contracting, this could lead to wildly different results. Consider an example:

\(^{182}\) Id.

\(^{183}\) RESTATEMENT (FIRST) CONFLICTS OF LAW § 332.

\(^{184}\) Id. § 311 Comment D.

\(^{185}\) RESTATEMENT (FIRST) CONFLICTS OF LAW § 326.

\(^{186}\) Id. § 358.

\(^{187}\) See RESTATEMENT (SECOND) CONFLICTS OF LAW §§ 6, 188 (cataloguing the multiple factors that a court would consider in deciding the most appropriate forum, including the place of contracting, the place of performance, the location of the subject matter of the contract, where the contract was negotiated, the relevant policies of the forum, the residency (or state of incorporation) of the parties, and the policies underlying the field of law in issue).

\(^{188}\) BRILMAYER, supra note 173, at 67.

\(^{189}\) RESTATEMENT (SECOND) CONFLICTS OF LAW § 196.
A licensor maintains offices in Texas and California, with its computer development group in New York. It licenses a software product developed in New York, through its sales office in California, to a Utah-based licensee, to provide information services to the licensee’s executives. The parties create the contract electronically between the licensor’s and the licensee’s main offices, but an MIS employee of the licensee accesses and downloads information from the licensor while vacationing in Mississippi, a state in which the licensee does not have an office.

A “most significant” relationship analysis under the *Restatement (Second’s)* approach clearly could yield almost any result.

c. U.C.C. Approaches

As a general rule, Article 2 currently leaves choice of law issues to Article 1.*190* Article 1 somewhat weakly echoes the general concept of the *Restatement (Second) of Contracts*, except where the U.C.C. otherwise specifically provides:*191* When a transaction bears a reasonable relation to this state and also to another state or nation the parties may agree that the law of either this state or such other state nation shall govern their rights and duties. Failing such agreement this Act applies to a transaction bearing an appropriate relation to this state.*192* Parties are given the first choice as long as they are reasonable in making the choice. The choice must have some reasonable relation to the transaction. Interestingly, the U.C.C. takes the internal approach to an extreme, with a twist: if the parties fail to agree, the forum state’s U.C.C. applies to all transactions bearing “an appropriate relation” to the forum. In other words, one looks at the forum’s law and applies it whenever appropriate.

d. Article 2B

Proposed Article 2B begins by flatly validating all contractual choice of law terms.*193* The Reporter’s notes make clear that this breathtaking validation of contractual choice would give way to laws limiting such terms based on policy grounds.*194* But generally, the choice by contract will be given effect. The party need not satisfy any reasonableness test, nor must he select the laws of a state having any relationship whatsoever to the transaction. If somehow the parties neglect to address the choice of law by contract, then Article 2B reluctantly fixes the law for them:

- As to a *consumer* contract requiring delivery of a copy to the consumer other than through electronic communication, the law of

---

*190. But see U.C.C. § 2-402.

191. U.C.C. § 1-105(2). Even when the U.C.C. specifically directs the application of a law, the parties can vary that mandated selection—but “only to the extent permitted by the law (including the conflict of laws rules) so specified.” Id. This limits the laws that may be chosen where the U.C.C. is specific—a very rare event.

192. Id. § 1-105(1). Article 2A has some specific rules, as do other Articles of the U.C.C. (e.g., Article 9 as to perfection).


194. Id. § 2B-107, Reporter’s note 2.
the state in which the copy is located when the consumer receives physical possession of the copy (or where receipt was to have occurred) governs the contract. The theory supporting this rule is that both parties probably will be aware of the point of delivery or receipt, and that each will expect the law of that state to govern. However, a specific contract provision can alter that choice.

- As to online services “or delivery of a copy by electronic communication,” Article 2B selects the law of the licensor’s location. Theoretically, the licensor does business in all states where it makes its information available; therefore, the licensor has the burdensome obligation of complying with the law of all states where it does business. Thus, in transactions where a vendor makes digital information generally available, no single state can have a significant relation to the transaction other than the licensor’s state.

Finally, if the arrangement does not fall into the preceding categories, “the contract is governed by the law of the jurisdiction with the most significant relationship to the contract.” However, if the parties have not contractually chosen a law, and the choice by operation of these rules leads to a selection of a non-U.S. law, Article 2B suddenly becomes protective. For the law of the non-U.S. jurisdiction to apply, that law must “provide substantially similar protections and rights to a party not located in that jurisdiction as are provided under [Article 2B].”

2. Conclusion to Choice of Law Issues

With so much confusion in applying the proper principles, we recommend that parties specify their choice of law in any electronic contract. Whether the parties form the contract through a web transaction or not, we generally take the view that one should specify the law. Even that may not be enough in all cases, for it does not take into account that different parts of a contract, or a series of related contracts, may have the validity of their choice of law provisions gauged by different measures. Thus, the choice of law principles relating to a sale or lease of goods that happens to take electronic form may be governed by a choice of law rule different from the one applying to information contracts. The U.C.C. may very well make the outcome depend on the type of transaction in terms of legal categories.

C. Jurisdiction

1. General Jurisdictional Principles

The body of law relating to jurisdiction over those who host a web site (or engage in other Internet commerce) is no more definite than the cyberspace choice of law principles. Here, we speak of the power of any court given to exercise personal jurisdiction.

---

195. Id. § 2B-107(b)(2).
196. Id. § 2B-108(b)(1); see also Reporter’s note 3.
197. Id. § 2B-107(b)(1).
198. Id. § 2B-107(c).
jurisdiction over the web site host. 199 When a web site host creates and maintains a site offering or advertising goods or services, the site theoretically offers or advertises to anyone with the means to visit the site. Therefore, even the smallest of businesses could conduct some form of business internationally.

The international jurisdictional standards are in complete disarray. Presently, only anecdotal evidence indicates that some courts have exercised, or threatened to exercise, authority over web site hosts maintaining sites violating their local laws. For example, the Singapore Broadcasting Authority has the power to regulate Internet content. Various web site operators must register their sites with the Singapore Broadcasting Authority. Allegedly, this board has ordered at least one web site to shut down for posting offensive jokes. 200 In another example, a United States law school professor, and other persons in Canada and Germany, were threatened with a UK copyright infringement action for posting reports describing alleged child abuse by social workers in England. 201 We could advance several other reported incidents of similar threats to enforce the claims against a web site host, but most of the “international” Internet jurisdictional controversies involve actions by authorities or persons against someone physically located in their jurisdiction. When a complaint brought in France alleged that Georgia Tech violated French law by maintaining an English-only advertisement for French courses offered at an affiliated school in France, the French action was formally instituted against the French school, as opposed to Georgia Tech. We will not see how international Internet jurisdictional issues will be governed until a court enters a judgment in one country against a web site host located in another country.

For our purposes, we will focus on jurisdictional cases in the United States. Courts have decided a number of cases since early 1996, creating a body of law that has at least the beginning of identifiable trends. The United States Constitution circumscribes the personal jurisdiction of a state or federal court by the “due process clauses.” Due process requires a court to exercise personal jurisdiction over only those defendants having “minimum contacts” with the forum so that “the maintenance of the suit does not offend ‘traditional notions of fair play and substantial justice.’” 202 The minimum contacts must be of a quality that the defendant should reasonably anticipate being brought into a court in the jurisdiction. This means that somehow the defendant must have purposely availed herself of the forum state and that the exercise of the jurisdictional power would otherwise be reasonable under the circumstances. 203 Blended into this analysis is a second limitation that “traditional notions of fair play and substantial justice” must not be offended. Courts must weigh the burden on the defendant of allowing a suit to be maintained in the forum state, the forum’s interest in adjudicating the dispute, the plaintiff’s interest in securing relief in a convenient forum, the judicial system’s interest in resolving interstate controversies efficiently, and the shared interest of the various affected states in furthering substantive policies. 204

199. We do not here address the subject matter jurisdiction of various courts, obviously. Subject matter jurisdiction is an issue peculiar to individual courts. At this juncture we wish merely to treat the deeper question of whether a court has power to render a judgment that would be enforceable against someone assuming that it had subject matter jurisdiction.
201. See <http://samsara.law.crwu.edu/comp1law/injunct.html>.
204. WorldWide Volkswagen, 444 U.S. at 292-93.
Based on these general principles, two types of personal jurisdiction exist. One is general personal jurisdiction based on a defendant’s presence through “continuous and systematic” activities, even if unrelated to the cause of action. This allows a court to exercise jurisdiction in any lawsuit for actions inside or outside of the forum. The second type of personal jurisdiction, “specific” personal jurisdiction, allows a court to exercise authority over a defendant who is not present in a forum concerning claims or actions arising out of or relating to a defendant’s activities in the forum. Here the courts focus on “the relationship among the defendant, the forum and the litigation.” This latter form of personal jurisdiction is of interest as it relates to web use. If the web site host is physically not in a state, or has not otherwise conducted systematic and continuous activities in that state, the “purposeful availment” element of minimum context tests apply. Clearly, the defendant’s conduct does not have to occur in the jurisdiction for the defendant to purposely avail himself of the jurisdiction. The issue is the purposefulness and intent of the availment. The Supreme Court’s deeply divided views on the subject have clouded the issue.

2. Internet Jurisdiction Cases

Many of the recently decided Internet jurisdiction cases fit within traditional jurisdictional principles: the defendant transacted business with persons in the forum state over the Internet, sending goods, transmitting software, or performing services intended to be used or delivered in the forum state. Other decisions involve web sites accessible to users in forum states, but where the web site holder did not actually transact business with persons in the forum states. These cases involved “passive” web sites, where the web host only advertised its goods or services. The final set of cases related to so-called “interactive” web sites involve users who obtain and transmit information via the web site. Once again, in these cases the parties did not actually transact any independent business, and did not ship goods or services, other than the exchange of information.

An example of the first type of case is CompuServe, Inc. v. Patterson. This case involved a Texas resident who provided software to CompuServe, an online provider located in Ohio. CompuServe promoted the distribution of Patterson’s software in exchange for a percentage of sales. Patterson and CompuServe essentially contracted all business electronically; Patterson, however, transmitted thirty-two software files to CompuServe in Ohio. Later, CompuServe began distributing competing software and sought a declaratory judgment stating that CompuServe’s software did not infringe on Patterson’s trademarks. When Patterson challenged the Ohio court’s ability to exercise personal jurisdiction over him, the district court dismissed the case because only six hundred-fifty dollars worth of software had been sold to individuals in Ohio. The Sixth Circuit reversed the district court, despite the contacts with the forum state being essentially only electronic.

207. Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102 (1987). The Supreme Court found that a product liability suit could not be maintained in California against a Japanese manufacturer that sold the allegedly defective product to a company in Taiwan. Justice O’Connor’s plurality opinion found a purposeful availment of the benefits of the laws of the state required more than merely placing goods into the stream of commerce; in addition there must be conduct indicating the deliberate intention or purpose to transact business there. Justice Brennan’s concurring opinion took a decidedly more expansive view of intention.
208. 89 F.3d 1257 (6th Cir. 1996).
Patterson had entered into a written contract designating Ohio law and listing CompuServe as the exclusive advertising and distributing agent. Additionally, Patterson obtained at least some benefits from his relationship with CompuServe, and he was the one who threatened an infringement suit.

The second set of cases, involving passive web sites, has created a split between courts. In *Inset Systems, Inc. v. Instruction Set, Inc.*, Patterson claimed that Instruction Set had infringed its “Inset” trademark by using “inset” in Instruction Set’s domain name and telephone number. The plaintiffs brought suit in Connecticut; however, Instruction Set never had employees or offices in Connecticut and did not conduct business in Connecticut, other than advertising over the Internet. With the most cursory analysis, the district court held that because Instruction Set had made its advertising continuously available over the Internet to thousands of users, including those in Connecticut, and offered a toll-free number for the customers to use, it availed itself in Connecticut, with sufficient purpose. The court essentially believed that any advertising over the Internet provided sufficient minimum contacts everywhere.

This case closely relates to cases involving domain name bandits, which are responsible for most of the cases discussing jurisdictional issues. *Panavision Int’l v. Toeppen* illustrates this. Toeppen, an Illinois resident, appropriated “Panavision” as his Internet domain name, cleverly establishing a web site to display aerial photographs of Pana, Illinois. The court maintained that it had personal jurisdiction in California because the infringement of the famous Panavision marks was the equivalent of a tort claim; Toeppen knew that the infringing acts would harm Panavision in California since California was Panavision’s principal place of business. The court found that Toeppen intended to reach out to California because his out-of-state activities intended to harm Panavision in California. Toeppen’s nefarious activity as a “cybersquatter” demonstrably moved the court.

A contrasting line of cases follows *Bensusan Restaurant Corp. v. King*. Bensusan, owner of “The Blue Note” Club in New York, instituted an infringement action in New York against a Missouri resident operating a restaurant under the name “The Blue Note.” The Missouri resident operated a web site to advertise musical performances at his Missouri restaurant. Web site visitors could obtain information about shows and ticket prices and purchase tickets over the phone; however, they had to travel to Missouri to claim the tickets. The web site had no password protection and continuously advertised nationwide. The defendant even provided a hyperlink to the plaintiff’s web sites. The defendant had no other contacts with the State of New York.

This case and *Hurst Corp. v. Goldberger* reached the constitutional due process issue on alternative grounds, though clearly influenced by the preceding cases. *Goldberger* court held that the New York long-arm statute did not give New York jurisdiction for the trademark infringement. The court held that the infringement could occur only where the passing off occurs for the purposes of the New York long-arm statute. The court seemed to think of the web site as “existing” primarily in Missouri, and not as offering products or services in New York. Indeed,
most of the users’ activity, if they really wanted to purchase something, would have to
occur in Missouri. They would have to call Missouri for tickets, as well as travel to
Missouri to claim the tickets and enjoy the performance. These facts also led the
court to state that due process could compel dismissal even if the New York long-arm
statute did apply.  

Among the most difficult cases are those involving “interactive” web sites, such as Maritz, Inc. v. CyberGold, Inc. CyberGold’s web site server was located in
California. Its web site advertised a service where it would e-mail advertisements
tailored to each customer’s particular areas of interest. One hundred thirty-one
subscribers resided in Missouri. The plaintiff sued in Missouri, claiming that the
defendant’s Internet activities under “CyberGold” infringed his trademarks. The
court held that the commission of a tortious act occurred outside the state, but caused
economic harm in Missouri, thereby allowing the Missouri long-arm statute to
apply. Since CyberGold had attempted to reach a global audience, anticipating that
users would access the web site and sign the site’s mailing list, and actively solicited
everyone worldwide to sign the mailing list, CyberGold had sufficient qualitative and
quantitative contacts in Missouri. CyberGold’s one hundred thirty-one transmissions
into Missouri purposefully availed CyberGold to the Missouri courts. Moreover, the
trademark infringement caused harm in Missouri, and certainly Missouri had an
interest in protecting against infringement of its state marks.

3. Conclusion to Internet Jurisdiction

Most of these cases are recent, and more will pass before the lines of authority
solidify. Moreover, most of the Internet jurisdictional cases involve infringement—
most commonly trademark infringement. They do not implicate, as such, commercial
practice. Only when electronic transactions become the norm, and the stakes grow
large, will we see jurisdictional principles fitted to commercial contracts. By then,
provisions such as those in proposed Article 2B that broadly embrace choice of forum
clauses should be in effect. Given the uncertainty of jurisdictional cases, parties
should contractually choose a forum. This may not help in an infringement action,
but we would hope that a court would enforce the parties’ jurisdictional choice.

V. CONCLUSION

We conclude with an admonition to lawyers and cyberspace traders to mind
their contracts. This is true not only with respect to choice of law and choice of
forum provisions, but also generally. For no matter what the legislatures do, no
matter which survive, commercial practices enshrined in contracts will generally be
given effect. Maintaining tangible records validating subsequent electronic
transactions is conservative, but effective. Even without a paper validating electronic
transactions, the best advice is to remember the fiction of paper contracting and
device a process of forming contracts electronically that mimics traditional methods.
That “lemming” approach to the law is not necessarily the best approach from a
purely theoretical view, but it is what the cyberspace law merchants have formed over

217. Id. at 1733-34.
Contracting in Cyberspace

the past years. The statutory works are now in process to validate or incorporate much of this developing cyberspace law. Stay tuned.