



GW Law Faculty Publications & Other Works

Faculty Scholarship

2002

Regulating Electronic Commerce

Gregory E. Maggs

George Washington University Law School, gmaggs@law.gwu.edu

Follow this and additional works at: http://scholarship.law.gwu.edu/faculty_publications

 Part of the [Law Commons](#)

Recommended Citation

Gregory E. Maggs, Regulating Electronic Commerce, 50 Am. J. Comp. L. 665 (2002).

This Article is brought to you for free and open access by the Faculty Scholarship at Scholarly Commons. It has been accepted for inclusion in GW Law Faculty Publications & Other Works by an authorized administrator of Scholarly Commons. For more information, please contact spagel@law.gwu.edu.

Citation: 50 Am. J. Comp. L. 665 (2001)

NOTE: This is not an ordinary law review article. It is a report submitted at the 16th International Congress of Comparative Law, held in Brisbane, Australia, on July 14-20, 2002. The report addresses a number of subjects identified by Dr. Anne Fitzgerald, the General Reporter for the section on Electronic Commerce. The general purpose of the report is merely to summarize the current state of the law in the United States.

REGULATING ELECTRONIC COMMERCE

Gregory E. Maggs*

I. Introduction

The term ‘electronic commerce’ generally refers to contracts and payments made using computers and other electronic equipment.¹ As commonly used, the phrase encompasses agreements concluded through the exchange of email, purchases made at internet websites, transfers of money made by electronic means, and other similar activities. The term further includes both business-to-business and business-to-consumer transactions.

What law governs electronic commerce? Oliver Wendell Holmes Jr., the great American jurist and legal scholar, once told a humorous tale about a justice of the peace who heard a lawsuit over a broken butter churn.² He looked up ‘butter churn’ in the index of his law books, but found nothing. Accordingly, the justice of the peace concluded there was no law on point.

A modern jurist almost could make the same mistake by looking up ‘electronic commerce’ in modern statutes and cases. As this article will show, a few new laws in the United States establish special rules for electronic transactions. But that does not mean that other laws do not apply.

* Gregory E. Maggs is Professor of Law, The George Washington University. This report addresses a number of subjects identified by Dr. Anne Fitzgerald, the General Reporter for this section. At her suggestion to the National Reporters, I have concentrated on the principal issues and developments from the perspective of the American legal system.

¹ For general books on the law of electronic commerce, see J. Carl Poindexter & David L. Baumer, *Cyberlaw and E-Commerce* (2001); Susan Singleton, *Ecommerce: A Practical Guide to the Law* (2001); Jane K. Winn & Benjamin Wright, *The Law of Electronic Commerce* (2000); Barry B. Sookman, *Computer, Internet and Electronic Commerce Law* (2000).

² See Holmes, Jr., “The Path of the Law,” 10 Harv. L. Rev. 457, 474-75 (1897).

Instead, many general rules of contract and commercial law govern electronic commerce.

For example, suppose that a consumer purchases a book over the internet. The consumer visits the seller's website, browses through the titles for sale, selects a book by clicking on some part of the computer screen, and then inputs a credit card number. If all goes as planned, the seller will ship the book, and charge the consumer's credit card. The issuer of the credit card, most likely through an intermediary*666 bank, will pay the seller, and then bill the consumer. At the end of the month, the consumer will pay the credit card.

Although this transaction occurred online, the transaction is a contract for the sale of goods governed by article 2 of the Uniform Commercial Code.³ The book is a good because it is a 'movable thing,'⁴ and the transaction involves a sale because title to the book passes from the seller to the buyer for a price.⁵ The consumer formed a contract by clicking on the computer screen because the U.C.C. says that a contract can be formed by any method sufficient to show an agreement.⁶ In addition, in making the purchase, the buyer would have the usual statutory protection afforded to credit cardholders.⁷ The federal laws limiting liability for unauthorized charges and allowing cardholders to assert claims and defenses against the issuer contain no exception for internet charges.⁸

Examples like this one show that much of the law of electronic commerce in the United States is ordinary commercial law. In addressing disputes arising out of electronic transactions, courts often simply must decide how these ordinary laws apply. Only in special circumstances must they consider new laws applicable only to computer-based transactions.

This report will address five current topics concerning electronic commerce in the United States. Part II begins by discussing constitutional power to regulate internet commerce. Part III then looks at court decisions and new statutes concerning the formation of electronic contracts. Part IV covers electronic commerce payments. Part V describes laws governing

³ See U.C.C. § 2-102 (scope of article 2).

⁴ See *id.* § 2-105 (defining goods).

⁵ See *id.*

⁶ See *id.* § 2-104(3).

⁷ 15 U.S.C § 1644 (limiting liability for unauthorized use of credit cards); *id.* § 1666i (affording cardholders the right to assert against the card issuer certain claims and defenses arising out of the transaction).

⁸ See *id.* §§ 1644, 1666i.

internet crime and website security. Part VI then talks about the ‘digital divide’ separating Americans who have access to internet commerce from those who do not. Part VII states a brief conclusion.

Discussions of electronic commerce law often address legal issues relating to intellectual property and internet governance. This report, however, will not touch upon either of these important subjects because they are covered in conference topic III.B. (‘Copyright Issues and the Information Highways, and Domain Names on the Internet’). Similarly, this report will not consider questions relating to the regulation of on-line content and privacy because they are covered by conference topic IV.B.2 (‘Protection of Fundamental Rights in the Digital Era’).

*667 II. Constitutional Power to Regulate Electronic Commerce

The United States Constitution limits governmental power and divides it between the federal government and the fifty states. Accordingly, as Congress and state legislatures seek to enact new laws regulating electronic commerce, questions inevitably arise about what the Constitution does and does not permit. Although only a few cases specifically have addressed these questions, the answers most likely will turn on the application of several well-established constitutional principles.

A. Federal Power

The ‘Commerce Clause’ of the Constitution empowers Congress to ‘regulate Commerce . . . among the several States.’⁹ The Supreme Court has held that this power enables Congress to regulate interstate commerce and its channels and instrumentalities.¹⁰ It further has held that the power permits Congress to regulate intrastate economic activities, provided that Congress rationally could conclude that the activities might have a substantial effect on interstate commerce, either by themselves or through their repetition nationwide.¹¹

Using this power, Congress presumably could regulate most aspects of electronic commerce. Not only does much of this commerce cross state lines, but even commerce located wholly within one state may affect

⁹ U.S. Const. art. I, § 8.

¹⁰ See *Gibbons v. Ogden*, 22 U.S. (9 Wheat.) 1, 193-98 (1824).

¹¹ See *United States v. Darby*, 312 U.S. 100, 118-119 (1941); *Wickard v. Filburn*, 317 U.S. 111, 127-128 (1942); *Heart of Atlanta Motel v. United States*, 379 U.S. 241, 257-258 (1964); *Katzenbach v. McClung*, 379 U.S. 294, 298 (1964); *United States v. Lopez*, 514 U.S. 549, 559-560 (1995).

interstate commerce.¹² Indeed, pursuant to this power, Congress already has passed various laws. A prominent example is the Electronic Signatures in Global and National Commerce Act of 2000 (ESIGN).¹³ As discussed more fully below, this act validates contracts formed by electronic means.¹⁴ Congress also has used its commerce power to pass laws aimed at computer crime.¹⁵

B. State Power

The Commerce Clause does not give Congress the exclusive power to regulate commerce.¹⁶ Rather, the states share that power as part of their reserved sovereignty.¹⁷ When a state seeks to regulate commerce within its borders, it faces only a few important limitations.

First, under the Supremacy Clause,¹⁸ federal legislation may preempt state regulation. A federal statute preempts or supercedes a state statute whenever the two conflict.¹⁹ In addition, federal legislation will preempt a state law whenever Congress indicates that the federal legislation should occupy the field to the exclusion of state law.²⁰ For example, in the Internet Tax Freedom Act of 1998, Congress preempted new state and local laws that would tax internet access or discriminate against electronic commerce.²¹

Second, as an implication of the Commerce Clause,²² a state law cannot impose a burden on interstate commerce that is excessive in relation to legitimate local interests.²³ Under this test, a federal court invalidated a New York law that restricted the distribution of obscene materials to

¹² See, e.g., *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 169-184 (S.D.N.Y. 1997) (holding that interstate communications on the internet fall within the meaning of 'commerce').

¹³ 15 U.S.C. §§ 7000-7013.

¹⁴ See *infra* part III.a.

¹⁵ See *infra* part V.

¹⁶ See *Gibbons v. Ogden*, 22 U.S. (9 Wheat.) at 237.

¹⁷ See U.S. Const. amend. 10.

¹⁸ See U.S. Const. art. VI, cl. 2.

¹⁹ See *Silkwood v. Kerr-McGee Corp.*, 464 U.S. 238, 248 (1984).

²⁰ See *id.*

²¹ See Internet Tax Freedom Act § 1101, Pub. L. 105-277, Div. C, Title XI, Oct. 21, 1998, 112 Stat. 2681-719 (not codified, but included as note at 47 U.S.C. § 151).

²² See U.S. Const. art I, § 8, cl. 3.

²³ See *South Carolina Department of Transportation v. Barnwell Brothers*, 303 U.S. 177, 189 (1938); *Southern Pacific v. Arizona*, 325 U.S. 761, 767 (1945).

minors over the internet.²⁴ The court found the law excessively burdensome because it would regulate websites located in other states that might have different legal standards.²⁵

Third, as another implication of the Commerce Clause,²⁶ a state law cannot treat interstate commerce differently from intrastate commerce, and cannot have a disparate impact on interstate commerce, when there is a reasonable, non-discriminatory, alternative way of furthering the state's legitimate interests.²⁷ No reported case has addressed this kind of discrimination in the context of electronic commerce. As a hypothetical example, however, a state could not prohibit an out-of-state corporation from providing internet access in the state.

Even if the limitations of the Supremacy Clause and Dormant Commerce Clause do not invalidate a state law, the requirement of Due Process may limit judicial application of the law outside of the state boundaries.²⁸ For example, suppose that an internet user in New York wants to press a claim under a New York law against a California business arising out of the business's website in California. Due process may pose obstacles for the internet user, whether the internet users sue the business in New York or California.

***669** If the internet user sues the California business in New York, the business may argue that Due Process prevents a New York court from asserting jurisdiction. The Supreme Court has interpreted the Due Process Clause to prohibit a court from exercising jurisdiction over any person or business that does not have 'minimum contacts' with the state in which the court is located.²⁹ A number of American cases have considered whether maintaining a website accessible by users located in another state suffices to create minimum contacts with the state, but they do not all agree.

Some courts have held that they may exercise jurisdiction consistent with due process because a website and other factors may create minimum contacts. For example, in *Minnesota v. Granite Gate Resorts, Inc.*,³⁰ the state of Minnesota sued the owner of a gambling business located in

²⁴ See *American Libraries Ass'n v. Pataki*, 969 F. Supp. at 173.

²⁵ See *id.* at 175-76.

²⁶ See U.S. Const. art. I, § 8, cl. 3.

²⁷ See *Dean Milk v. City of Madison*, 340 U.S. 349, 354 (1951); *Hughes v. Oklahoma*, 441 U.S. 322, 336 (1979).

²⁸ See U.S. Const. amends. 5, 14.

²⁹ *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945).

³⁰ 568 N.W.2d 715 (Minn. 1997).

Nevada for consumer fraud. The court ruled that the business had minimum contacts with the state of Minnesota sufficient for the exercise of jurisdiction based largely on the ability of Minnesota internet users to see the gambling business's website.³¹ The court rejected the business's argument that minimum contacts did not exist because its maintenance of the website was 'passive' and Minnesota citizens had chosen to visit the website.³² The court likened websites to broadcast and direct mail solicitation, both of which have sufficed to establish minimum contacts in non-electronic commerce cases.³³ Other cases also have found jurisdiction on similar facts.³⁴

A few courts have reached a somewhat contrary conclusion. In *Ty Inc. v. Clark*,³⁵ a federal court located in Illinois refused to exercise jurisdiction over a company in the United Kingdom. The court emphasized that, although the company in the United Kingdom maintained a website that internet users could access while using computers in Illinois, the company did not engage in online transactions.³⁶ Other courts also have refused to exercise jurisdiction using similar reasoning.³⁷

If the New York internet user sues the business in California, a California court could exercise jurisdiction because of the business's *670 location in the state.³⁸ Due Process, however, may preclude the California court from applying New York law. The United States Supreme Court has held that a state 'must have a significant contact or significant aggregation of contacts, creating state interests, such that choice of its law is neither arbitrary nor fundamentally unfair.'³⁹ Most states' choice of law rules

³¹ See *id.* at 718.

³² See *id.*

³³ See *id.* at 719-20.

³⁴ See, e.g., *Euromarket Designs, Inc. v. Crate & Barrel Ltd.*, 96 F. Supp. 2d 824, 841 (N.D. Ill. 2000); *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

³⁵ *Ty, Inc. v. Clark*, 2000 WL 51816 (N.D. Ill.).

³⁶ See *id.* at *3.

³⁷ See, e.g., *Soma Medical International v. Standard Chartered Bank*, 196 F.3d 1292, 1297 (10th Cir. 1999); *America Online, Inc. v. Huang*, 106 F. Supp.2d 848, 855 (E.D. Va. 2000); *Stewart v. Vista Point Verlag & Ringier Publishing*, 2000 WL 1459839, *4 (S.D.N.Y.).

³⁸ See *Helicopteros Nacionales de Columbia, S.A. v. Hall*, 466 U.S. 408, 414-16 (1984) (indicating that a court may exercise personal jurisdiction over a defendant whenever the defendant has engaged in 'systematic and continuous' activities in the forum state).

³⁹ See *Allstate Ins. Co. v. Hague*, 449 U.S. 302, 313 (1981).

satisfy this standard. Accordingly, at least to date, no reported case involving electronic commerce has questioned whether a court's choice of law violated due process.

III. Formation of Electronic Contracts

Most electronic commerce, like most commerce generally, involves the creation of contracts. Perhaps for this reason, many of the most significant developments in the law governing electronic commerce have concerned contract formation. The following discussion addresses four of the most important issues in this area.

A. Assent to Contractual Terms

A controversial electronic commerce issue arises when a business wishes to sell or distribute goods or services to an internet user, but only subject to certain conditions or limitations. The issue is how to bind the internet user to contractual terms specifying the conditions and limitations. For example, a distributor of software may wish to require the user to mediate any disputes that arise. What must the vendor do to obtain the user's assent to a term requiring mediation?

Vendors engaged in electronic commerce have attempted three somewhat controversial methods of obtaining the assent of internet users. These methods go by the names of 'shrink wrap,' 'click wrap,' and 'browser wrap.'⁴⁰ They all use different ways of presenting the contract terms to the internet user.

The 'shrink wrap' method involves putting a message on a product telling the purchaser that any use of the product constitutes assent to specified terms.⁴¹ The two leading cases on shrink wrap both come from the United States Court of Appeals for the Seventh Circuit.*671 In both cases, the court upheld the use of shrink wrap as a means of binding a purchaser to contractual terms.

⁴⁰ For general discussion of these topics, see Radin, "Humans, Computers, and Binding Commitment," 75 *Ind. L.J.* 1125 (2000); Note, Goodman, "Honey, I Shrink-wrapped The Consumer: The Shrink-wrap Agreement as an Adhesion Contract," 21 *Cardozo L. Rev.* 319 (1999).

⁴¹ Judge Frank Easterbrook has explained the origins of the term 'shrinkwrap' as follows: 'The 'shrinkwrap license' gets its name from the fact that retail software packages are covered in plastic or cellophane 'shrinkwrap,' and some vendors ... have written licenses that become effective as soon as the customer tears the wrapping from the package.' *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996).

In *ProCD Inc. v. Zeidenberg*, a vendor sold a CD containing a telephone directory and software that allowed the user to access the directory data.⁴² The box containing the CD indicated that the software came with use restrictions stated in an enclosed license.⁴³ The enclosed manual contained the license.⁴⁴ In addition, the license appeared on the screen when the consumer used the software, and the software would not allow the user to proceed without indicating assent.⁴⁵ In an often-cited opinion by Judge Frank Easterbrook, the court held that the consumer was bound by the terms of the license, even though the consumer had not seen the terms at the time of paying for the product.⁴⁶ The court explained that, although the buyer had paid the purchase price, he had not completed acceptance of a contract until indicating assent to the license.⁴⁷ The inability of the buyer to see the terms of the license before paying (although not before accepting) did not trouble the court because consumers often cannot examine the contents of purchases in advance. The court explained: ‘Terms of use are no less a part of the ‘the product’ than are the size of the database and the speed with which the software compiles listings. Competition among vendors, not judicial revision of the package’s contents, is how consumers are protected in a market economy.’⁴⁸

In *Hill v. Gateway 2000*,⁴⁹ consumers purchased a computer over the telephone.⁵⁰ When the computer arrived, the box contained an elaborate form contract.⁵¹ The terms of the contract required arbitration of all contract disputes but provided that the purchaser could return the computer within thirty days of the purchase.⁵² The consumers later attempted to sue the manufacturer in court.⁵³ In another opinion by Judge Easterbrook, the court followed *Pro-CD*, and held that the consumers could not maintain their lawsuit because they were bound by the arbitration clause.⁵⁴ The

⁴² See *id.* at 1149.

⁴³ See *id.* at 1450.

⁴⁴ See *id.*

⁴⁵ See *id.*

⁴⁶ See *id.* at 1451.

⁴⁷ See *id.* at 1452 (noting that the vendor, as master of the bargain, was free to set the terms of acceptance).

⁴⁸ *Id.* at 1453.

⁴⁹ 105 F.3d 1147 (7th Cir. 1997).

⁵⁰ See *id.* at 1148.

⁵¹ See *id.*

⁵² See *id.*

⁵³ See *id.*

⁵⁴ See *id.* at 1148-49.

court explained that the consumers knew before ordering the computer that it would *672 come with a contract containing some important terms, but they did not ask to see them.⁵⁵

To summarize, under these two cases, a seller can bind a buyer to shrink wrap terms in two situations. First, the seller may structure the transaction so that a sale is not complete until a buyer agrees to contractual terms sent with a product, whether or not the buyer paid in advance.⁵⁶ Second, the seller may structure the transaction so that at the time the sale becomes complete the buyer at least knows that the product comes subject to some contractual terms, even if the buyer does not know exactly what those terms say.⁵⁷ These rules simplify the process of selling products subject to use limitations.

At least one court, however, has disagreed with *Hill v. Gateway 2000* and *ProCD v. Zeidenberg*. In *Klocek v. Gateway, Inc.*,⁵⁸ a federal district court refused to enforce shrink-wrap terms requiring arbitration.⁵⁹ The court held that the consumer had offered to purchase the computer, and the manufacturer had accepted the offer by shipping the merchandise.⁶⁰ Although the manufacturer had included terms in the box with the computer, the manufacturer ‘did not communicate to plaintiff any unwillingness to proceed without plaintiff’s agreement to the [license terms.]’⁶¹ Accordingly, the court said, the terms could not become part of the contract unless the purchaser agreed to them, which the purchaser did not.⁶² Whether other courts also will reject the Seventh Circuit’s analysis remains uncertain.

Another method of obtaining assent for sales over the internet is ‘click wrap.’ After selecting a product to purchase, the internet user sees the contract terms on the computer screen, and cannot complete the purchase

⁵⁵ See *id.* at 1150.

⁵⁶ If the buyer decides not to agree to the sale, the buyer should have a right to return of the purchase price, presumably under a theory of restitution.

⁵⁷ The seller, for example, might tell prospective purchasers the goods come ‘subject to contractual limitations stated with the product.’

⁵⁸ 104 F. Supp. 2d 1332 (D. Kan. 2000).

⁵⁹ See *id.* at 1339.

⁶⁰ See *id.* at 1340.

⁶¹ *Id.* at 1340.

⁶² See *id.*

without clicking a box on the screen to indicate assent.⁶³ A few courts have upheld the use of click wrap. For example, in *In re RealNetworks, Inc. Privacy Litigation*,⁶⁴ the court held that internet users had agreed to a license agreement requiring arbitration. Similarly, in *Hotmail Corp. v. Van \$ Money Pie, Inc.*,⁶⁵ a court *673 upheld the validity of restrictions on the use of free email accounts for sending advertisements.⁶⁶

Although the opinions in *RealNetworks* and *Hotmail* do not contain detailed legal analysis, most courts probably will consider click wrap to be less controversial than shrink wrap. With click wrap, unlike shrink wrap, the purchaser sees the terms of the contract, and indicates assent, before parting with any money. This feature greatly diminishes the possibility of disappointed expectations.

A final method of presenting contractual terms to a consumer is ‘browser wrap.’⁶⁷ When using this method, an internet vendor affords the user the opportunity to look at the terms of the sale, but does not require the user to click on anything to indicate assent to these terms before paying for the product. For example, the website may contain a button saying “click here for legal terms,” which the purchaser may click or ignore.

One court has held that browser wrap does not suffice to obtain assent. In *Specht v. Netscape Communications Corp.*,⁶⁸ the court decided that a computer user who downloaded software did not assent to a license agreement.⁶⁹ The website contained a message saying ‘Please review and agree to the terms of the Netscape Smart Download software license agreement before downloading and using the software.’⁷⁰ The user,

⁶³ *Specht v. Netscape Communications Corp.*, 150 F. Supp.2d 585, 593-94 (S.D.N.Y. 2001) (‘A click-wrap license presents the user with a message on his or her computer screen, requiring that the user manifest his or her assent to the terms of the license agreement by clicking on an icon. The product cannot be obtained or used unless and until the icon is clicked.’).

⁶⁴ 2000 WL 631341, *4 (N.D. Ill.).

⁶⁵ 1998 WL 388389, *6 (N.D. Cal.).

⁶⁶ In *Groff v. America Online*, 1998 WL 307001, *5 (R.I. Super.), a court also upheld assent based on website that required the user to click on ‘I agree’ or ‘I disagree.’

⁶⁷ See *Pollstar v. Gigmania, Ltd.*, 2000 WL 33266437, *6 (E.D.Cal. 2000) (using the term ‘browser wrap’).

⁶⁸ 150 F. Supp.2d 585 (S.D.N.Y. 2001).

⁶⁹ See *id.* at 595-96.

⁷⁰ *Id.* at 595.

however, was not required to review the terms of the agreement. The court held that this scheme did not suffice to create a contract.⁷¹

Another court appears to have disagreed. In *Pollstar v. Gigmania Ltd.*,⁷² a website contained information about the scheduling of music concerts. The website also stated terms restricting copying the information.⁷³ Although users could see the license, they did not have to click on anything in order to see the concert information.⁷⁴ When the proprietor of the website sued a user for breaching the license, the user sought to dismiss on grounds that the user had not assented to it.⁷⁵ The court, however, refused to dismiss the case, *674 concluding that the browser wrap ‘agreement may be arguably valid and enforceable.’⁷⁶

Vendors might combine browser wrap with shrink wrap. They might make the terms of contracts available for viewing online, but ship the products subject to later assent by the purchaser. This approach may eliminate some of the objections to shrink wrap and browser wrap that currently exist.⁷⁷ Not only would purchasers know that they will have to accept contractual terms to complete the purchase, they also will have an opportunity to see the terms in advance. Adding click wrap would further ensure that purchasers have the opportunity to assent to contractual terms.

B. Statute of Frauds

A ‘statute of frauds’ is a statute making certain kinds of contracts unenforceable absent a signed writing.⁷⁸ The federal government and the fifty states have enacted numerous statutes of frauds. The Uniform Commercial Code, for example, requires a signed writing for contracts for

⁷¹ The court said: ‘Couched in the mild request, ‘Please review,’ this language reads as a mere invitation, not as a condition. The language does not indicate that a user must agree to the license terms before downloading and using the software.’ Id. at *596.

⁷² 2000 WL 33266437 (E.D. Cal.).

⁷³ See id. at *5.

⁷⁴ See id.

⁷⁵ See id. at 6.

⁷⁶ Id.

⁷⁷ See Maggs, “Internet Solutions to Consumer Protection Problems,” 49 S.C. L. Rev. 887, 894-96 (1998) (discussing how the Gateway 2000 could have made the terms of its computer sales contracts available online, as most computer vendors do).

⁷⁸ Black’s Law Dictionary 661-62 (6th ed. 1990).

the sale of goods for \$500 or more.⁷⁹ The Federal Arbitration Act, similarly, requires a writing for contracts to arbitrate disputes.⁸⁰

The requirement of a writing and a signature under a statute of frauds potentially could pose an obstacle to internet commerce. For example, suppose that two parties attempt to form a contract by email for the sale of goods for a price of more than \$500. Do their electronically exchanged messages satisfy the 'writing' requirement of Uniform Commercial Code? Can they 'sign' their writing electronically?

Two significant pieces of legislation address these questions. One is the Uniform Electronic Transaction Act of 1999 (UETA), a model state law enacted 37 states.⁸¹ The other is the federal Electronic Signatures in Global and National Commerce Act of 2000 (ESIGN).⁸² Both of these statutes have the effect of creating exceptions *675 to statutes of frauds so that they do not automatically prevent enforcement of electronic contracts.⁸³

UETA, the state legislation, strives to eliminate obstacles that statutes of fraud might impose by stating four basic principles:

- (a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
- (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
- (c) If a law requires a record to be in writing, an electronic record satisfies the law.
- (d) If a law requires a signature, an electronic signature satisfies the law.⁸⁴

⁷⁹ See U.C.C. § 2-201(1).

⁸⁰ 9 U.S.C. § 2.

⁸¹ The National Conference of Commissioners of Uniform States Laws drafted and published UETA. For information and state adoption statistics. See <<<http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>>> (visited Sept. 25, 2001). For the full text of UETA, see <<<http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>>> (visited Sept. 25, 2001).

⁸² 15 U.S.C. §§ 7000-7013.

⁸³ No reported cases had addressed either ESIGN or UETA as of September 2001.

⁸⁴ See UETA § 7.

Pursuant to these principles, electronic records and signatures may take the place of traditional paper and ink.⁸⁵

ESIGN, the federal legislation, serves a similar function. ESIGN provides that, notwithstanding any previously existing statute of frauds, ‘a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form.’⁸⁶ It thus also allows electronic commerce to take place without hindrance from statutes of frauds.

Both UETA and ESIGN contain various exceptions.⁸⁷ For example, neither law applies to writing requirements for wills, codicils, or testamentary trusts.⁸⁸ In addition, both laws exclude almost all of the Uniform Commercial Code except for the articles dealing with contracts for the sale and lease of goods.⁸⁹

Although ESIGN is a federal statute, it does not preempt UETA.⁹⁰ On the contrary, ESIGN specifically provides that, if a state has enacted UETA, then UETA rather than ESIGN will govern exceptions to state statutes of frauds.⁹¹ Although the similarity of the statutes *676 generally makes it irrelevant which law applies, a number of subtle differences do exist.⁹²

C. Attribution of Electronic Records

When a plaintiff sues a defendant for breach of contract, the plaintiff must show more than the existence of a promise. The plaintiff also must show that the defendant, or the defendant’s agent, made the promise.⁹³

⁸⁵ UETA defines a record as ‘information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.’ Id. § 2(13). It defines an electronic record as ‘a record created, generated, sent, communicated, received, or stored by electronic means.’ Id. § 2(7).

⁸⁶ 15 U.S.C. § 7001(1)(a).

⁸⁷ See UETA § 3 (defining the scope of the statute); ESIGN, 15 U.S.C. § 7003 (identifying exceptions).

⁸⁸ See UETA § 3(b)(1); ESIGN, 15 U.S.C. § 7003(a)(1).

⁸⁹ See UETA § 3(b)(2); ESIGN § 7003(a)(3).

⁹⁰ See Patricia Brumfield Fry, “A Preliminary Analysis of Federal and State Electronic Commerce Laws,” <<http://www.nccusl.org/nccusl/uniformact_articles/uniformacts-article-ueta.asp>> (visited Sept. 17, 2001) (providing an in-depth analysis of the ESIGN’s preemptive effects).

⁹¹ See ESIGN, 15 U.S.C. § 7002(a)(1).

⁹² See Fry, *supra* n. 90 (discussing these differences).

⁹³ See, e.g., *Van Brunt v. Jackson*, 512 P.2d 517, 520 (1973) (requiring the plaintiff to prove that the defendant executed the contract).

When litigating non-electronic commerce transactions, the plaintiff often uses documentary evidence to address this issue of attribution. For example, the plaintiff may introduce a document purportedly signed by the defendant or the defendant's agent.⁹⁴

In litigating electronic commerce transactions, however, the plaintiff generally has no paper and ink documents to use for attributing a promise to a defendant. Instead, the plaintiff may have evidence only that someone visited the plaintiff's website, and typed the defendant's name or email address when promising to pay for a purchase. The question arises whether this type of evidence can suffice to attribute the promise to the defendant.

UETA addresses this issue of attribution with the following provision:

An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.⁹⁵

Although no cases have yet addressed this provision, the UETA commentary confirms that an electronic record and electronic signature would be attributable to a person if the 'person types his/her name as part of an e-mail purchase order.'⁹⁶ The commentary also makes clear that the plaintiff would have to overcome any evidence presented by the defendant of fraud or forgery.⁹⁷ In reality, many businesses still may wish that they had the customer's signature in ink on paper, notwithstanding UETA, because a genuine signature would simplify proof.⁹⁸

*677 D. Automated Transactions (Electronic Agents)

Using machines to make contracts predates the invention of computers. Businesses, after all, have made sales through vending machines for decades. Yet, in most non-electronic commerce transactions of substantial

⁹⁴ At least for some classes of contracts, a signature in the name of the defendant is prima facie evidence that the defendant agreed to the contract. See, e.g., U.C.C. § 3-308 (presumption of validity of signatures on negotiable instruments).

⁹⁵ UETA § 9(a).

⁹⁶ Id. § 9 cmt. 1.

⁹⁷ See id.

⁹⁸ See Julia Angwin, "Credit-Card Scams Bedevil E-Stores: With No Signatures to Prove Who Placed Orders, Sites Are Left Footing the Bills," Wall St. J., Sept. 19, 2000, at B1 (explaining how credit card issuers charge back allegedly fraudulent charges to internet business more frequently than other businesses).

significance, humans rather than machines participate in the formation of agreements. When non-human entities like corporations make purchases and sales, they generally rely on human agents to form their contracts.

In electronic commerce transactions, by contrast, businesses and individuals may rely on computers to make contracts of considerable sophistication. For example, when an internet user purchases a camera at a website, the website may process the order entirely without human intervention. It make take the credit card number, send an order to the warehouse, prepare the shipping labels, and so forth. The question whether a person or business may use an electronic agent to form a contract therefore becomes more significant.

UETA and ESIGN each contain provisions designed to remove any doubt that electronic agents may form contracts. UETA says:

A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.⁹⁹

Similarly, ESIGN states:

A contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound.¹⁰⁰

These provisions do not purport to change existing law. Instead, as the UETA commentary asserts, they merely confirm that machines may act as agents.¹⁰¹ No cases have yet addressed these sections.

⁹⁹ UETA § 14(1). UETA further states: '(2) A contract may be formed by the interaction of an electronic agent and an individual, acting on the individual's own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance. (3) The terms of the contract are determined by the substantive law applicable to it.' Id. § 14(2)-(3).

¹⁰⁰ 15 U.S.C. § 7002(h).

¹⁰¹ See UETA § 14 cmt. 1.

***678** IV. Electronic Commerce Payments

In addition to the formation of contracts, most electronic commerce involves some sort of payment. Internet users, for example, need to pay for any goods or services that they purchase at websites. The following discussion addresses issues relating to electronic transactions involving credit and debits cards, negotiable instruments, and other payment devices.

A. Credit Cards and Debit Cards

Few if any legal obstacles inhibit using credit cards and debit cards in electronic commerce. Private contracts rather than legislative enactments establish most of the rights and duties of cardholders, card issuers, and merchants.¹⁰² To the extent that these contracts require modernization to accommodate electronic commerce, these parties can modify them. Indeed, some changes relating to internet purchases have already taken place.¹⁰³

Although private agreements generally govern the rights of cardholders, cardholders also enjoy statutory limitations on their liability for the unauthorized use of their credit cards and debit cards. In particular, section 134 of federal Consumer Credit Protection Act and section 909 of the federal Electronic Fund Transfer Act may limit their liability to \$50.¹⁰⁴ This limitation on liability greatly relieves anxiety that consumers otherwise might have about using their credit and debit cards to make electronic purchases. Nothing in these statutes makes them inapplicable to electronic commerce transactions.

A consumer credit cardholder has another federal statutory right aimed at facilitating dispute resolution. In particular, if the cardholder has a claim or defense against a merchant, section 170 of the Consumer Credit Protection Act gives the cardholder a limited right to assert this claim or

¹⁰² See Matthews, "Credit Cards--Authorized and Unauthorized Use," 13 Ann. Rev. Banking l. 233, 240-42 (1994) (discussing agreement between cardholder and issuing bank).

¹⁰³ See, e.g., "AT&T Offers Protection for Net Buys," Cards International, Feb. 27, 1996, at 6 (discussing how AT&T has modified its contracts with cardholders for purchases on the internet).

¹⁰⁴ See Consumer Credit Protection Act, 15 U.S.C. § 1643(a)(1)(B) (limiting liability for unauthorized use of credit cards to \$50); Electronic Funds Transfer Act, id. § 1693g(a) (limiting liability for unauthorized use of debit cards connected with a bank account to \$50 in certain circumstances).

defense against the card issuer.¹⁰⁵ The consumer can assert this claim or defense simply by withholding payment to the card issuer, which the cardholder may find more convenient than suing the merchant.

*679 Nothing in section 170 prevents the provision from applying to electronic commerce. Internet purchases, however, do raise one unresolved issue. By its terms, section 170 applies only to transactions occurring within the same state or within 100 miles of the cardholder's billing address.¹⁰⁶ If an internet user located on the East Coast visits the website of a company located in West Coast, a dispute may arise about where the transaction took place. In deciding where contracts made over the telephone are formed for the purpose of section 170, courts traditionally have said that formation occurs at the place where the acceptance of the offer is uttered.¹⁰⁷ This rather formalistic test requires a careful analysis to determine which party made the offer and which party made the acceptance.¹⁰⁸ How or even whether courts will apply this test to purchases made over the internet remains unclear.

B. Negotiable Instruments and Documents of Title

Americans use ordinary checks to make an extraordinary number of payments.¹⁰⁹ Under current law, they cannot create these checks electronically. The Uniform Commercial Code defines a check as a form of a 'draft,'¹¹⁰ and a draft as an 'order.'¹¹¹ It then specifies that an order is 'a written instruction to pay money signed by the person giving the instruction.'¹¹² Neither UETA nor ESIGN create an exception to the writing and signature requirements.¹¹³ The official commentary to UETA explains that

¹⁰⁵ See 15 U.S.C. § 1666i. The card issuer, by contract, may have a right to charge back of the amount claim or defense to the merchant. See Angwin, *supra* n. 98, at B1.

¹⁰⁶ See *id.*

¹⁰⁷ See *In re Standard Financial Management Co.*, 94 B.R. 231, 239 (Bankr. D. Mass 1988); *Plutchok v. European American Bank*, 540 N.Y.S.2d 135, 137 (Dist. Ct. 1989).

¹⁰⁸ See *In re Standard Financial Management Co.*, 540 N.Y.S.2d at 137.

¹⁰⁹ See Lucinda Harper, "Americans Won't Stop Writing Checks-- Electronic Payments Are Viewed as Too Complicated," *Wall St. J.*, Nov. 24, 1998, at A2 (describing how Americans write more than 65 billion checks each year).

¹¹⁰ U.C.C. § 3-104(f).

¹¹¹ *Id.* § 3-104(e).

¹¹² *Id.* § 3-103(a)(6).

¹¹³ See UETA § 3(b)(2) (excluding article 3 of the U.C.C.); ESIGN, 15 U.S.C. § 7003(a)(3) (same).

the check collection system simply involves too many parties and relationships to change the present rules.¹¹⁴

Although the U.C.C. requires the creation of a physical check, it permits some electronic handling of checks. For example, it permits the electronic presentment of checks. In other words, a depository bank need not actually send the check to the payor bank, but instead *680 may transmit just the information contained on the check.¹¹⁵ An increasing number of banks are using this procedure.¹¹⁶

In addition, the U.C.C. does not require banks to return canceled checks to their customers; instead, they can send the customer a statement listing the check numbers and their amounts.¹¹⁷ Although many state statutes require parties to retain cancelled checks for recordkeeping purposes,¹¹⁸ UETA and ESIGN both provide that electronic retention of the information on the front and back of checks will satisfy these requirements.¹¹⁹

Even though UETA and ESIGN do not apply to checks, they validate the creation of electronic 'transferrable records' that serve the same function as promissory notes and documents of title.¹²⁰ Just as holders of promissory notes and documents of title may assign their rights by physically transferring the paper on which the instruments are written,¹²¹ UETA and ESIGN allow holders of transferrable records to transfer their rights by transferring control of their records.¹²² If electronic transferrable records become widely used, they could reduce the burden of keeping track of promissory notes and documents of title, and provide added security.

The key requirement for a transferrable record under UETA and ESIGN is that any copies of the record must be readily identifiable as copies and not as the original.¹²³ Otherwise, disputes might arise about who controls

¹¹⁴ See UETA § 3 cmt. 5.

¹¹⁵ See U.C.C. § 3-501(b)(1).

¹¹⁶ Steven Marjanovic, "Electronic-Presentment Clearing House Grows," *The American Banker*, Mar. 11, 1999, at 16.

¹¹⁷ See *id.* § 4-406(c).

¹¹⁸ See UETA pref. note (describing a study which identified over 2500 laws requiring the retention of checks).

¹¹⁹ UETA § 12(e); ESIGN, 15 U.S.C. § 7001(d)(4).

¹²⁰ See UETA § 16; ESIGN, 15 U.S.C. § 7021.

¹²¹ See U.C.C. §§ 3-202 & 3-203 (negotiation and transfer of negotiable instruments); *id.* §§ 7-502, 7-504 (negotiation and transfer of documents of title).

¹²² See UETA § 16(d); ESIGN, 15 U.S.C. § 7021(d).

¹²³ See UETA § 15(c); ESIGN, 15 U.S.C. § 7021(c).

the original record. At present, techniques for creating records that satisfy this requirement remain under development. The drafters of UETA and ESIGN, however, apparently wanted to establish legal rules in advance to provide incentives for creating new systems.¹²⁴

C. Other payment Devices

For large payments, American businesses often employ letters of credit or funds transfers.¹²⁵ Although UETA and ESIGN do not apply*681 to these payment devices,¹²⁶ the U.C.C. itself permits their use in electronic commerce. U.C.C. Article 4A, which governs funds transfers, does not require a payment order initiating a funds transfer to have any particular form. Instead, it says that a payment order may be ‘transmitted orally, electronically, or in writing.’¹²⁷ The revised version of U.C.C. Article 5, which governs letters of credit, requires the issuer of a letter of credit to create a ‘record.’¹²⁸ The definition of record, however, includes electronically stored data so long as it can be retrieved in a tangible form.¹²⁹ In accordance with these rules, businesses and banks already use electronic means to create and transmit payment orders and letters of credit.

Various businesses currently are developing new systems for making payments over the internet.¹³⁰ These systems typically involve a combination of credit card charges and online accounts. For the most part, private contracts govern the rights of the parties who use these systems. At some point, however, courts may need to develop common law rules for resolving some disputes not addressed by contract. In such instances, the courts may choose either to analogize the new payment devices to traditional devices, or may attempt to find and apply general payment law principles.¹³¹

¹²⁴ See UETA § 15 cmt. 1.

¹²⁵ Funds transfers are also known as wholesale wire transfers. See U.C.C. art. 4A pref. note.

¹²⁶ See UETA § 3(b)(2) & cmt. 5 (excluding that articles of the U.C.C. that govern funds transfers and letters of credit); ESIGN 15 U.S.C. § 7003(a) (same).

¹²⁷ U.C.C. § 4A-103(a)(1).

¹²⁸ Id. § 5-104.

¹²⁹ See id. § 5-102(a)(14).

¹³⁰ Three commonly used systems are PayPal, BillPoint, and BidPay. See PayPal <<<http://www.paypal.com>>> (visited Sept. 28, 2001); BillPoint <<<http://www.BillPoint.com>>> (visited Sept. 28, 2001); BidPay <<<http://www.BidPay.com>>> (visited Sept. 28, 2001).

¹³¹ See Maggs, “New Payment Devices and General Principles of Payment Law,” 72 Notre Dame L. Rev. 753, 779-84 (1997) (discussing these approaches).

V. Security of Electronic Commerce

Companies doing business on the internet face security threats from two principal sources: hackers and competitors. Hackers generally seek to disrupt internet services, often for mischievous purposes rather than monetary gain.¹³² Sometimes hackers gain access to a website's computer files and make changes, seeking either to disable the website or to embarrass the proprietor. At other times, hackers take actions to overload the computers hosting the website, preventing legitimate users from gaining access. Existing laws make many types of hacking illegal.¹³³ The federal Criminal Code, in particular, ***682** has an extensive general provision entitled 'Fraud and related activity in connection with computers' that reaches most of this kind of conduct.¹³⁴

Competitors generally do not attempt to disable a business's website. Instead, they may seek to copy information from the website or to reach the business's customers. They often accomplish these actions simply by accessing the website just as ordinary internet users might. They then use automated means to obtain data contained within the website.

To some extent, copyright laws and private contracts may prevent the appropriation of information by competitors. For example, one business may not copy original photographs from another business's website. In addition, many websites require users to agree to terms and conditions that prevent users from making commercial use of information contained in the website.

When copyright laws and private contracts have not provided protection, the owners of some websites have attempted to bring actions against unwelcome visitors under the tort of 'trespass to chattels.' Traditionally, a person may commit this tort by impairing a chattel's 'condition, quality, or

¹³² See Eric J. Bakewell et al., "Computer Crimes," 38 Am. Crim. L. Rev. 481 (2001) (discussing forms of hacking and possible motivations).

¹³³ For general discussions of internet crime, see id.; Katyal, "Criminal Law in Cyberspace," 149 U. Pa. L. Rev. 1003 (2001); Sinrod & Reilly, "Cyber-crimes: a Practical Approach to the Application of Federal Computer Crime Laws," 16 Santa Clara Computer & High Tech. L.J. 177 (2000).

¹³⁴ 18 U.S.C. § 1030. Congress first enacted this provision in the federal Counterfeit Access Device and Computer Fraud and Abuse Law of 1984. It subsequently amended it in the Computer Fraud and Abuse Act of 1986, the National Information Infrastructure Protection Act of 1996, and other acts. See Bakewell et al., *supra* n. 132, at 487 (discussing this history).

value' or by depriving the owner of 'the use of the chattel for a substantial time.'¹³⁵

A few lower courts have granted preliminary injunctions on trespass to chattels claims. In *CompuServe Inc. v. Cyber Promotions, Inc.*, the court enjoined a business from sending unsolicited commercial email to the customers of an internet services provider.¹³⁶ In *Register.com, Inc. v. Verio, Inc.*, the court enjoined a competitor from using automated software processes to access and collect contact information from a competitor's database.¹³⁷ Similarly, in *eBay, Inc. v. Bidder's Edge, Inc.*, a court enjoined a competitor from obtaining and republishing information about on-line auctions.¹³⁸

Not all courts agree that these kinds of actions amount to trespass to chattels. In *Ticketmaster Corp. v. Tickets.com, Inc.*, a court refused to enjoin a competitor from using automated means to extract information about concerts and other events from a competing website.*683¹³⁹ The court explained: 'A basic element of trespass to chattels must be physical harm to the chattel (not present here) or some obstruction of its basic function (in the court's opinion not sufficiently shown here).'¹⁴⁰ At present, too few courts have addressed the issue to make predictions about what the future will hold.

VI. Access to Electronic Commerce

Electronic commerce through the internet has become widely available in the United States. One recent study found that 57 percent of American homes have access to the internet.¹⁴¹ In addition, another study found that

¹³⁵ Restatement (Second) of the Law of Torts § 218. The official commentary provides this illustration: 'A leaves his car parked near the corner. B, desiring to play a joke upon A, pushes the car around the corner where it cannot be easily seen by A. A comes out for his car, and fails to discover it for an hour. B is subject to liability for trespass to A.' Id. Illus. 4.

¹³⁶ 962 F. Supp. 1015, 1027-28 (S.D. Ohio 1997).

¹³⁷ 126 F. Supp.2d 238, 255 (S.D.N.Y. 2000).

¹³⁸ 100 F. Supp.2d 1058, 1071 (N.D. Cal. 2000).

¹³⁹ 2000 WL 1887522, *5 (C.D. Cal. 2000).

¹⁴⁰ Id. at *4.

¹⁴¹ See Julia Angwin, "E-Business: Has Growth of the Net Flattened?," Wall St. J., July 16, 2001, at B1.

more than 98 percent of all primary and secondary schools have internet access.¹⁴²

Access to the internet, however, is not evenly distributed throughout society. Of families that make more than \$100,000 a year, only about 7 percent do not have internet access.¹⁴³ By contrast, of families that make less than \$30,000, almost 60 percent do not have internet access.¹⁴⁴ Whites are more likely to have internet access than blacks or Hispanics; white collar employees more likely than blue collar workers; urban dwellers more likely than rural residents; younger people more likely than older people; Republicans more likely than Democrats.¹⁴⁵

In the context of internet commerce, this uneven distribution--often called the 'digital divide'--presents some reason for concern. To the extent that banks and businesses reward customers who have internet access, some percentage of the population may feel left behind. As a result, politicians and others recently have called for government programs designed to bring internet access to all.¹⁴⁶

The proposals generally call for government funding of some sort to reduce the cost of internet access or to make it available for free at public locations. Congress at present is considering various bills, sponsored by both Republicans and Democrats, designed to address *684 the Digital Divide.¹⁴⁷ In addition, the states also are weighing legislative action.¹⁴⁸

Despite great enthusiasm for digital divide legislation from some quarters, not much actually has happened. Opponents of governmental

¹⁴² See Melinda Patterson Grenier, "Web Access Extends to Over 75% of U.S. Public-School Classrooms," *Wall St. J.*, June 6, 200, at B2.

¹⁴³ See Albert R. Hunt, "American Opinion (A Special Report): A Quarterly Survey of Politics, Economics, and Values," *Wall St. J.*, Mar. 8, 2001, at A14.

¹⁴⁴ See *id.*

¹⁴⁵ See *id.*

¹⁴⁶ See, e.g., Edolphus Towns & Max Cleland, "New Legislation May Help Minority-Serving Institutions Address the Digital Divide," *Black Issues in Higher Education*, May 24, 2001, at 9; John F. Kerry, "Connecting Communities to the New Economy," *The Hill*, Feb. 7, 2001.

¹⁴⁷ See Capitol Hill, *Washington Internet Daily*, Jan. 5, 2001 (describing bills introduced at the start of the present Congress); "Digital Divide Problem, Solution Remain Elusive," *Electronic Commerce News*, Aug. 20, 2001 (describing pending Republican bills).

¹⁴⁸ See, e.g., "Digital Divide: Texas Can Close It, But It Must Do So Fairly," *Hous. Chron.*, May 16, 2001, at 24; Karin Fischer, "Democrats Pitch High-tech Agenda High-speed Access Vital to the State," *Charleston Daily Mail*, Apr. 6, 2001.

solutions to the digital divide problem have made five important arguments against the types of legislation proposed. These arguments appear to have at least enough support to delay or block most the proposed initiatives.

First, any plan to have taxpayers provide goods and services to the public is socialism, a form of government that most Americans reject and do not believe has proved successful. The current chairman of the Federal Communications Commission, Michael K. Powell, has voiced opposition to measures to eliminate the digital divide on this ground.¹⁴⁹

Second, computers and internet access have become so inexpensive that the government does not have to spend money on providing them to the public. Used computers fully capable of surfing the internet cost less than \$100.¹⁵⁰ In addition, consumers may obtain internet dial-up access for less than \$5 a month (the equivalent of one package of cigarettes), if they are willing to tolerate advertisements.¹⁵¹ These low prices suggest that many people who are not spending money on internet access simply have decided that they do not want it, not that they absolutely cannot afford it.¹⁵²

Third, some calls for increased spending appear to come not from the poor but from internet service providers. The suspicion is that these firms simply may want the government to provide them more business. For example, AOL Time Warner, one of the largest internet*685 service providers, recently funded the National Congress of American Indians'

¹⁴⁹ See Brendan I. Koerner, "Bright Young Thing," *Village Voice* 53 (July 31, 2001) (describing Chairman Powell's opposition to government funding of high speed internet access, on ground that it would be 'essentially the socialization of the deployment of the infrastructure').

¹⁵⁰ In searching the largest internet auction site, e-Bay.com, the author recently saw a number of Intel 486 based computers in the \$20 range. Although slow in comparison to today's computers, these machines would have seemed great just a few years ago.

¹⁵¹ AT&T, one of the largest telephone companies and internet services providers, recently offered a plan starting at \$4.95 a month. See <http://www.download.att.net/ucsemail> (describing the AT&T WorldNet(R) Service i495 plan). K-Mart, one of the nation's largest retailers, offers a plan for \$6.95 per month. See www.bluelight.com (visited August 20, 2001).

¹⁵² See Angwin, *supra* n. 141, at B1 (discussing another study that found that 23% of non-internet users said that they did not use the internet because they saw no need to use it).

Digital Divide Task Force.¹⁵³ This task force, not surprisingly, recently supported legislative measures to eliminate the digital divide.¹⁵⁴

Fourth, some proponents of spending public money to eliminate the digital divide have not sought to provide service to all the poor, or to just the poor, but instead have targeted their aim toward getting votes. For example, Democratic politicians from Western states want to give the money to Indian communities (who tend to vote Democratic), rather than to all residents of rural areas (who tend to vote Republican).¹⁵⁵ This approach makes their proposals less desirable to members of the opposing political party.

Fifth, to the extent that the government has additional money for the poor, it should spend it on more urgent needs. Critics advanced this argument prominently when former Speaker of the House Newt Gingrich proposed giving tax credits to families who buy laptops for school children.¹⁵⁶

VII. Conclusion

This article has attempted to summarize some of the most important American legislative and judicial developments in the area of electronic commerce. The federal and state governments have constitutional power to regulate most aspects of this commerce. They have not needed to exercise much of this power because existing laws already apply to most commerce, whether electronic or conventional. Most legislative efforts that have occurred have sought not to regulate but merely to facilitate developing commercial practices. If this trend continues, electronic commerce may become even more convenient.

¹⁵³ See David D. Haskell, "Closing the Indian Digital Divide," UPI (June 14, 2001).

¹⁵⁴ See *id.*

¹⁵⁵ See *id.*

¹⁵⁶ See, e.g., James Likeks, "No Grocery Money for the Nation's Poor? Let Them Eat Chips," *Star Tribune*, Jan. 14, 1995, at 14A. These criticisms died down, to some extent, after President Bill Clinton also embraced the idea. See "Clinton Embraces Idea of Laptops for Poor Kids," *The Record*, Mar. 24, 1995, at A20.