SURVEY

1996: SURVEY OF THE YEAR'S DEVELOPMENTS IN ELECTRONIC CASH LAW AND THE LAWS AFFECTING ELECTRONIC BANKING IN THE UNITED STATES

RICHARD L. FIELD*

TABLE OF CONTENTS

Synopsis ........................................ 968
Introduction .................................... 969
I. Recent Developments in U.S. Payment System Regulation ................................ 970
   A. State Laws ................................ 970
      1. U.C.C. Articles 3 and 4 ............... 970
      2. U.C.C. Article 4A ..................... 972
      3. U.C.C. Articles 5, 7, and 8 .......... 973
      4. U.C.C. Article 2B .................... 974
      5. NCCUSL Model Law on Electronic Commerce 975
   B. Federal Law and Regulations ............. 975
      1. Federal Reserve Board Regulation E .... 975
      2. Federal Reserve Board Regulation Z .... 978

This Article surveys the principal areas of electronic banking law development in the United States during 1996, providing a snapshot of U.S. laws relating to electronic money.
Part I focuses on U.S. laws and recent legal developments in electronic commerce payment. Part II addresses a wide spectrum of additional electronic commerce legal developments of interest to the financial industry, such as digital signature acts, cryptography export controls, and copyright protection.

INTRODUCTION

As the Internet accelerates its evolution from a purely academic utility to a primarily commercial one, there has been dramatically increased attention to Internet law and policy issues. These issues have focused on discrete areas, including banking, but there has been no comprehensive legislative effort to "tame" the Internet. Rather, legal developments have tended to occur in response to specific technological or business needs. Notably, these business needs include the need of the federal government to control its own costs better, in light of continuing deficit problems and the political difficulty of significantly increasing tax revenues. Separately, legislation has developed in response to a variety of social concerns.

At the start of 1996, electronic commerce technological developments clearly were leading and driving the legal discussions. Some activity in terms of hearings convened and task forces established occurred, but very little rulemaking in the area of electronic commerce law took place. In contrast, major developments were occurring weekly toward the end of 1996. They ranged widely from controls directed at morality, to controls directed at national security and crime, to those directed at electronic commerce and the payment systems. Consensus has not been reached on many fundamental issues. In significant areas no consensus even exists on how to proceed in defining the issues and establishing priorities. Digital cash and digital signatures are two such issues.

Financial institutions, although conservative by nature, are as aware as any industry of the potential, as well as the risks, in moving their business processes into the electronic world. Like other industries, they seek to develop new markets, to satisfy consumer desires, and to boost profitability by providing improved products and services and by lowering costs.

For banks, however, new technologies have a more fundamental impact. As a result of changes in technology, banks have seen once-secure franchises slip out of their exclusive control. The superior knowledge of—and resulting insight into—other industries and societies that has made banks valued intermediaries in risk assessment is no longer a special privilege of banks. By making vast quantities of
information much more widely available to non-banks, technology thus has eroded some of the unique value of bank intermediation.

One of the last traditional bank franchises is the payment system. There is no consensus on whether or to what extent the banks and the Federal Reserve Board ("FRB") will retain their traditional control over the creation, storage, movement, and settlement of money. It is clear, however, that once again advances in technology have opened a window of opportunity for non-banks to take a place at the payment table. It remains to be seen what part the banks' ultimate franchise, public trust, will play in the debate over control of these aspects of the payment system.

I. RECENT DEVELOPMENTS IN U.S. PAYMENT SYSTEM REGULATION

The payment systems of the United States are regulated under a complex matrix of federal and state laws. Some are intended to be comprehensive, such as the Uniform Commercial Code ("U.C.C.") Article 4A, which governs commercial wire transfers. Others are much more specific in their objectives, such as Federal Reserve Regulation E, which governs electronic funds transfer ("EFT") access to consumer bank accounts, and Federal Reserve Regulation Z, which governs credit cards and other types of bank lending. The principal U.S. payment system laws and regulations that are being examined with respect to electronic banking and commerce are summarized in the following subsections.

A. State Laws

1. U.C.C. Articles 3 and 4

The most mature payment system legislation, U.C.C. Articles 3 and 4, govern commercial paper, with an emphasis on (non-electronic) negotiable instruments, bank deposits, and collections. The U.C.C. was derived from still earlier banking and negotiable instrument laws, which in turn were derived in large part from English commercial law. The U.C.C. was drafted by a commission of academic and practicing lawyers and others, under the auspices of the National Conference of Commissioners on Uniform State Laws ("NCCUSL"), and has been

5. Id. art. 4.
updated and revised frequently over the past forty years.\textsuperscript{6} Efforts are made to encourage each of the fifty states to enact U.C.C. articles in a uniform manner. Although each state has enacted a version of the U.C.C., there is no longer complete uniformity. Dispute resolution, often requiring interpretation of specific U.C.C. provisions, generally is left to each state's courts. Although well-reasoned decisions of one court often are used to persuade other courts of the merits of a litigant's claim, decisions of a court located in one state are not binding on the courts of other states. Ultimately, U.C.C. provisions, that look alike may come to have different or even contradictory interpretations in the various states.

In addition, Articles 3 and 4 were redrafted recently to accommodate a number of changes, such as check truncation\textsuperscript{7} and electronic presentment.\textsuperscript{8} Although the majority of states have adopted these revisions,\textsuperscript{9} some, including New York, have not.

Article 3 embodies an important traditional principle of liability. Under Article 3, no person is liable on an instrument unless his signature (or that of his representative) appears on the instrument,\textsuperscript{10} or unless he subsequently ratifies the instrument.\textsuperscript{11} That is, the recipient generally assumes the risk of a forged instrument under Article 3. However, the negligence of the parties may be a factor in determining liability.\textsuperscript{12} This process is the first of three important models from the payment system that may be applicable to electronic commerce nonrepudiation.

Article 3 also establishes the rules and principles of negotiability. The concept of negotiability permits an innocent transferee who has paid for the instrument to enforce payment of the instrument, notwithstanding certain legal defenses that the drawer may have with respect to payment on the underlying transaction.\textsuperscript{13} This protection has permitted negotiable instruments to be accepted in trade without

\textsuperscript{6} See \textit{American Law Inst., Uniform Commercial Code}, at III (10th ed. 1987) (noting that NCCUSL has been responsible for U.C.C. for past forty years).
\textsuperscript{9} See \textit{U.C.C. art. 3} (amended 1990), 2 U.L.A. 3-5 (Supp. 1996) (listing states that have adopted revised Article 3); \textit{U.C.C. arts. 4, 4A} (amended 1990), 2B U.L.A. 3-5, 84-85 (Supp. 1996) (listing states that have adopted revised Article 4 and Article 4A).
\textsuperscript{10} See \textit{U.C.C. § 3-401(a)} (1990).
\textsuperscript{11} See \textit{id. § 3-403(a)}.
\textsuperscript{12} See \textit{id. § 3-406} (precluding assertion of forgery by person whose negligence substantially contributes to instrument's alteration).
\textsuperscript{13} See \textit{id. § 3-305}.
detailed inquiry into the business transaction that gave rise to the instrument. Negotiability, however, also allocates risk in a manner that has not been applied to electronic payments. It is likely that the Article 3 concept of negotiability will be the subject of serious future study in electronic commerce, provided that technical and public policy issues can be resolved. These open issues include the problem of duplication, as well as issues surrounding recordkeeping, auditability, and money laundering. Various groups, including the American Bar Association, Electronic Commerce Payment Committee (Section of Science and Technology), have begun to study issues in electronic negotiability.

There is general agreement among experts, confirmed by most of the case law, that Articles 3 and 4 traditionally have not covered electronic payments fully. In part, this interpretation hinges on the requirement that negotiable instruments must be in writing. State legislatures are beginning to see the introduction of proposals to expand the definition of a writing to include electronic writings. Under such an expanded definition, new forms of payment mechanisms such as the "electronic check" ultimately may be deemed to be governed by Articles 3 and 4.

2. U.C.C. Article 4A

Article 4A contains the U.S. rules for wholesale funds transfers. Between 1990 and 1996, it was enacted by forty-nine of fifty states. Article 4A was the first comprehensive legislation addressing


15. See U.C.C. § 3-104(a) cmt. 1 (defining "negotiable instrument" as promise to pay fixed amount of money, and "promise" as written undertaking to pay money).


17. U.C.C. art. 4A.

nonrepudiation of an electronic transaction. This statute was the first to recognize that, in the wholesale wire-transfer environment, the task of determining with certainty the actual identity of one's counterparty often is impossible. It establishes the second important model for electronic commerce nonrepudiation: the concept that a person may be bound by an unauthorized signature on a payment order, provided that satisfactory, prearranged procedures have been followed to identify him.19 The drafters of Article 4A recognized that they had formalized a new legal principle, and that they were abandoning the long-cherished protection embodied in Article 3.20 Accordingly, the statute treads carefully, by allocating liability for unauthorized transactions based, in part, on the level of security attained.21 A number of careful balances also are built into the statute.22 Article 4A remains, arguably, the most sophisticated statute enacted in any area of electronic commerce.

Because Article 4A expressly excludes most consumer payments, as well as debit orders and payment instructions transmitted through an intermediary (such as a merchant),23 experts believe that electronic checks, credit cards, and almost all forms of Internet consumer payments will come to be regarded as outside the scope of Article 4A.24

3. U.C.C. Articles 5, 7, and 8

There are ongoing efforts within NCCUSL, as well as other advisory organizations such as the American Bar Association ("ABA"), to update other articles of the U.C.C. Articles most relevant to payment include Article 5, Letters of Credit (revised 1995),25 Article 7, Warehouse Receipts, Bills of Lading, and Other Documents of Title (not recently revised),26 and Article 8, Investment Securities (revised

---

20. See id. art. 4A prefatory note (noting that bank customer can be held liable for unauthorized transactions if commercially reasonable security measures are provided by bank); see also id. §§ 4A-203 cmts. 1-2 (describing need for and scope of new rule).
21. See id. §§ 4A-201 to -203.
22. See, e.g., id. § 4A-203(a)(2).
24. See Sneddon, supra note 18, at 1112 n.14 (stating that debit transfers such as checks and drafts are not covered by Article 4A); R. David Whitaker, Key Issues and Considerations in Drafting Deposit Agreements and Funds Transfer Services Agreements for Financial Institutions, CONSUMER FIN. L.Q. REP., Winter 1996, at 37, 46 (noting that funds transfers that are subject to Electronic Funds Transfer Act of 1978 are exempted from Article 4A); see also 2B U.L.A. 457 (1991) (noting that payments governed by Article 4A overwhelmingly are between financial institutions).
1994). Some of these topics also are being studied by other organizations in which the United States has a role, such as the United Nations Commission on International Trade Law ("UNCITRAL").

A noteworthy new Article 8 was approved by NCCUSL in 1994. It establishes a system of regulation for securities held in certificated form, securities held by the issuing company in book-entry form, and, for the first time, securities held indirectly by a broker or other securities intermediary. The framework established in Article 8 may prove to be a particularly useful model for various categories of electronic money.

4. U.C.C. Article 2B

Article 2B currently is being drafted, and is considered at this point to be on a fast track toward completion. It had its first NCCUSL "reading" during the summer of 1996. Currently, its scope covers all licenses of information, as well as all contracts involving software (including sales of mass-market software). Its scope and form have changed considerably since its earliest drafts, and further changes and substantial debate are expected. Article 2B will have the greatest impact on the software industry and users of software. Due to heavy reliance on information and software within the financial industry, banks also will be affected significantly by this statute as both users and producers of information and software. New forms of banking products, such as intelligent agents, also may be governed by Article 2B.

27. U.C.C. art. 8 (1994).
32. See id. (reporting opposition to Article 2B from Consumer's Union following first reading at NCCUSL's annual meeting during summer of 1996).
33. See id. (explaining how Article 2B would validate "shrinkwrap licenses" used in retail software sales); see also Richard Raysman & Peter Brown, Shrinkwrap Licenses Revisited, N.Y. L.J., Aug. 13, 1996, at 3 (concluding that Article 2B will facilitate on-line commerce by allowing on-line contract formation).
5. **NCCUSL Model Law on Electronic Commerce**

NCCUSL recently announced its intention to draft a non-U.C.C. model law on electronic commerce. The scope of the model law was to be decided at the January 19-20, 1997, Executive Committee meeting. Electronic negotiability and electronic payment systems will not be addressed in the model law.\(^{34}\)

### B. Federal Laws and Regulations

#### 1. Federal Reserve Board Regulation E

With respect to stored value cards ("SVC"), consumer payment systems through the Internet, and perhaps electronic cash, Federal Reserve Board Regulation E\(^{35}\) ("Reg E") is the most important of the consumer protection regulations. It has been in effect since 1979, and was issued by the Federal Reserve under authority granted by Congress in the Electronic Fund Transfers Act of 1978.\(^{36}\) Reg E is primarily a consumer protection law. It establishes the basic rights, liabilities, and responsibilities of consumers who use electronic money transfer services and of financial institutions that offer these services.\(^{37}\) It also regulates other persons or entities who issue cards, codes, or other access devices to a consumer to be used for initiating EFTs to or from the consumer's account held by another financial institution.\(^{38}\)

Reg E presents the third payment system model that may be applicable to electronic commerce nonrepudiation. It protects an account holder absolutely (except for some statutory amounts),\(^ {39}\) and shifts the burden of proof that a withdrawal was authorized to the

---

34. See Memorandum from Patricia B. Fry, Chairperson, Drafting Comm., to NCCUSL Scope & Program Comm. (Jan. 7, 1997) (on file with The American University Law Review); Memorandum from Patricia B. Fry, Chairperson, Drafting Comm., to Drafting Comm. (Jan. 29, 1997) (on file with The American University Law Review) (confirming Executive Committee's decision to exclude these topics from scope of Act); see also Memorandum from ABA Sec. of Business Law Ad Hoc Task Force on Electronic Contracting, to Patricia B. Fry & Benjamin Beard, Members, Drafting Comm. (Dec. 10, 1996) (recommending that Model Law adopt electronic equivalents to negotiable instruments and documents of title).


37. See 12 C.F.R. § 205.1(b) (describing purpose and scope of Regulation E as directed primarily toward protecting rights of consumers engaged in electronic fund transfers).

38. See id. §§ 205.1, 205.2(i) (making regulation applicable to financial institution and defining such as person who provides access device and electronic fund transfers services).

39. See id. § 205.6(b) (limiting consumer's liability for unauthorized electronic fund transfers to lesser of $50 or amount of transfer unless consumer fails to notify financial institutions after discovery of loss or transmittal of periodic statement).
This protection exists even if the account holder's negligence enabled the unauthorized person to access the account. As a result, the bank cannot deny a claim by an account holder merely because he wrote his personal identification number ("PIN") on his card.

On May 2, 1996, the FRB proposed amendments to Reg E. These amendments would define, for the first time, the level of Reg E consumer protection for funds located on SVCs. They also would validate the use of electronic communications as writings under Reg E; for example, pre-authorized, recurring payments that currently must be approved in advance and in writing by the consumer, and must be confirmed by the financial institution in writing.

The proposed amendments would divide SVCs into three categories:

1. **Off-line unaccountable**: the card can be used independently; no database at the bank need be consulted;
2. **Off-line accountable**: the value on the card can be transferred off-line, but similar information on a central database also must be updated after the transaction occurs; and
3. **On-line accountable**: the card is used only to request a transfer at the bank's central database.

In general, the FRB has proposed that off-line unaccountable cards would not be regulated by Reg E, off-line accountable cards would be regulated minimally, with only disclosure to consumers required, and on-line accountable cards would be regulated under the current Reg E, with modifications. In addition, any card capable of storing a maximum of $100 would be exempted from the regulation.

---

40. See id. § 205.11(c)(1) (concerning investigation of errors).
41. See 12 C.F.R. pt. 205, Supp. I (Official Staff Interpretations); id. § 205.6(b).
42. See id. § 205.6(b) (noting that extent of consumer's liability is determined by promptness in reporting loss or theft of access device, not by degree of consumer negligence).
44. See id. at 19,698.
45. See 61 Fed. Reg. 19,662, 19,704 (proposing amendment to section 205.4(c)(2)); see also id. at 19,667 19,672, 19,692 (explaining that digital signatures or similar authentication can take place of written authorization for transfers from consumer's account).
47. See id. at 19,699.
48. See id. at 19,702.
49. See id. at 19,701.
50. See id. at 19,700.
51. See id. at 19,702 (suggesting exceptions for period statement regulations and change-in-terms notices).
52. See id. at 19,703.
The public comment period for the proposed Reg E amendments ended September 6, 1996. Finalization was not expected for at least a few months. Depending on the nature of the comments, proposals can be withdrawn or revised substantially. Regulation E observers believe that there was a fairly good chance that the amendments would not be finalized as proposed. Comments have been mixed, however. Some banks and bank-led organizations have favored the proposal, because it imposes only minimal obligations on banks. Others have criticized the proposed categorization of accounts as unworkable and not meaningful to consumers, or have questioned the wisdom of prematurely regulating a still-evolving service.53

Congress apparently shared that assessment. A provision deep within the September 9, 1996, Omnibus Appropriations Act prohibits the FRB from taking any action to finalize amendments to regulations under the Electronic Fund Transfers Act ("EFTA") that would regulate electronic stored value products until at least July 1997.54 The FRB is required to conduct a study of electronic stored value products that evaluates whether provisions of the EFTA could be applied to such products without adversely affecting the cost, development, and operation of such products. In conducting its study, the FRB must consider whether alternatives to regulation under the EFTA, such as allowing competitive market forces to shape the development and operation of electronic stored value products, could achieve the objectives embodied in the Act more efficiently. A report of its study is to be submitted to Congress no later than April 1997.

Meanwhile, the European Community has been developing Commission Draft Recommendations addressing some of the same issues as the proposed Reg E amendments and concerning payments effected through a payment card—including pre-paid cards—and payments by means of an electronic payment facility without a payment card.55 Articles in the latest working draft generally cover the following subjects: scope; definitions; minimum information contained in the terms and conditions governing the issuing and use of a payment card or an electronic payment facility; information

53. See Give Us a Few Guidelines Please, CREDIT CARD MGMT., Sept. 1, 1996, at 24 (noting that regulation of stored value generally is considered a positive development, but that regulators should wait).
subsequent to a card payment or payment by means of electronic payment facility; obligations of the holder or user; liabilities of the holder or user; obligations of the issuer or system provider; liabilities of the issuer or system provider; notification; and redress.

2. Federal Reserve Board Regulation Z

Federal Reserve Board Regulation Z ("Reg Z")\(^{56}\) regulates credit card practices, as well as other types of lending. Its credit card rules are similar to the Reg E rules governing access to a bank account.\(^{57}\) Specifically, it regulates issuance of credit cards and limits the liability of a cardholder for unauthorized use.\(^{58}\) In addition, it grants cardholders extensive rights to assert claims or defenses against a card issuer;\(^{59}\) and it establishes procedures for resolving billing errors.\(^{60}\)

It is clear that the use of credit cards over the Internet, such as in MasterCard’s and Visa’s Secure Electronic Transaction ("SET") approach,\(^{61}\) will be regulated under Reg Z. To the extent these cards may be issued or advertised electronically, various interest rate disclosure and other rules will apply. The Reg Z commentary is updated periodically, and is expected to address novel issues that arise through Internet credit card use.

3. Regulations CC, D, J, and operating circulars

These additional Federal Reserve rules also address payment issues and are updated frequently. Regulation CC ("Reg CC"), Availability of Funds and Collection of Checks\(^{62}\), primarily mandates when a financial institution must make various types of deposits available for withdrawal by its customer. In general, it shortens the length of time a financial institution may hold funds, when compared to prior practices.\(^{63}\) In order to mitigate the risk of fraud against financial institutions, the FRB also received new authority to regulate the


\(^{57}\) See Electronic Fund Transfers, 12 C.F.R. pt. 205.

\(^{58}\) See id. § 226.1(b) (stating that purpose of regulation is to promote informed use of consumer credit by requiring disclosures about terms and costs).

\(^{59}\) See id. (noting that, for example, regulation gives consumers right to cancel certain transactions).

\(^{60}\) See id. § 226.13 (giving examples of billing errors).


\(^{63}\) See id. § 229.1 (stating that regulation contains rules to expedite collection and return of checks by banks).
collection and return of checks. Reg CC establishes new legal and operational principles designed to expedite the collection and return of checks. As a result, it preempts portions of U.C.C. Articles 3 and 4.

Regulation D ("Reg D"), Reserve Requirements of Depository Institutions, requires that depository institutions set aside reserves to cover a percentage of their transaction account balances, such as checking accounts. Non-transaction account balances, such as savings accounts, require little or no reserves. Permitting remote access to an account, such as by computer or telephone, may require it to be classified as a transaction account. A reserve requirement analysis pertaining to SVCs also may be forthcoming, although no proposal has been announced.

Regulation J ("Reg J"), Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers through FedWire, describes the FRB's responsibilities in its check collecting and FedWire services.

A series of operating circulars issued and frequently revised by each federal reserve bank details the specific rules and requirements of a large number of FRB operational and payment services.

4. Federal Deposit Insurance Corporation ("FDIC")

On August 2, 1996, the FDIC published its General Counsel's Opinion No. 8. The opinion sets forth the Legal Division's conclusions on whether and under what circumstances funds underlying SVCs may be considered deposits under the Federal Deposit Insurance Act ("FDIA"). The FDIC declined to follow the categories proposed by the FRB for SVCs. Instead, for purposes of analyzing deposit insurance coverage, the General Counsel's Opinion

65. See 12 C.F.R. §§ 229.30 to -.42.
66. See id. § 229.41.
67. Id. pt. 204 (1996).
68. See id. § 204.1.
69. See id. § 204.3 (addressing computation and maintenance of required reserves).
70. See id. § 204.2(e).
73. See id. § 210.1.
74. See generally U.C.C. § 4-103 (1987) ("The term 'operating letters' means these 'letters of instructions,' sometimes called 'operating circulars,' issued by the Federal Reserve Bank.").
76. See id. at 40,490 (noting that FDIC's departure from FRB's classification system is "not intended as a criticism or rejection" of that method).
classified all SVC systems into four different categories\textsuperscript{77} based on the statutory definition of "deposit" in the FDIA.\textsuperscript{78} The categories are:

(1) Bank Primary—Customer Account System: in which the funds underlying the SVC remain in a customer's account until the value is transferred to a merchant, who, in turn, collects the funds from the customer's bank,\textsuperscript{79}

(2) Bank Primary—Reserve System: in which the funds are withdrawn from a customer's account (or paid directly by the customer) and paid into a reserve or general liability account held at the institution to pay merchants as they make claims for payments,\textsuperscript{80}

(3) Bank Secondary—Advance System: in which the electronic value is created by a third party and is provided to the depository institution to make available to its customers. As customers exchange funds for electronic value, the funds are held for a short period of time and then forwarded to the third party,\textsuperscript{81} and

(4) Bank Secondary—Pre-Acquisition System: in which the electronic value is created by a third party and the depository institution exchanges its own funds for electronic value from the third party and, in turn, exchanges electronic value for funds with its customers.\textsuperscript{82}

The General Counsel's Opinion concludes that in most cases SVCs are not protected by deposit insurance.\textsuperscript{83} However, a banking institution could design an SVC in such a way that the underlying funds would be insured. For example, if the funds represented by the card are maintained in the customer's own account until a payment is made, deposit insurance would apply. In such a situation, institutions would be required to tell customers whether the card they are buying is insured or not.

The FDIC also asked for public comment on a variety of electronic payment system issues, including concerns raised by Internet banking and the use of electronic cash.\textsuperscript{84} In addition, the FDIC asked for comment on whether the agency should, by future regulation, determine that SVCs are entitled to deposit insurance if they are

\textsuperscript{77}See id.; infra notes 79-82 and accompanying text (listing four categories of SVC systems).


\textsuperscript{79}See id. at 40,490.

\textsuperscript{80}See id.

\textsuperscript{81}See id.

\textsuperscript{82}See id.

\textsuperscript{83}See id. at 40,494 ("The FDIC would expect that institutions clearly and conspicuously disclose to their customers the insured or non-insured status of their stored value products.").

treated as insured deposits under general usage. In considering whether to promulgate such a regulation, the FDIC would weigh a number of policy issues, including the level of public confidence in the new payment systems, consumer expectations, and the similarities between SVCs and other payment mechanisms.

The General Counsel’s Opinion is well reasoned. It also is difficult to understand, and therefore is not very meaningful to the consumers whom it is intended to protect. The FDIC likely will use its general authority to develop a simpler test for SVCs. It may go so far as to ask Congress to rewrite the law in order to cover SVCs directly.

5. Comptroller of the Currency

The Office of the Comptroller of the Currency ("OCC"), in a July 1, 1996, interpretive letter, granted its permission for nationally chartered banks to design, build, and operate a system of electronic tollbooths.

On September 10, 1996, the OCC issued Guidelines on SVCs. The Guidelines emphasized adherence to the payment system risk factors previously identified by the OCC.

6. Bank Secrecy Act regulations

On January 3, 1995, the Financial Crimes Enforcement Network ("FinCEN") of the Department of the Treasury and the Board of Governors of the Federal Reserve System jointly adopted a final rule requiring financial institutions to collect and retain certain information pertaining to transmittals of funds. This enhanced recordkeeping requires institutions to collect and retain for five years customer and beneficiary information regarding wire transfers in amounts of $3000 or more. Because fund transfers of under $3000 are not covered by the rule, initially most Internet payment systems will be unaffected.

---

85. See id. at 40,497 (specifying policy issues to be considered in comments).
86. See OCC Interpretive Letter No. 731 (July 1, 1996).
88. See id.
90. See id. at 229.
91. See id. at 230.
On September 19, 1996, the Treasury announced two new initiatives: a consumer protection study; and a development of G7 international cooperation issues.

C. Private Sector Rules

Private sector payment system rules, such as those for Visa, MasterCard, the National Automated Clearing House Association ("NACHA"), and the Clearing House Interbank Payments System ("CHIPS"), contain many additional member requirements. NACHA, notably, has been revising its rules and capabilities in order to accommodate financial Electronic Data Interchange ("EDI") transaction set information, for the purpose of enabling electronic commerce. MasterCard and Visa are in the process of finalizing their SET documents for secure Internet credit card payments and other transactions.

II. RECENT DEVELOPMENTS IN OTHER AREAS OF ELECTRONIC BANKING AND COMMERCE

A. Electronic Contracting and Digital Signatures

Historically two initial types of legal barrier to the development of widespread electronic contracting and electronic commerce exist: (1) the paper-based requirements of many current laws and regulations; and (2) the absence of a legal infrastructure governing electronic commerce applications.

First, many traditional laws and regulations written prior to the electronic information age, impose paper-based requirements relating to the form of documents and communications. The Statute of Frauds, for example, first enacted in England in 1677 and incorporated into a number of areas of U.S. law, requires that certain documents must be in writing to be enforceable. These documents include: (1) contracts for the sale of goods in excess of $500; (2) contracts that, by their terms, cannot be completed within one year; (3) contracts for the sale of land; (4) contracts that guaran-

93. See supra note 61 and accompanying text (discussing use of Visa and MasterCard on Internet and providing cites to Internet pages of MasterCard and Visa).
95. See id. § 110(2)(a).
96. See id. § 110(1)(e).
97. See id. § 110(1)(d).
ty the debts of another person;\textsuperscript{98} and (5) certain other contracts, such as agreements made in contemplation of marriage.\textsuperscript{99}

U.S. law also commonly requires that certain documents be signed, specifically at the bottom of the document,\textsuperscript{100} and that the original document be used for official purposes, retained for a specified number of years, or both.\textsuperscript{101} There is substantial concern, as well, that business documents be admissible as valid evidence in court.\textsuperscript{102} Once admitted, they should have appropriate probative value.\textsuperscript{103}

Finally, there has been some confusion over how and when an electronic contract is created, as well as its enforceability.\textsuperscript{104} The legal community has been studying the underlying purposes of these types of laws, with a goal of developing equivalent characteristics of authenticity, ceremony, approval, and efficiency in the electronic environment.\textsuperscript{105} Evidentiary and nonrepudiation issues have received substantial focus.\textsuperscript{106}

Laws and regulations at the federal, state, and local levels are being revised to accommodate these fundamental concerns. The payment laws already have been expanded to cover electronic signature equivalents and the absence of writings.\textsuperscript{107} The laws of evidence, both at the state and federal levels, now permit the introduction of electronic records and documents.\textsuperscript{108} The Federal Acquisition Regulations ("FAR") have been modified to permit electronic bidding and contracting in contracts with the federal government.\textsuperscript{109} Most federal government agencies have addressed the use of electronic

\textsuperscript{98} See id. § 110(1)(b).
\textsuperscript{99} See id. § 110(1)(c).
\textsuperscript{100} See, e.g., U.C.C. § 2-201(1) (1990).
\textsuperscript{101} See, e.g., 15 C.F.R. § 762.4 (1996).
\textsuperscript{103} See id. § 185 (stating that to be admissible, evidence must have probative value, with tendency to establish proposition that it is offered to prove).
\textsuperscript{107} See, e.g., U.C.C. § 4A-201 (1990).
records and documents. And states such as California have enacted legislation permitting the use of electronic signatures in communications with public entities.

The second type of barrier to widespread electronic commerce is the absence of a legal infrastructure at the application level. This absence has created confusion and a hesitation to develop electronic commerce applications for fear that they will be subject to an unknown risk or illegality. The main focus at this level has been the Public Key Infrastructure ("PKI") and digital signatures.

There is increasing consensus that digital signatures are an appropriate solution for many problems in electronic commerce. They can be used to authenticate the accuracy of a message that has been transmitted via unsecure communication facilities, such as the Internet. They also can be used to authenticate the sender of a message, and thus provide to the recipient protection against

---

110. See, e.g., 7 C.F.R. § 729.407 (1996) ( obligating farmers to maintain records, including electronic records, of their peanut crops); 12 C.F.R. § 12.3 (1996) (requiring banks to maintain records sufficient for an audit, including through electronic means); 36 C.F.R. § 1222.48 (1996) (mandating that contractors deliver to federal agencies sufficient technical documentation to support electronic records).

111. See CAL. GOVT CODE § 16.5 (West Supp. 1996). A digital signature has the same force and effect as a manual signature provided that:
   (1) It is unique to the person using it.
   (2) It is capable of verification.
   (3) It is under the sole control of the person using it.
   (4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.
   (5) It conforms to regulations adopted by the Secretary of State.

Id. New York has proposed a similar law. See S.B. 7420, 219th Leg., 2d Reg. Sess. (N.Y. 1996) (authorizing use of digital signatures in communications with public entities and according them same weight as manual signatures).

112. See infra notes 149-50 and accompanying text (discussing Federal PKI Steering Committee).

113. See infra notes 120-38 and accompanying text (explaining use of digital signatures and surveying state laws relating to digital signatures).


115. See Richard Raysman, Digital Signatures: Time-Saving Technology at Your Fingertips, TRUSTS & ESTATES, Apr. 1996, at 5 ("Digital signatures will increase the accuracy, efficiency and economy of financial and commercial transactions . . . ."); M.A. Stapleton, Panel: Law Needed on Digital Signatures, CHI. DAILY L. BULL., Sept. 10, 1996, at 1 (suggesting that electronic commerce succeeds because signatures give consumers confidence to transact business over the Internet); supra note 114 and accompanying text.
repudiation by the apparent sender.\textsuperscript{116} Finally, through the use of
a trusted third party Certification Authority ("CA"), they can allocate
the risk of error or fraud in a manner suitable to the application for
which the digital signature is being used.\textsuperscript{117} Securing the message,
instead of the entire communications system, is widely believed to be
a natural and desirable evolutionary step.\textsuperscript{118}

The leading academic study of digital signature law was carried out
by the Information Security Committee of the American Bar
Association, Section of Science and Technology (in consultation with
international legal and technology experts) over a period of four
years. The Committee published a final version of its \textit{Digital Signature
Guidelines} on August 1, 1996.\textsuperscript{119} The \textit{Guidelines} previously had been
distributed widely in draft form, and have been influential in
advancing United States and international development of PKI
thinking. They have formed the basis of digital signature legislation
in a number of states. Utah was the first state to pass a law authoriz-
ing the use of digital signatures in commerce, making extensive
reference to the \textit{Guidelines}.\textsuperscript{120} Early drafts of the proposed German
digital signature law also cited the \textit{Guidelines}.\textsuperscript{121}

In addition to California and Utah, widely varying forms of digital
signature legislation have been enacted in the following states:

\begin{itemize}
  \item \textsuperscript{116} See generally Henry H. Perritt, Jr., \textit{Legal and Technological Infrastructures for Electronic Payment Systems}, 22 \textit{RUTGERS COMPUTER & TECH. L.J.} 1 (1996) (calling for technological infrastructure that guards against forgery of signatures, thereby protecting recipients from repudiation); Henry H. Perritt, Jr., \textit{President Clinton's National Information Infrastructure Initiative: Community Regained?}, 69 \textit{CHI.-KENT L. REV.} 991, 1006-07, n.43 (1994) (acknowledging that authentication is a problem confronting any market not reliant on face-to-face transactions).
  \item \textsuperscript{117} See generally Theodore S. Barassi, \textit{Cybernotary: Addressing Technical Problems with On-Line Commerce; A Brave New Area of Specialization for Lawyers?}, \textit{COMP. L. STAT.}, Mar. 1996, at 1 (suggesting that certification authorities ("CA") will form "trust backbone" of all electronic transactions conducted over the Internet); Froomkin, supra note 106, at 55 (examining pivotal role of CAs for proper functioning of electronic commerce).
  \item \textsuperscript{118} See generally \textit{DIGITAL SIGNATURE GUIDELINES}, supra note 105.
  \item \textsuperscript{119} See id. at 36; see also ABA Section Creates First Digital Signature Guidelines to Aid in Security of the Internet (last modified Dec. 20, 1996) <http://dev.abanet.org/media/dec96/dsg.html> (on file with \textit{The American University Law Review}).
  \item \textsuperscript{120} See \textit{UTAH CODE ANN.} § 46-3-101-46-3-504 (1995), as amended by S.B. 188, 52d Leg., Gen. Sess. (Utah 1996) (facilitating commerce by means of reliable electronic communications, including digital signatures).
  \item \textsuperscript{121} See generally Germany Drafts Multimedia Law Regulating Internet, \textit{REUTERS BUS. REP. (BONN)}, Nov. 11, 1996, available in LEXIS, News Library, Non-US File (reporting that German government has drafted multimedia law to regulate Internet content and to establish widespread use of digital signatures). The bill was approved by German Chancellor Helmut Kohl's cabinet on December 11, 1996. \textit{See Terrence Gallagher, Bonn Aims to Rein in Lawlessness in Cyberspace, REUTER EUR. COMMUNITY REP. (BONN), Dec. 12, 1996, available in LEXIS, NEWS Library, NON-US File.}
Arizona,¹²² Connecticut,¹²³ Florida,¹²⁴ Hawaii,¹²⁵ Iowa,¹²⁶ Louisiana,¹²⁷ Virginia,¹²⁸ and Washington.¹²⁹ Legislation has been introduced or planned in Georgia,¹³⁰ Illinois,¹³¹ Massachusetts,¹³² Michigan,¹³³ New York,¹³⁴ Oregon,¹³⁵ and Rhode Island.¹³⁶ Other states reportedly have begun to study the issue.¹³⁷ Although a few states are following the sophisticated Utah model of regulating the CA industry, most are opting for simpler, more generic

¹²² See ARIZ. REV. STAT. § 41-121 (Supp. 1997) (authorizing Secretary of State to accept digital signatures for documents filed with the office of the Secretary of State).
¹²⁴ See FLA. STAT. chs. 292.70-.74 (Supp. 1997) (creating standards and definitions for digital signature use in Florida).
¹²⁵ See S.B. 2401, 18th Leg. (Haw. 1996), available in LEXIS, STATES Library, ALLCDE File (establishing legal framework for using digital signatures as a means of authenticating computer information).
¹³⁷ See, e.g., DEL. CODE ANN. tit. 6, § 1409 (1997) (authorizing Secretary of State to accept electronically transmitted signatures for state filings); OKLA. STAT. tit. 65, § 1-722 (Supp. 1997) (validating physician's electronic signature on medical records, provided that signature is generated by confidential code that only user possesses); N.D. CENT. CODE § 31-08-01.2 (Supp. 1995) (allowing authentication of medical records by electronic signature, so long as appropriate safeguards have been taken to limit access to records); S.B. 454, 76th Leg., 1996 Reg. Sess. (Kan. 1996), available in LEXIS, LEGIS Library, TRCK96 File (enabling director of taxation to accept electronic signatures).
legislation or are limiting themselves to specific types of electronic documents.¹³⁸

Some states and companies are seeking to enable biometric-based forms of signature, in addition to encryption-based signatures.¹³⁹ Because biometric signatures cannot be stolen, lost, or forgotten, they are expected to play a significant role in the future. There is continued concern, however, over personal privacy and the potential misuse of biometric information and databases.¹⁴⁰ The Chase Manhattan Bank, for example, now is using voiceprint identification for its retail customers in branches to expedite customer identification at teller windows.¹⁴¹ It is not yet using voiceprints for legal signature purposes, but it hopes to use the technology in the near future to permit remote telephone transactions.¹⁴² Because voiceprints are less intrusive than fingerprints or retina scans and are less likely to find their way into any form of national database, they have been comparatively well received by customers.¹⁴³

Finally, methods are being developed to apply digital signatures as a means to identify and register objects of value. Verification Technologies, Inc., of San Francisco, has created such a technique to

¹³⁸ An on-line comparison and review of state digital signature laws is available at the State of Massachusetts digital signature law and policy web page. See Legislative Matrix (visited Jan. 28, 1997) <http://www.magnet.state.ma.us/itd/legal/matrix10.html> (on file with The American University Law Review). Massachusetts also has a draft plan for digital signature legislation, but has not yet introduced the law. See supra note 132.

¹³⁹ See generally Sherry L. Harowitz, Biometrics: More than Meets the Eye, SEC. MGMT., Feb. 1993, at 24 (exploring various forms of biometric security procedures, including voiceprint identifications and retinal scans); Emma Newham, Knowing Me Knowing You: Security Systems, COMM. INT’L, Apr. 1996, at 55 (describing biometrics as highest level of security that exploits a person’s physical characteristics to provide a foolproof method of verifying identities).

¹⁴⁰ See A Credit Union Points a Finger at Biometrics, BANK NETWORK NEWS, Jan. 13, 1997, at 1 (noting difficulty in convincing customers that enrolling their fingerprints in credit union’s trial biometric identification program does not infringe on their privacy); Unitime Systems, Inc. Releases Affordable Biometric Timeclock Technology, BUS. WIRE, Nov. 8, 1996, available in LEXIS, NEWS Library, WIRES File (attempting to alleviate privacy concerns by introducing biometric fingerprint technology that reads only spots off fingerprint rather than whole print, thereby providing enough information for time-keeping purposes but not enough information for use by the government); John D. Woodward, Biometrics Offers Security—But Legal Worries, Too, AM. BANKER, Aug. 23, 1996, at 11 (noting that many people believe turning over their fingerprints or retina patterns to a credit card company seems “too Orwellian for comfort,” and suggesting that financial institutions promise their customers that biometric identification information will be for institution’s use only and will not be disseminated in any form to third parties).

¹⁴¹ See Woodward, supra note 140, at 11 (acknowledging that Chase Manhattan employs voiceprint authentication technology); see also Moscom and Chemical Bank to Commence Voice Verification, Press Release, Mar. 21, 1996; CHEMICAL BANK, INTRODUCING XTRA SECURE, A VOICE VERIFICATION SYSTEM (brochure) (May 1996).


¹⁴³ See id.
identify securely gems, artwork, and other objects. No new legal infrastructure is needed, but it is expected that courts would give substantial weight to such evidence under existing law in cases of criminal theft or forgery.

A related U.S. development is the proposed creation of a "cybernotary." A cybernotary would be a person or firm with the capability to authenticate international electronic transactions. Because the cybernotary would combine the key authentication functions of a CA with the contract validity assurances of a lawyer, the ABA currently is considering the recognition of a new legal specialty in this area. Substantial assistance has been provided by the International Union of Latin Notaries, which is expanding the cybernotary concept internationally.

A federal PKI Steering Committee has been organized to coordinate efforts by executive agencies to use public key digital signature technology. It has established a Technical Working Group to consider the technical issues associated with a federal PKI. The Technical Working Group has announced that it expects the X.509 certificate to be the predominant vehicle for digital signatures in general electronic commerce.

The United States Postal Service is developing "Postal Electronic Commerce Services" that will provide security and integrity to...
electronic correspondence and transactions, giving them attributes usually associated with first-class mail. As part of this effort, the Postal Service is testing a limited prototype of an electronic postmarking service that will offer customers a third-party validation of the time and date that an electronic mail document was received by the Postal Service. Further, the prototype will validate the existence of a document by ensuring that it was not changed after its handling by the Postal Service. The test is intended to be concluded within sixty days, although it may be extended. To provide guidance for implementing the test, the Postal Service has proposed to add new regulations to title 39 of the Code of Federal Regulations. Commercial banks, the largest U.S. users of first-class mail, have the potential to become an important user of this type of service.

Notably, the Postal Service withdrew from its prior announcements its offer of general CA services. It advised that it might offer general CA services at a later time if a market for such services developed.

The United States also has taken an active role in international efforts in the areas of electronic contracting and digital signatures. Two such efforts have been through the auspices of the United Nations and the International Chamber of Commerce ("ICC").

In the United Nations, the UNCITRAL Model Law on Electronic Commerce was completed by UNCITRAL in June 1996. It was approved by the United Nations General Assembly in December 1996, by non-vote resolution. The UNCITRAL Model Law primarily addresses the level-one barriers to legal recognition of data messages. It has been crafted carefully and is a valuable model for commercial transactions, as well as special rules governing electronic bills of lading.

151. See Gary H. Anthes, Postal Service Plugging in to On-line Potential, COMPUTERWORLD, Jan. 22, 1996, at 1A.


154. See Bankers Bash Post Office Move into E-Commerce, FIN. NETNEWS, Sept. 16, 1996, at 7 (addressing banks' concerns that postal service will try to shift its monopoly on first-class mail into electronic forum and force banks to do business with it).

155. In May 1996, the Postal Service had announced that it would serve as a CA to verify users and would add tamper-proof digital identification numbers to a "smart disk," which contains encryption software. See Gary H. Anthes, Feds to Secure Net Access, COMPUTERWORLD, May 27, 1996, at 69.


158. See id. (covering validity of computer messages in commercial transactions).
national legislation in this area. In the United States, such legislation is more likely to be enacted at the state level.

The ICC has initiated Project E-100, intended to address international commercial policy and techniques of interest to the business community. Project E-100 includes two working groups: an ETERMS working group that is developing standard electronic commerce terminology as well as a registry for electronic commercial documents, and a Uniform International Authentication and Certification Practices working group that is developing practice guidelines. The ICC also is working on standards for incorporation by reference, a necessity when considering public key certificates that are intended to incorporate underlying Certification Practice Statements or other computer-readable EDI documents.

One additional barrier to the use of on-line contracts has been a continued question as to their enforceability. This debate follows similar questions about the enforceability of "shrink-wrap" licenses, which are standard form licenses distributed inside a software or similar package. Reversing a trend in recent court rulings that held shrink-wrap licenses to be unenforceable, a federal appeals court recently upheld the enforceability of a shrink-wrap license. In the case of ProCD v. Zeidenberg, the Seventh Circuit Court of Appeals endorsed the practice of shrink-wrap licenses, reversing the holding

---

159. The ICC E-100 Project is an international, multidisciplinary effort to study, facilitate, and promote the emerging global electronic trading system. Existing ICC Commissions participating in the E-100 Project include the commissions on Banking, Air Transport, Maritime and Surface Transport, Computing, Telecommunications and Information Policies, Commercial Practices, Financial Services, and Insurance all of which seek to provide a globally comprehensive approach to implementing digital commerce. Six E-100 working groups have been formed to examine specific critical issues in the context of digital commerce including: (1) the ICC Working Party on Electronic Credits; (2) the ICC Working Party on Open Account Trading; (3) the ICC Working Party on Electronic Transport Documents; (4) the ICC Working Party on Legal and Regulatory Affairs; (5) the ICC Working Party on E-terms; and (6) the ICC Working Party on Digital Authentication. The American affiliate of the ICC is the U.S. Council for International Business, headquartered in New York. The International Chamber of Commerce is headquartered in Paris. Information about ICC activities is available at <http://www.iccwbo.org>.


162. See supra note 160.

163. See Lockhart & Miles, supra note 104, at 516.


165. 86 F.3d 1447 (7th Cir. 1996).
of the trial court. To the extent the reasoning of the ProCD case applies also to on-line licenses, it is expected that these licenses will be upheld with the following caveats: that customers are put on notice of the license agreements; that there is an opportunity to review the terms of the agreement prior to acceptance; and that the conduct constituting acceptance is specified clearly.

Finally, a clear validation of on-line contracts would be contained in U.C.C. Article 2B, as it currently is being drafted.

B. Regulation of Cryptography

The use of cryptography, which until recently was presumed to have primarily military application (with special accommodation to the banking industry), has become a fundamental requirement of electronic commerce. It also lies close to the hearts of privacy and anonymity advocates, and to those who believe the government has no right to read private communications. During the past few years, cryptography regulation has become one of the most passionate issues in U.S. electronic commerce. Events have unfolded like a pulp novel, and each chapter has been followed closely and analyzed extensively to uncover the slightest real or imagined motivations and strategies.

The domestic use of cryptography is not regulated in the United States. However, export of cryptography applications is strictly regulated and often prohibited under a set of trade regulations created after World War II and updated frequently.

Two Executive Branch agencies are primarily responsible for cryptography export regulation. The Department of State has issued the International Traffic in Arms Regulations ("ITAR"), which

167. See id. at 1452 (holding that opportunity to review terms of the contract and conduct constituting acceptance was specified clearly because "the software splashed the license on the screen and would not let him proceed without indicating acceptance").
169. See John C. Hoag, Oasis a Mirage of Reliability, 134 FORT. 1 (1996) ("While cryptographic technology appears readily available, its use so far has been limited by the U.S. Government as a 'munition.'); see also Office of the Press Secretary, Press Release on "Clipper Chip" Encryption Initiative, Apr. 19, 1993, at 1, 2, available in 1993 WL 357773 ("[I]t is not to protect electronic funds transfer.").
contains a Munitions Control List of controlled military articles, including cryptography.\textsuperscript{172}

Items and technology that are not controlled by ITAR may be regulated under the Export Administration Regulations ("EAR"),\textsuperscript{173} issued by the Commerce Department. Regulated items include some types of cryptography used by banks in their ATM networks or for signature or message authentication purposes.\textsuperscript{174} Recently, the regulations were restructured and reorganized.\textsuperscript{175}

The National Security Agency ("NSA"), branches of the U.S. military, and others advise regulators on cryptography export issues.\textsuperscript{176} In practice, the NSA retains substantial control over U.S. cryptography export policy.\textsuperscript{177} Enforcement of export policy is assigned to the U.S. Customs Service.\textsuperscript{178} United States shipments, transmissions, and disclosures of hardware, software, and technical data to a location abroad are considered regulated exports.\textsuperscript{179} Re-exports of U.S.-origin materials also are regulated,\textsuperscript{180} as are disclosures to foreign nationals within the United States.\textsuperscript{181} Some of the major U.S. financial institutions have developed a working understanding of these extremely complex regulations, but many others remain only vaguely aware of the requirements. Nevertheless, banks increasingly find themselves needing to export computer and telecommunications equipment, as well as software, under these regulations. As cryptography use becomes common in consumer banking, the need will be even greater.

Indeed, the NSA's Office of Information Security Research and Technology, Cryptology Division, recently released a research monograph entitled \textit{How to Make a Mint: The Cryptography of Anony-
It reviews the basic cryptography of anonymous cash, as well as the cryptography of optional features such as transferability, divisibility, and multiple spending prevention.

The NSA long has been concerned about the potential for widespread proliferation of strong encryption programs. In 1993 it first announced the Clipper Chip, which was to be a standard encoding device. The original Clipper proposal (informally called “Clipper I”) used a government-provided undisclosed encryption algorithm. Keys would be issued by the government, and two government agencies each would retain half of the key. Complete keys were to be available to any government agency only with good cause, and only in accordance with proper judicial or agency process. Use of other encryption systems was to be permitted domestically, but permission to export was likely to be denied.

Clipper I received an extremely negative public reaction, and was withdrawn. Modified Clipper proposals followed. The “Clipper II” proposal would have required the escrow of keys with a third-party escrow agent as a condition of export. As with Clipper I, the government would have access to keys (informally referred to as “GAK”) in accordance with legal process. No clear distinction was

183. See id. at 1137-43.
184. See id. at 1149-51.
185. See id. at 1151-54.
186. See id. at 1154-55.
187. See Singhal, supra note 170, at 194; see also Charlene L. Lu, Note, Seeking Privacy in Wireless Communications: Balancing the Right of Individual Privacy with the Need for Effective Law Enforcement, 17 HASTINGS COMM. & ENT. L.J. 529, 544 (1995) (noting that Clipper Chip was developed to strike a balance between privacy and government’s ability to intercept communications).
188. See Rustad & Eisenschmidt, supra note 168, at 235 (describing odyssey of government’s Clipper Chip).
189. See id.; Edward L. Radio, Legal Issues in Cryptography, 13 COMPUTER LAW. 1, 8 (1996) (explaining that this aspect of key escrow system was highly controversial).
190. See Rustad & Eisenschmidt, supra note 168, at 235.
192. See Lawrence Lessig, Symposium, Emerging Media Technology and the First Amendment: The Path of Cyberlaw, 104 YALE L.J. 1743, 1755 (1995) (explaining that reaction to Clipper has been devoted mostly to stopping it).
made between keys used to sign documents and encryption keys. Public reaction to Clipper II was almost as negative as reaction to Clipper I.\textsuperscript{195}

In an effort to bolster its position, the Department of Defense, together with the National Institute of Standards and Technology ("NIST"), commissioned the National Research Council ("NRC") to study national cryptography policy. The NRC is a private entity whose members are drawn from the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. A highly respected NRC committee drafted a comprehensive report, entitled *Cryptography's Role in Securing the Information Society*, which was released in prepublication form on May 30, 1996.\textsuperscript{196} The recommendations of the NRC Report are included as the Appendix of this article.\textsuperscript{197}

The NRC recommended a substantial shift in emphasis in favor of commercial use of cryptography, and a relaxation of cryptography export controls.\textsuperscript{198} Nevertheless, it was all but ignored by the Administration in its Clipper III proposal, also released in May 1996, which permitted export of up to sixty-four bits with escrow.\textsuperscript{199} The latest proposal (Clipper IV), announced by Vice President Al Gore on October 1, 1996, and formalized by a November 15, 1996, Executive Order, directs a number of changes to cryptography export policy, effective December 30, 1996.\textsuperscript{200} Major features of the new policy include:

---

\textsuperscript{195} See Robyn Blumner, *Under Clinton, Government Is All Ears*, COMM. APPEAL, Aug. 11, 1996, at B5 (claiming that Clipper Chip is the most notorious of proposals to invade privacy); Art Kramer, *Netwatch the AJC's Daily Online Guide Privacy Advocates Again Protest White House Idea of "Key Escrow,*" ATLANTA J. & CONST., May 21, 1996, at D3 ("Clipper II . . . provided widespread objection from electronic privacy advocates.").

\textsuperscript{196} COMMITTEE TO STUDY NATIONAL CRYPTOGRAPHY POLICY, NATIONAL RESEARCH COUNCIL, *CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY* (prepublication copy, May 1996). The text of the Committee's recommendations are reprinted at the Appendix, infra pp. 1025-26.

\textsuperscript{197} See Appendix, infra pp. 1025-26.

\textsuperscript{198} See Appendix, infra pp. 1025-26.


(1) transfer of jurisdiction over encryption export licensing to the Department of Commerce, granting the Department of Justice a formal vote in the process;201

(2) permission to export 56-bit encryption products for the next two years, contingent on industry commitments to build and market future products that support key recovery;202

(3) requirement of key escrow capabilities after two years in all exportable products with more than 40 bits,203 and

(4) encouragement of the adoption of key escrow systems through international agreements, standards processes, and a new key management infrastructure.204

Although the Administration asserts that its latest policy generally conforms to the recommendations of the NRC, many commentators have disputed that assertion. The New York Times, for example, called it “a flawed encryption policy.”205 The Administration has emphasized that it will not mandate key recovery through legislation, although it announced its intention to introduce a bill in early 1997 establishing standards on the conduct of third-party key holders.206

Separately, in July 1996, the U.S. government granted Netscape Communications Corp. approval to distribute the highly secure RC4 128-bit version of its Netscape Navigator Internet client software and Netscape servers on-line to its U.S. customers.207 Users are required to submit information that determines their eligibility before they will be allowed to download the software.208 The 128-bit software is not exportable currently.209

Meanwhile, there has been vocal opposition in Congress to the Administration’s cryptography export policies. Senator Leahy (D-Vt.)

---

201. See Statement by Vice President Gore, supra note 200, at 831.
202. See id. at 832. Six-month licenses for 56-bit exports would be granted and renewed for up to two years, contingent on satisfactory progress towards key escrow. See id. at 831. Export of longer key lengths would continue for certain sensitive financial applications. See id.
203. See id. Export of longer key lengths may be allowed more generally once key escrow mechanisms are in place. See id.
204. See id.
206. See Statement by Vice President Gore, supra note 200, at 831.
208. See US Government OKs Netscape’s Online Encryption Distribution, NEWSBYTES, July 17, 1996, available in 1996 WL 10927966 (“[U]sers must submit information that determines their eligibility before they will be allowed to download the software.”).
introduced the Encrypted Communication Privacy Act of 1996\textsuperscript{210} in March.\textsuperscript{211} Congressman Goodlatte (R-Va.) introduced the SAFE\textsuperscript{212} bill soon thereafter.\textsuperscript{213} Senator Burns (R-Mont.) has introduced the Promotion of Commerce On-line in the Digital Era ("Pro-CODE") Act of 1996,\textsuperscript{214} which would deregulate substantially encryption that is available in foreign markets,\textsuperscript{215} and which was co-sponsored in the Senate by then-Senator Dole (R-Kan.) and enjoyed broad bi-partisan support.\textsuperscript{216} Senator Burns has held open hearings on his bill that have been transmitted over the Internet.\textsuperscript{217} He promised to re-introduce the bill when Congress reconvened in January 1997.\textsuperscript{218} It is expected that substantial policy debate will occur at that time.

In congressional hearings before the Subcommittee on Capital Markets, Securities and Government Sponsored Enterprises of the House Committee on Banking and Financial Services, credit card industry executives said that laws restricting the use of digital signatures and the export of encryption technology are making it difficult for U.S. financial institutions to offer new services.\textsuperscript{219}

The Justice Department dropped its case against Phil Zimmerman, inventor of the cryptography program Pretty Good Privacy ("PGP") without comment on January 11, 1996.\textsuperscript{220} The program had been

\begin{itemize}
  \item \textsuperscript{210} S. 1587, 104th Cong. (1996).
  \item \textsuperscript{211} See 142 CONG. REC. S1516 (daily ed. March 5, 1996) (statement of Sen. Leahy).
  \item \textsuperscript{213} See 142 CONG. REC. E276 (daily ed. March 5, 1996) (statement by Rep. Goodlatte).
  \item \textsuperscript{214} See id. S4619 (daily ed. May 2, 1996) (statement of Sen. Wellstone).
  \item \textsuperscript{215} See On-Line Security Issues: The Promotion of Commerce Online in the Digital Era Act of 1996: Testimony on S.1726 Before the Commerce Sub-Committee on Science, Technology and Space, available in 1996 WL 332977 (presented by Dr. Aharon Friedman, Founder, Chairman and Chief Technology Officer, Digital Secured Network Technology) (discussing how Act benefits American cryptology companies by relaxing export laws).
  \item \textsuperscript{217} For information on the bill, see Open Letter to the Internet from Senator Burns (last modified Feb. 27, 1997) \url{http://www.senate.gov/~bums/open97.htm} (on file with The American University Law Review).
  \item \textsuperscript{218} See Burns Introduces Internet-Friendly Bill (Feb. 27, 1997) \url{http://www.senate.gov/~burns/p-feb27.htm} (on file with The American University Law Review) (announcing re-introduction of Pro-CODE bill).
  \item \textsuperscript{219} See generally Online Banking: Hearings Before the Subcomm. on Capital Markets, Sec. & Gov't Sponsored Enters. of the House Comm. on Banking & Fin. Servs., 104th Cong. (1996) (testimony of Steve Mott, Senior Vice President, MasterCard Int'l) (advocating "liberalized perspective on exporting of encryption and related security technology" to promote use of electronic commerce worldwide), available in 1996 WL 392638.
  \item \textsuperscript{220} See Computer Software Writer Won't Be Prosecuted; Technology: U.S. Government Was Unhappy That Encryption Program Reached the Internet, L.A. TIMES, Jan. 12, 1996, at D2.
\end{itemize}
placed on the Internet in the spring of 1991.\textsuperscript{221} The Justice Department began its investigation in 1993.\textsuperscript{222} With little precedent, it was not clear whether placing the software on the Internet so that it could be copied by individuals outside the United States violated export laws.\textsuperscript{223} After the investigation was dropped, Mr. Zimmerman promised to continue working on technology that furthers privacy ends.\textsuperscript{224}

Civil liberties advocates have begun to go on the offensive. In \textit{Bernstein v. Department of State},\textsuperscript{225} mathematician Daniel Bernstein, with backing from the Electronic Frontier Foundation ("EFF"), sought to have the ITAR restrictions on export of encryption ruled unconstitutional on First Amendment grounds.\textsuperscript{226} At an April 15, 1996, hearing on the first phase of this litigation, the San Francisco federal district court ruled that source code is protected expression for First Amendment purposes.\textsuperscript{227}

On August 7, 1996, Professor Peter Junger of Case Western Reserve Law School in Cleveland filed suit in federal district court in Ohio, challenging government regulations that restrict his ability to teach a course in computer law.\textsuperscript{228} In \textit{Junger v. Christopher},\textsuperscript{229} he argued that ITAR's cryptographic licensing scheme effectively prevents him from admitting foreign students to the course and prohibits him from publishing his course materials and articles containing cryptographic software.\textsuperscript{230} Junger's challenge, like Bernstein's, is based on the

\begin{itemize}
  \item \textsuperscript{221} See id.
  \item \textsuperscript{222} See id.
  \item \textsuperscript{223} See id. Under the Bureau of Export Administration's December 30, 1996, Interim Rule, see 15 C.F.R. § 734.2(b), the definition of "export" was revised to include specifically making encryption software available for Internet download unless the individual making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States.
  \item \textsuperscript{225} Two reported district court opinions flow from this case. In \textit{Bernstein v. Department of State}, 922 F. Supp. 1426, 1439 (N.D. Cal. 1996) [hereinafter \textit{Bernstein I}], the court denied defendant's motion to dismiss and determined that plaintiff's claims were justiciable. In \textit{Bernstein v. Department of State}, 945 F. Supp. 1279, 1290 (N.D. Cal. 1996) [hereinafter \textit{Bernstein II}], the district court ruled on both parties motions for summary judgment. The court granted plaintiff's motion in part, holding that the ITAR leasing scheme constituted a prior restraint on speech in violation of the First Amendment. See id.
  \item \textsuperscript{226} See \textit{Bernstein II}, 945 F. Supp. at 1282.
  \item \textsuperscript{227} See \textit{Bernstein I}, 922 F. Supp. at 1436.
  \item \textsuperscript{228} A number of materials concerning the \textit{Junger} lawsuit, including press releases and pleadings, can be found on the Internet at \textit{Junger v. Christopher} (visited Jan. 28, 1997) <http://samsara.law.cwru.edu/comp_law/jvc> (on file with The American University Law Review).
  \item \textsuperscript{230} See id. ¶¶ 32-40.
\end{itemize}
unconstitutionality of requiring the permission of the government before one can communicate knowledge.\textsuperscript{231} Earlier decisions have held that such a prior restraint, except in the most unusual of circumstances, is a violation of the First Amendment.\textsuperscript{232} Oral argument in \textit{Junger} was scheduled for November 20, 1996.

International events also have affected U.S. policy in the encryption area. Nippon Telegraph \& Telephone Corporation's ("NTT") June 1996 announcement of its high-level encryption chip clearly affected the debate within U.S. policy circles.\textsuperscript{233} In addition, the Organization for Economic Cooperation and Development recently moved ahead in drafting cryptography policy guidelines that would provide internationally comparable criteria for encryption of computerized information.\textsuperscript{234} Completion of the guidelines is expected by early 1997.\textsuperscript{235}

Questions about the security of payment information were addressed internationally in 1996, with the release of the \textit{Security of Electronic Money} report, which concluded that existing security measures to protect electronic money products, when implemented correctly, can provide consumers and issuers adequate protection from fraud.\textsuperscript{236}

On September 26, 1996, scientists at Bell Communications Research ("BellCore"), unaware of the G-10 report, announced the discovery of a potential security flaw in smart cards that utilize public key technology.\textsuperscript{237} The Smart Card Forum and other industry groups responded immediately with assurances that their architecture

\textsuperscript{231} See id.
\textsuperscript{232} See Nebraska Press Assoc. v. Stuart, 427 U.S. 539, 559 (1976) (asserting that prior restraints "are the most serious and least tolerable infringement on first amendment rights"); New York Times Co. v. United States, 403 U.S. 713, 714 (1971) ("'Any system of prior restraints of expression comes to this court bearing a heavy presumption against its constitutional validity.'" (quoting Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963))).
\textsuperscript{233} See Michelle Slatalla, \textit{The Cutting Edge: Decoding the Controversy over Exports of Encryption Security: From Terrorism to Privacy, the Debate Touches Everyone}, L.A. TIMES, June 10, 1996, at D1 (reporting on sale of "triple-DES" encryption chip by Japanese "corporate behemoth" NTT).
\textsuperscript{236} See COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS AND THE GROUP OF COMPUTER EXPERTS, CENTRAL BANKS OF THE GROUP OF TEN COUNTRIES, BANK FOR INTERNATIONAL SETTLEMENTS, SECURITY OF ELECTRONIC MONEY (1996).
includes multiple levels of security, and that roll-out plans for smart cards will not be delayed.\textsuperscript{238}

\textbf{C. Intellectual Property Developments}

\textbf{1. Copyright}

Does cyberspace require a new copyright law? In intellectual property circles, this is the question most in need of resolution; the answer has been elusive so far.

Under current copyright law, copyright owners retain a number of on-line rights with respect to a work. These include: reproduction, adaptation, distribution, public performance, and public display.\textsuperscript{239} These rights may be limited or interpreted in the on-line environment to provide certain rights to users. Users may have implied licenses or an on-line fair use right, the copying may be "de minimus," or the work may be considered non-copyrightable or in the public domain.\textsuperscript{240}

Banks increasingly are creators as well as users of software. A better understanding of permissible on-line uses of, and protections for, software is critical to the development of electronic commerce. Further questions arise with respect to on-line information. The courts have not clarified these issues sufficiently.

In one recent case, \textit{Lotus Development Corp. v. Borland International, Inc.},\textsuperscript{241} the First Circuit ruled in Borland's favor, holding that the Lotus menu command hierarchy structure was not an uncopyrightable method of operation.\textsuperscript{242} This holding, however, conflicts with decisions in other circuits.\textsuperscript{243} The Supreme Court affirmed the

\textsuperscript{238} \textit{Cf.} David Bank, \textit{Smart Cards Are Open to New Attack by Hackers, Say Israeli Researchers}, WALL ST. J., Oct. 21, 1996, at B14 (discussing recent criticism of so-called smart cards and noting response by Smart Card Forum that smart cards are still far more secure than magnetic strip credit cards).


\textsuperscript{241} 49 F.3d 807 (1st Cir. 1995), \textit{aff'd by an equally divided court}, 116 S. Ct. 804 (1996) (per curiam).


\textsuperscript{243} \textit{See id.} at 819 & n.14 (acknowledging disagreement with courts in Tenth and Ninth Circuits); Autoskill Inc. v. National Educ. Support Sys., 994 F.2d 1476, 1495 n.2 (10th Cir. 1993) (rejecting defendant's argument that computer program's keying procedure was uncopyrightable method of operation); Brown Bag Software v. Symantec Corp., 960 F.2d 1465, 1477 (9th Cir. 1992) (indicating that menus and keystrokes may be copyrightable).
Lotus decision in early 1996, but did so in a way that did not resolve the uncertainty among the courts.  

The release of the final report of the Clinton Administration's Working Group on Intellectual Property and the National Information Infrastructure ("White Paper") in September 1995 also disappointed many in the on-line service provider community. The White Paper provided Congress with the Administration's official recommendations for tailoring federal intellectual property law to fit the growing digital marketplace. It concluded that existing copyright law was adequate, with a few minor adjustments.

The National Information Infrastructure Copyright Protection Act—intended to follow the White Paper's recommendations to adapt existing copyright law to the Internet—was introduced but was not passed by Congress in 1996. Debate is expected to continue over whether the unique issues that arise when information is transmitted over computer networks require a new approach to copyright protection.

In the interim, copyright owners are taking aggressive action on their own. In October 1996 the Software Publishers Association ("SPA"), a trade association of software publishers, announced that it has filed five lawsuits for copyright infringement on the Internet. The suits were filed against Internet service providers and individuals, alleging both direct and contributory copyright infringement. The SPA also maintains a hotline where people can report suspected acts of piracy.

2. Trademarks

Network Solutions, Inc., ("NSI") a private company that assigns Internet domain names under a contract with the National Science

245. See REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY, NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 114-24 (1995) (asserting that online service providers should be held strictly liable for user copyright infringement).
246. See id.
247. See id.
250. See SPA Files Copyright Suits Against ISPs, Individual End Users, SOFTWARE INDUS. REP., Oct. 21, 1996, at 7.
251. See id.
252. See id.
Foundation, has been under increasing attack in 1996 for its policies.\textsuperscript{253} NSI now has approximately 660,000 "\.com" names registered in its InterNIC data base, representing 89\% of NSI registrations.\textsuperscript{254} Claims that NSI's domain name policies are not neutral, but rather favor trademark owners over domain name owners are ongoing.\textsuperscript{255} As a result, some critics have argued that overzealous trademark owners are forcing legitimate users to give up their domain names, even in cases where the trademark owner's rights are not infringed by the domain name.\textsuperscript{256} Domain name owners have brought eighteen lawsuits against NSI and trademark claimants.\textsuperscript{257}

Concern over the rush for, and misuse of, domain names prompted at least one state to act. The California Senate introduced a bill in 1995\textsuperscript{258} that would expose an unauthorized user of another's trademark as a domain name or e-mail address to penalties under unfair competition laws.\textsuperscript{259} Some experts considered the bill alarmingly overbroad.\textsuperscript{260}

3. \textit{Patents}

Patent protection of encryption and electronic payment protocols has created a dangerous minefield. Many of the early patents are broad, and the degree of their enforceability is unclear. Some are not widely known by developers, and the community has found itself blindsided more than once by patent holder demands for royalty payments. Claims by companies such as Refac, Interactive Gift Express, and E-Data ultimately may have a substantial effect on the emerging field of on-line commerce.\textsuperscript{261}

\textsuperscript{253} See David J. Loundy, \textit{Internet Name Game Gets New Set of Rules}, CHI. DAILY L. BULL., Sept. 12, 1996, at 5 (discussing complaints about NSI policies and monopoly over "corporate namespace").

\textsuperscript{254} See generally Internet International Ad Hoc Committee, \textit{Domain Name Surveys and Statistics} (last modified Dec. 11, 1996) \url{http://www.iahc.org/dns.refs/dns-stat.html} (on file with The American University Law Review); see also Record Year for Internet Name Registration, NEWS-BYTES NEWS NETWORK, Jan. 9, 1997, available in 1997 WL 7969973 (reporting that total number of second level domains increased 452\% during 1996).

\textsuperscript{255} See Loundy, supra note 253, at 5.


\textsuperscript{257} See Gabe Battista, \textit{Our Approach Is Balanced}, USA TODAY, Jan. 15, 1997, at 10A.


\textsuperscript{259} See id. § 1.

\textsuperscript{260} See Ilana DeBare, \textit{State Trademark Bill Ignites Net Turmoil}, SACRAMENTO BEE, Mar. 22, 1996, at F1 ("[O]n-line activists are aghast at the broad scope of the bill, which would apply to the part of e-mail addresses that identifies individuals as well as the part that identifies organizations.").

Patents that are recognized widely as enforceable create their own problems. Payment systems, for example, optimally should be low cost and not subject to transaction level royalty payments. DigiCash, Mondex, and Citibank, among others, have obtained important, recognized patents in the electronic payment area. Furthermore, many of the underlying encryption schemes are patented. One of the earliest, the Diffie-Hellman key exchange patent, which was developed by RSA, is nearing the end of its protection and will expire in September 1997. This will put the Diffie-Hellman algorithm in the public domain. Another notable patent, Merkle Hellman, also will be expiring within the next few years. The U.S. government holds the patent on the Digital Signature Algorithm (“DSA”) and makes it available from the NIST royalty-free to users worldwide.

4. **Trade secrets**

On October 11, 1996, President Clinton signed the Economic Espionage Act of 1996. The Act strengthens protections against theft or misuse of proprietary business information. It makes the theft of trade secrets a federal crime and provides financial penalties and prison sentences for specific acts of economic espionage. The Act also eliminates gaps in the criminal laws that address attacks against computers and the information they contain.

5. **Web site links**

A much-criticized new Georgia law, known as the Georgia Computer Systems Protection Act, makes it illegal for organizations to use

---


266. See id. § 101(a), 1996 U.S.C.C.A.N. (110 Stat.) at 3489 (to be codified at 18 U.S.C. § 1832(a)) (authorizing fines of up to $500,000 and prison sentences of up to 15 years for persons convicted of economic espionage).


trademarks and logos on the Internet without permission.\textsuperscript{269} The law also prohibits sending e-mail anonymously in some circumstances,\textsuperscript{270} as well as fraudulently representing one's Website as that of another organization.\textsuperscript{271} The Georgia law imposes a penalty of as many as twelve months in prison and $1000 in fines.\textsuperscript{272} The law became effective July 1, 1996. On September 24, 1996, the American Civil Liberties Union ("ACLU") filed suit in federal district court in Georgia, challenging the law on the ground that it illegally imposes state restrictions on interstate commerce, an area properly left to the control of Congress.\textsuperscript{273} The challenge is considered one of the first major assaults on state laws that seek to rein in the Internet.\textsuperscript{274}

\section*{D. Privacy and Publicity}

\subsection*{1. Banking Privacy}

Courts have held that there is no expectation of privacy in bank accounts, and that bank accounts therefore are not subject to constitutional protections against warrantless searches.\textsuperscript{275} It is likely that this reasoning also will apply to many types of customer-related banking information transmitted over the Internet.

Nevertheless, banking information is protected under various privacy laws. The Right to Financial Privacy Act\textsuperscript{276} prohibits the government from obtaining certain types of banking information without due process of law.\textsuperscript{277} The EFTA\textsuperscript{278} and Reg E\textsuperscript{279} contain minimal restrictions on use or disclosure of customer information.\textsuperscript{280}

\begin{thebibliography}{99}
\bibitem{269} See id. § 1. A rival state lawmaker who is a vocal critic of the law says that the law was a political reprisal for a Web site that he set up privately that displayed the state seal on its opening page and provided voting records and some harsh political commentary. See Jared Sandberg, \textit{Suit Challenges State's Restraint of the Internet}, \textit{WALL ST. J.}, Sept. 25, 1996, at B1.
\bibitem{271} See id.
\bibitem{273} See Sandberg, \textit{supra} note 269, at B1.
\bibitem{274} See id.
\bibitem{277} See id. § 3402.
2. Database protection

In 1991, the U.S. Supreme Court held that telephone databases, as well as other databases that can be compiled without creative effort, are not protected under U.S. copyright law.281

The World Intellectual Property Organization has backed a United Nations proposal that, contrary to the Supreme Court’s position, would define all organized information as a “database” and grant it protection against commercial infringement.282 Congress similarly has considered the Database Investment and Intellectual Property Antipiracy Act of 1996.283 Introduced by Representative Moorhead (D-Pa.) in the House on May 23, 1996,284 the Act would have established a new form of intellectual property protection for databases, sometimes called “sweat of the brow” works.285 Unlike patent or copyright protection, which are creatures of the Constitution,286 database protection would be created by legislation. In this respect it would be similar to trademark protection.287 There is not yet sufficient support for this form of intellectual property, and it is seen by some as a windfall to benefit large commercial database interests. Nevertheless, the proposed legislation has the strong support of Bruce Lehman, the Commissioner of Patents and Trademarks, as well as database developers.288

Meanwhile, on March 11, 1996, the European Union (“EU”) passed a similar directive on the legal protection of databases.289

—

285. “Under [the] sweat of the brow [standard], a person who exercises sufficient 'skill, judgment and labour' in compiling pre-existing works may acquire copyright in the result and the one who puts forth the skill, judgment and labour in assembling the collection is the author of the compilation.” Fogt & Smith, supra note 282, at 35. Under the Database Investment and Intellectual Property Antipiracy Act, H.R. 3531, 104th Cong. (1996), a similar standard would apply. Specific exemptions exist “for use of insubstantial portions of databases for any purpose. The bill specifically allows innovators to create their own databases independently, as a result of their own work and investment, as opposed to ‘free-riding’ on the work and investment of others.” 42 CONG. REC. E891 (daily ed. May 23, 1996) (statement of Rep. Moorhead).
286. See U.S. CONST. art. III.
288. See Carol Levin & Don Willmott, Is It Mine Online? International Panel Irons out Internet Policy, PC MAC., Feb. 4, 1997, at 30; see also Seth Schiesel, Global Agreement Reached to Widen Copyright Law, N.Y. TIMES, Dec. 21, 1996, at A1 (noting that agreement was reached on two treaties on literary and artistic works and on rights of performers and producers of music, but contentious database protection proposal was abandoned because of objections from other countries); Treaties to Protect Rights on Internet, DAYTON DAILY NEWS, Dec. 22, 1996, at 8B.
Country members of the EU are expected to adopt laws that abide by this directive within three years.

In early 1996, Minnesota worked toward becoming the first state to protect consumer privacy on-line. The Online Privacy Option Bill would regulate the use and dissemination of "personally identifiable information on consumers of computer information services."

3. Consumer database privacy

In September 1996, word quickly spread through the Internet that the on-line database company LEXIS-NEXIS was selling personal consumer information, including Social Security numbers, telephone numbers, and addresses. LEXIS-NEXIS, a respected provider of law and news databases, was caught off guard by the unprecedented groundswell of reaction. It tried to respond on-line to some of the exaggerated rumors, and it permitted individuals to request the removal of their names from the database, called P-TRAK. LEXIS-NEXIS argued that other companies also sold the information in question and that it was available publicly, as unregulated "header" information, from one of the three major private sector U.S. credit reporting agencies.

The Federal Trade Commission ("FTC"), on September 20, 1996, recommended that credit reporting agencies no longer should be able to supply this information to database operators such as LEXIS-
NEXIS.\textsuperscript{296} It said that "the ready availability of this information through a tracking service may facilitate identity fraud, credit fraud and other illegal activities," and recommended broader privacy protections.\textsuperscript{297} Specifically, the FTC recommended that the Fair Credit Reporting Act\textsuperscript{298} be amended to provide confidentiality for a person's maiden name, Social Security number, prior addresses, and date of birth, in order to make this information available only to those with legal authority to obtain it.\textsuperscript{299}

In addition, in an October 8, 1996, letter to the FTC, Senators Bryan (D-Nev.), Hollings (D-S.C.), and Pressler (R-S.D.) asked regulators to probe whether companies that run such computer databases violate consumers' right to privacy.\textsuperscript{300} The senators asked the FTC to provide a report within six months and to include recommendations for any new laws.\textsuperscript{301} It is notable that the top story in the October 11, 1996, issue of American Banker, addressed the FTC's advice, taking the position that the agency's actions were "threatening to ensnare banks and other information-intensive businesses in a tighter regulatory web."\textsuperscript{302}

4. Employee e-mail monitoring

Financial institutions must consider the developing issues surrounding the use of e-mail by their employees and consultants. First, an employer may be bound by an e-mail promise made by an employee, especially when the employee signs e-mail messages as an officer of the employer. Second, e-mail messages, written with no thought as to their permanence, nevertheless may be recoverable by an opponent and used as evidence in court.

The Electronic Communications Privacy Act\textsuperscript{303} prohibits a third party from intercepting or disclosing electronic communications.\textsuperscript{304} It also prohibits unlawful access to, and disclosure of, stored electron-
ic communications, including both voice and e-mail. Exceptions are available when there has been "prior consent" or when the access and disclosure is for "business use." Most states additionally have adopted wiretapping statutes that address unauthorized access to, and interception of, electronic communications. Laws and court interpretations vary widely among the states.

In the case of Smyth v. Pillsbury Co., a federal court held for the first time that an employer, under Pennsylvania law, has the right to monitor an employee's e-mail, because an employee has no reasonable expectation of privacy in his e-mail communication.

In light of the concerns outlined above, most legal experts advise employers to develop clear policies regarding employee uses of, and privacy in, e-mail.

Considering the recent social and legal trends within the United States in the area of personal privacy, it is expected that other privacy issues will develop more fully during the next few years.

E. Telecommunications Act of 1996

Passage of the Telecommunications Act of 1996 in February signaled the most complete restructuring of the U.S. telecommunications industry since the establishment of the Federal Communications Commission ("FCC") in 1934. The Act removes barriers to competition among communications companies and loosens other restrictions. The fundamental assumption is that telephones no longer are a natural monopoly, and that competition now is important. The government's role is to foster that competition.

The Act contains seven titles. The first five cover: telecommunication services, with an emphasis on the development of competitive markets; broadcast services; cable services; regulatory re-

---

305. See id. § 2510(17).
306. See id. § 2511(2)(d).
307. See id. § 2511(2)(a).
The Act directs the FCC to write more than eighty implementation rules in these areas.\footnote{318}

The most significant effect of the Act on financial institutions may be the potential for lower prices, as well as a wide variety of new service offerings and technologies. Financial institutions increasingly will be able to consider telecommunications, broadcast, and cable as potential distribution channels for financial services.

A more market-driven telecommunications environment generally is considered most beneficial to large corporate users such as banks. At greater risk are high-cost, low-profit users, typically consumers and small businesses in remote areas. This is because service providers in a market-driven environment tend to eliminate subsidies to high-cost users, in order to compete more effectively in other markets and to keep profitable users from bypassing the system. The Act seeks to address the bypass problem. It requires the FCC to institute a Federal-State Joint Board to study policies for the preservation and advancement of universal telecommunications and information services, and to make its recommendations to the FCC in 1997.\footnote{319}

The Joint Board will be required to base its policies on the following principles: (1) that quality service should be affordable at just, reasonable, and affordable rates;\footnote{320} (2) that access to advanced telecommunications and information services should be provided in all regions of the nation;\footnote{321} (3) that access in rural and high-cost areas should be reasonably comparable to those services provided in urban areas at reasonably comparable rates;\footnote{322} (4) that all providers of telecommunications services should make an equitable and nondiscriminatory contribution to the preservation and advancement of universal service;\footnote{323} (5) that specific and predictable federal and state support mechanisms should be established to preserve and advance universal service;\footnote{324} and (6) that access to advanced telecommunications services should be provided for schools, health care facilities, and libraries.\footnote{325}

Of particular interest to the Internet community are the provisions of Title V, known as the Communications Decency Act of 1996.
It criminalizes the sending of "obscene, lewd, lascivious, filthy, or indecent" communications through the Internet. Immediately after passage of the Act, the ACLU and others sought a court injunction to declare the CDA unconstitutional, because it restricted the right to free speech in an overbroad and vague way. A three-judge panel in a Philadelphia federal district court held a well-publicized trial on the issue. On June 11, 1996, the court issued a preliminary injunction to prevent enforcement of the CDA, unanimously declaring the indecency provisions of the Act unconstitutional. After the decision in Philadelphia, a court in New York also declared the indecency sections unconstitutional in a similar case. The government has appealed both decisions directly to the U.S. Supreme Court, in accordance with procedures specified in the Act. The Supreme Court has agreed to hear the appeal, and the case will be argued in March 1997, with a decision expected by July.

At the same time, eleven state legislatures have passed their own Internet statutes, and nine others have considered taking action. In 1995, Connecticut passed a law that makes it a crime to send an e-mail message "with intent to harass, annoy or alarm another person." Virginia passed a bill in 1996 making it illegal for a state employee to use state-owned computers to access sexually explicit material. New York's governor has signed into law a bill to reinstitute prohibitions on disseminating indecent material to a minor, similar to those that were struck down at the federal level in Shea v. Reno. The New York law is effective November 1,
1996. The New York Civil Liberties Union says it will continue to fight the law and will seek its repeal.

Title V also includes protections for Internet service providers. In 1995 a New York court ruled, in *Stratton Oakmont, Inc. v. Prodigy Services Co.*, that an Internet service provider could be held liable for defamatory messages posted by users of its on-line service. The court held Prodigy to the same standards of liability for defamation as any other publisher of news or information, based on the fact that Prodigy had a policy of screening bulletin board postings for offensive language. The court maintained that because Prodigy exercised editorial control over posted messages, it was a publisher rather than a mere distributor.

The lawsuit itself eventually was dropped when Prodigy issued an apology to Stratton Oakmont; however, the court ruling drew serious concern over potential liability from other Internet service providers, from users who worried about censorship, and from legislators who did not want service providers to stop screening messages for offensive language as a result of the ruling. As a result, Title V of the Telecommunications Act includes a provision that protects access providers who do not advertise, conspire in, or contribute to the creation of a defamatory, obscene, or harassing message.

In the miscellaneous provisions of Title VII, the Telecommunications Act also requires telecommunications carriers to protect the

---

343. See Stratton Oakmont, 23 Media L. Rep. (BNA) at 1798 (stating that Prodigy's "conscious choice" to monitor content of its bulletin board imposes greater liability on it and that mere distributor would not be liable for these types of messages).
confidentiality of proprietary information relating to other telecommunications carriers, equipment manufacturers, and customers.  

F. Taxation and the Internet

There is substantial uncertainty over whether and how to apply conventional tax concepts to the Internet. It is clear, however, that state and local governments are coming to see on-line computer networks as a rich, new revenue source. Observers assume that Internet taxes are inevitable.

In 1994, a state court in Texas determined that a state sales tax scheme that taxes information services, but exempts newspapers, does not violate the free speech or equal protection clauses of the U.S. or Texas Constitutions. As a result, cities in Texas and Colorado reportedly are considering special on-line taxes.

A Tennessee law demands that on-line services doing business in the state turn over their tax records and a listing of the total number of customers they have in the state. A recent effort to impose a six percent sales tax on Internet users in Tacoma, Washington, was withdrawn only after public outrage forced city officials to abandon the effort.

After a review of existing state laws, Netcom On-Line Communication Services, Inc., a leading Internet service provider, notified its Massachusetts customers in August 1996, that the company would start adding the Commonwealth's five percent sales tax to its bills. It similarly notified customers in Pennsylvania, Illinois, and a number of other states. The General Counsel of the Massachusetts Department of Revenue announced in September 1996 that all on-line service providers that do business in the Commonwealth should be

348. See Reuters Am., Inc. v. Sharp, 899 S.W.2d 646, 657 (Tex. App. 1994) (holding that tax scheme was related to legitimate state interest).
352. See Hiawatha Bray, Governments Look to Internet as Rich, New Source of Tax Revenue, B. GLOBE, Sept. 15, 1996, at E1 (reporting NetCom's decision and concluding that tax would amount to $1.00 on a $19.95 monthly account).
353. See id.
paying the telecommunications sales tax. Those who have not been paying, he said, could face audits, penalties, and demands for back taxes from up to seven years ago. Some service providers have argued that this would be unfair. There also is substantial concern that chaos could result if the fifty state governments and thousands of cities and counties each make their own rules about taxing computer networks and the transactions that occur on them.

In a related development, in October 1996, the European Commission introduced a new interpretation of article 27 of the value-added tax ("VAT") legislation. It is planning to implement a change in the application of the VAT from the seat (headquarters) of an organization to the point of its consumption. This means that European subscribers to CompuServe, AOL, and other U.S.-based Internet and telecommunications providers, who have not been charged VAT because their service is headquartered in the United States, will begin paying VAT early in 1997. This will strengthen further U.S. state government efforts to apply sales taxes to Internet services domestically.

With regard to federal taxation, the Internal Revenue Service ("IRS") announced on September 11, 1996, that it had cancelled its implementation of "Cyberfile," a system designed to allow PC users to file their federal tax returns electronically over the Internet. The IRS said that it was "still committed to the concept of home filing," and in January announced that electronic and on-line income tax filing would be available to citizens through third-party contractors.

354. See id. (quoting General Counsel as saying that "ability to telecommunicate through the Internet" is taxable); Mass. Regs. Code tit. 830, § 64H.1.6 (1996) (imposing tax on telecommunications services).


357. See U.S. Gives Wide Berth to Taxes on Internet, Chi. Trib., Nov. 22, 1996, at 23 (discussing rejection of imposing federal taxes on Internet and urging states to follow federal example); Weber, supra note 949, at B10 (providing overview of difficulties that accompany local and state taxation of Internet services); Elizabeth Weise, Internet Firms Are Faced with Collecting Taxes, Cincinnati Post, Apr. 12, 1996, at 6B (reporting that Internet service providers worry about online taxes in nomenclature of "50 states and myriad counties").


G. Securities Industry On-line

The use of on-line media for underwriting and delivery in the securities industry has increased rapidly in recent months. Early in 1996, the Securities and Exchange Commission ("SEC") permitted the Spring Street Brewery Company of New York to make an initial public offering over the Internet.\textsuperscript{360} The SEC asked, and the company agreed, to suspend trading temporarily, pending review of legal implications of such a trading system and minor procedural changes.\textsuperscript{561} Spring Street subsequently said it planned to establish an on-line stock exchange.\textsuperscript{362}

In late June 1996, a California company that sells energy-saving solar panels received SEC approval to trade its stock over the Internet.\textsuperscript{363} Approval was granted to the company, Real Goods Trading Corporation, through a "no-action" letter.\textsuperscript{364}

The SEC has indicated further, through a series of releases, that it is comfortable with expanding permissible securities activities to the Internet.\textsuperscript{365} It is expected that other activities soon will be approved, and that financial institutions will want to make use of them.

H. Government Benefits

The Debt Collection Improvement Act of 1996\textsuperscript{366} requires federal agencies to convert from checks to EFTs in two phases.\textsuperscript{367} The

\textsuperscript{360.} See Spring Street Brewing Co., SEC No-Action Letter, [Current Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 77,201 at 77,001 (Apr. 17, 1996) (describing Spring Street's wishes to trade over Internet as "an innovative mechanism").


\textsuperscript{362.} Spring Street's online trading bulletin board, entitled "Wit-Trade," allows users to trade Spring Street stock over the Internet. See \textit{id.} at 42,148; see also Wit Capital Corp. (visited Mar. 12, 1997) <http://www.witcap.com/caphub.htm> (on file with \textit{The American University Law Review}).


\textsuperscript{364.} See \textit{id.} A no action letter permits the requesting company to perform a requested activity, without fear of any enforcement action against it. See 17 C.F.R. § 200.81 (1996).


Financial Management Service of the U.S. Treasury has implemented these requirements. Under the Act, all Federal payments made after January 1, 1999, except payments under the Internal Revenue Code and other exempted payments, must be made by EFT.

The Department of the Treasury Bureau of the Public Debt has finalized new rules to govern its book-entry treasury bonds, notes, and bills with the release of its Treasury/Reserve Automated Debt Entry System ("TRADES") regulations. These regulations "incorporate recent and significant changes in commercial law addressing the holdings of securities in book-entry form through financial intermediaries."

A question remains as to how electronic benefits transfer ("EBT") payments that utilize SVCs will be governed under the Federal Reserve's Reg E.

The Senate Committee on Banking, Housing, and Urban Affairs held hearings in July 1996, with a goal of eliminating the bank practice of surcharging for use of their ATM machines. Congress did not pass the so-called Fair ATM Fees for Consumers Act, however, and surcharging has become increasingly common. The government is particularly sensitive about surcharging recipients of electronic fund transfers for all federal payments as phase two).


371. Id. at 43,626. The Treasury was concerned about maintaining "uniformity of treatment of holders of interests in Treasury securities." Id. These changes are contained in the new U.C.C. article 8. See U.C.C. art. 8 (1996).

372. See 62 Fed. Reg. 3242, 3242-44 (1997) (to be codified at 12 C.F.R. pt. 205) (proposed Jan 22, 1997). As mandated by Congress under its welfare reform law, the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, the FRB has proposed to exempt from Reg E needs-tested EBT programs established or administered by state or local government agencies. Federal programs and employment-related programs would continue to be subject to the modified Reg E requirements that the FRB adopted in 1994 (effective March 1, 1997). The main effect of this change is to enable states to reduce or eliminate their liability under the Food Stamps, Aid to Families with Dependent Children, and similar needs-based programs for unauthorized transfers resulting from lost or stolen access devices. This has been a major concern of State EBT authorities since Reg E was expanded in 1994 to include their programs. In its 1994 amendments, the FRB for the first time determined that it had the authority to expand the definition of "consumer account" to include accounts of governmental bodies earmarked for consumers. This may have implications in determining the definition of an account for SVC purposes.


government benefits payments, suggesting that further efforts to prohibit this activity may be initiated in the upcoming year.

The U.S. Court of Appeals for the District of Columbia Circuit ruled on August 13, 1996, that the Treasury Department must permit non-banks to bid for electronic benefits transfer contracts.\(^{375}\) It held that the Treasury Department illegally required that banks be the primary contractors for delivering welfare payments and food stamps through electronic terminals.\(^{376}\)

I. Advertising and Deceptive Practices

Banks and other financial service providers are approaching advertising on the Internet with caution. Under Internet tradition, unsolicited e-mail and newsgroup commercial advertising is frowned on.\(^{377}\) Banks instead have focused on advertising through their own Web sites or have paid to advertise on popular third party sites.\(^{378}\) While engaging in such practices, however, banks must remain aware that existing bank advertising rules apply to this medium.\(^{379}\) There is an increased focus on prosecuting deceptive practices over the Internet at both the state attorney general and federal levels.\(^{380}\) In addition, new concerns regarding Web links and related practices are developing.\(^{381}\)

The Internet currently is engaged in a war against "spammers," distributors of unsolicited e-mail advertisements who typically flood hundreds of thousands of Internet mailboxes with junk mail.\(^{382}\) Lists of e-mail addresses regularly are gathered from various sources, such as postings to public newsgroups, and sold.\(^{383}\) Early spammers, including a husband and wife law firm in Arizona, were threatened

---

376. See id. at 236-37 (finding that Treasury Department acted arbitrarily in making its decision).
377. See Kim Girard & Mitch Wagner, You Can't Send Mail There from Here; Anti-Spam Efforts Hinder E-Mail Delivery, COMPUTERWORLD, Dec. 16, 1996, at 3A (pointing out that efforts to reduce mass junk e-mail are mostly unsuccessful); David Hoye, Spamming the Globe, ARIZ. REPUBLIC, Dec. 50, 1996, at E1 (expressing frustration at plethora of junk e-mail and commercial advertising on Internet).
380. See Audra D.S. Burch, Internet Shopping a New Frontier for Fraud, MIAMI HERALD, July 6, 1996, at C1 (discussing "huge potential" for prosecuting deceptive business practices that occur on the Internet).
381. See supra Part II.C.5 (surveying state legislative response to such concerns).
383. See id. (discussing various ways in which spammers obtain e-mail address lists).
and vilified by other users, yet increased their spamming activities. Current spammers, such as Sanford Wallace of Philadelphia and his company, Cyber Promotions, Inc., aggressively have sought to protect their activities in court. Internet service providers CompuServe and America Online ("AOL") took early, unilateral action to control spamming. A lawsuit between Cyber Promotions and AOL was scheduled to go to trial in November 1996, but the court granted partial summary judgment to AOL.

One network service provider, Concentric Network Corp., recently obtained a degree of relief from spammers that other service providers hope to receive as well. Concentric claimed that a large volume of junk messages from Cyber Promotions had been altered to appear to have originated from Concentric's network. As a result, undeliverable return messages were flooding Concentric's system, preventing adequate service to its real customers. On October 7, 1996, Concentric obtained a federal court order in California requiring Cyber Promotions to submit an affidavit to the court swearing under oath that they would not engage in such conduct in the future.

Certainly, spamming is not widely appreciated. Nevertheless, in the United States there is substantial hesitation to regulate it in light of the Constitution's guarantee of freedom of speech. Despite this desire to safeguard the First Amendment, however, Judge Charles Weiner of the U.S. District Court for the Eastern District of Pennsylvania, recently held that Cyber Promotions did not have a First Amendment right to send unlimited e-mail.

The FTC is the federal agency charged with regulating advertising and unfair competition. The agency is "actively monitoring the Net

386. See Cyber Promotions 24 Media L. Rep. (BNA) at 2514 (holding that Cyber Promotions does not have First Amendment right to send unsolicited e-mail).
387. See Patrick McKenna, Cyber Promotions, NEWSBYTES, Oct. 10, 1996, available in LEXIS, News Library, Curnws file (quoting Concentric spokesperson that Cyber Promotions "forced the orientation point" of e-mail).
388. See id. (stating that service was interrupted for as long as 12 hours).
389. See id.
By early 1996, the FTC already had charged nine businesses and their principals with making false or unsubstantiated claims while marketing their products or services on the Internet. In addition, the Department of Transportation in late 1995 levied a first-of-its-kind fine of $14,000 against Virgin Atlantic Airways when it failed to update airfares listed on the Virgin Web page.

Banking regulators also traditionally have reviewed bank advertisements with scrutiny. A number of banking regulations, such as Truth in Lending ("Regulation Z") and Truth in Savings ("Regulation DD") contain detailed interest rate disclosure requirements. Financial institutions must understand that posting on the Web clearly is advertising that is subject to the rules and regulations that apply to all advertising. In addition, they must be mindful of potential liabilities unique to the Web. These include the potential for appearing to endorse a third-party product or service merely by providing a link to it, as well as the risk of a copyright or trademark violation in providing a third-party Graphical Image File ("GIF") or Uniform Resource Locator ("URL") on one's Web page. The laws of other states also must be considered.

Many states have statutes prohibiting the use of an individual's likeness or name for commercial purposes without the person's written consent. Failure to obtain written consent (even of one's

---


395. Id. pt. 230.

396. *See id. §§ 226.6, .8, .18-20, .31-33, 230.3-6.*

397. *See supra notes 268-74 and accompanying text (discussing Georgia statute); infra Part IIJ (addressing jurisdictional issues raised by virtual presence within state).

398. *See CAL. CIV. CODE §§ 990, 3344 (West Supp. 1997) (providing remedies for unauthorized use of living or deceased person's name, likeness, photograph, signature, or voice); FLA. STAT. ANN. ch. 506.13 (Harrison 1994) (prohibiting unauthorized use of name or seal of any person); N.Y. CIV. RIGHTS LAW § 50 (Mckinney 1992) (criminalizing use of living person's name, portrait, or picture for trade or advertising purposes).
In an interesting recent development, a Virginia resident named Ram Avrahami is suing *U.S. News and World Report* because, he alleges, the magazine sold mailing lists containing his name and address without his permission.\(^{400}\) He has asked the Virginia Supreme Court to rule on his assertion that the sale of his name (a widespread commercial practice) represents misappropriation of one's property for commercial purposes.\(^{401}\)

**J. Jurisdiction and Interstate Banking**

With the erosion of the McFadden Act's restrictions on interstate branching,\(^{402}\) the concept of virtual banking over the Internet becomes less problematic. Although banks still must be concerned with registration in those states in which they are performing a banking business, virtual banking raises a number of other jurisdictional questions, such as: (1) is virtual presence in a state enough to subject the bank to that state's income taxation requirements (including unified taxation states); and (2) is virtual presence sufficient to subject the bank to the jurisdiction of the courts of that state.

These types of jurisdictional questions are arising rapidly in many commercial and noncommercial cases. By way of example, a California couple, Robert and Carleen Thomas, were convicted in 1994 in Tennessee of posting illegal, sexually explicit files on their web site in California.\(^{403}\) A U.S. postal inspector working from Tennessee downloaded and ordered by mail a number of the pornographic files.\(^{404}\) The Thomas' actions were held illegal in Tennessee, but because the laws governing obscenity in the United States are based on a local moral standards test,\(^{405}\) it is possible that

---

399. See *FLA. STAT. ANN.* ch. 506.13; *GA. CODE ANN.* § 10-1-453 (1994); *N.Y. CIV. RIGHTS LAW* § 50.

400. See Steve Twomey, *A Brave Heart Fights Fiercely for Our Names*, *WASH. POST*, Sept. 30, 1996, at B1 (recounting how Avrahami intentionally misspelled his name in subscription application to *U.S. News and World Report* in order to trace from whom his name and address were sold).

401. See *id*.


404. See *id.* at 705 (recounting how postal inspector, after receiving complaint from Tennessee resident, applied for membership in Thomas' bulletin board system and indicated Tennessee phone number as his own).

405. See *id.* at 710-11 (rejecting Thomas' argument that California community standards of obscenity should apply); see also Miller v. California, 413 U.S. 15, 24 (1973) (holding one
a California court may have reached the opposite conclusion. Despite widespread criticism of the "forum-shopping" tactics used in this prosecution, on October 7, 1996, the U.S. Supreme Court refused, without comment, to hear an appeal of the conviction. Similar cases are being heard in other states, with widely varying results. In Maritz, Inc. v. CyberGold, Inc., the court ruled that it had personal jurisdiction over the defendant, whose only contact with the State of Missouri was the accessibility of its Web page to Missouri residents. On the other hand, in McDonough v. Fallon McElligott, Inc. and in Bensusan Restaurant Corp. v. King, intellectual property actions were dismissed under similar circumstances for lack of personal jurisdiction.

K. Criminal Conduct On-line

Many new federal, state, and local criminal provisions tailored to computers and on-line transactions have developed especially quickly, many of which can be placed in the following categories: (1) unauthorized access or use; (2) alteration or destruction of data; (3) theft of services; (4) computer fraud and abuse; (5) denial of access; and (6) unauthorized possession of passwords.

Banks traditionally have been faced with specific federal and state criminal reporting requirements. Developments in 1996 include the institution of a simplified criminal reporting procedure under the Bank Secrecy Act. The White House issued an Executive Order on July 15, 1996, establishing a high-level President's Commission on Critical Infrastruct-
toward Protection. The critical infrastructures to be assessed include banking and finance. The Commission’s tasks include recommending a “comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation.”

Michael Nelson, a leading Clinton Administration official on information security and cryptography matters, suggested in September 1996, that traditional notions of sovereignty, national security, and warfare will be undermined by the year 2020, when the whole world is “wired” and e-cash is the norm. The result will be less powerful governments in relation to criminal organizations such as the Mafia and international drug cartels. In addition, computer hackers will pose a more significant threat.

Nelson advocated resolving the issue of whether unauthorized access of a computer is an “act of trespass” or an “act of war,” and prosecuting the intrusions accordingly.

L. Evidentiary Issues and Dispute Resolution

Although some considerations regarding computer evidence have been discussed previously in this Article, one unique development in this area is the creation of on-line forms of dispute resolution. Online dispute resolution potentially is efficient and inexpensive, and solves the difficult problem of the inconvenient forum for electronic commerce transactions. Arrangements for a “Virtual Magistrate” to perform on-line mediation have been endorsed widely and are moving forward. Another pilot project, funded by a grant from the National Center for Automated Information Research, was established at the University of Massachusetts. The project is aimed at using on-line tools to resolve disputes


417. Id. at 37,348.


419. See id.

420. See id.

421. See id.

422. See supra Part IIA (discussing barriers to electronic contracting found in paper-based requirements of current law and reviewing emerging solutions, such as digital signatures).


arising out of both on-line and non-on-line activities. The project is targeted particularly to disputes involving copyrights, domain names, First Amendment, on-line service providers, and harassment.

M. Escheatment

Property that has been abandoned by its owner, under the laws of each state, is escheated or transferred to the state to be used for the benefit of all its citizens. States have enacted detailed escheatment schedules and procedures for all types of property held by financial institutions. This typically includes bank accounts, proceeds of official checks or traveler's checks, safe deposit box property, insurance proceeds, and book-entry securities and dividends.

No state has passed any rule on escheatment of unused value on a SVC yet, although New York has begun to study the issues. Commentators have recommended that stored value be escheatable only when it is redeemable for cash. In all other cases (such as non-redeemable telephone cards), the proceeds should be considered income to the issuer, regardless of whether the card is used. The problem of an issuer avoiding escheatment obligations by contractually limiting redemption options has been identified, but remains unresolved.

N. Antitrust

Antitrust law sometimes is thought of as a counterweight to intellectual property protection. It is intended to promote competi-
tion and to minimize market dominance, while intellectual property laws grant monopoly rights.

In the antitrust area, one must contend with shifting and somewhat vague standards of enforcement; however, continued vigilance is warranted in the areas of horizontal and vertical monopolies. Tying arrangements, by which one product or service is obtainable only in conjunction with another independent product or service, are investigated regularly when the practice is shown to hurt competition. In addition to the general antitrust laws, specific anti-tying laws apply directly to banks. Netscape openly has encouraged the Justice Department to investigate Microsoft for antitrust violations.

The financial industry also continues to be subject to antitrust scrutiny, particularly as it consolidates within geographic regions. Corestate Bank (original owner of the MAC ATM Network in Pennsylvania), Checkfree and Intuit (non-bank bill payment processors), and Visa and MasterCard have been the subjects of federal and state investigations.

O. Regulation Y

The Federal Reserve announced on August 23, 1996, that it is seeking public comment on proposals that will lighten banks' regulatory load when they apply to acquire other banks and broaden their list of permitted non-banking activities. The proposals would amend Federal Reserve Regulation Y. Underlying the proposal is the recognition of rapidly changing financial markets due to technology and new products. Included in this announcement are proposals to expand banks' permitted data processing services to

---

434. See Northern Pac. Ry. Co. v. United States, 356 U.S. 1, 5-7 (1958) (defining tying arrangement as “an arrangement by a party to sell one product but only on the condition that the buyer also purchases a different (or tied) product, or at least agrees that he will not purchase that product from any other supplier” and finding such an arrangement to be an unlawful restraint on trade).


437. See Linda Fickenscher, IBAA Backs Visa in Amex-Inspired Antitrust Probe, AM. BANKER, Feb. 27, 1997, at 12 (reporting that MasterCard is being investigated by DOJ); Microsoft and Intuit Abandon Merger Challenged by Justice Department, BNA ANTITRUST & TRADE REG. DAILY, May 25, 1995, available in WESTLAW, BNA-ATD Database; Justice Targets Regional ATM Network in Administration’s First Tying Case, BNA ANTITRUST & TRADE REG. DAILY, Apr. 22, 1994, available in WESTLAW, BNA-ATD Database; see also SCFC ILC, Inc. v. Visa USA, Inc., 36 F.3d 958, 972 (10th Cir. 1994) (holding, in private civil action, that Visa’s denial of membership to Sears, Roebuck did not violate antitrust laws).


include services of a non-financial nature, provided that the non-financial services do not exceed thirty percent of the company's total annual revenues derived from data processing and data transmission activities.440

P. Omnibus Appropriations Act

President Clinton signed an omnibus budget bill on September 30, 1996, guaranteeing that the government would not shut down when the new fiscal year started the next day.441 Due to a self-created budget emergency, the bill was passed by Congress quickly with little or no debate of its provisions. The bill combined six major spending bills.442

Title II of Division A of the spending bill is named the Economic Growth and Regulatory Paperwork Reduction Act of 1996.443 Sections of Title II that are especially relevant to banks in the electronic commerce area include: (1) credit reporting reform;444 (2) asset conservation, lender liability, and deposit insurance reform;445 (3) new criminal sanctions for fictitious financial instruments and counterfeiting (including e-cash);446 (4) a bank fee study;447 (5) elimination of unnecessary banking regulations;448 (6) streamlining of the process for determining new permissible nonbanking activities;449 and (7) elimination of branch application requirements for automated teller machines.450

450. See id. § 2205 (to be codified at 12 U.S.C. §§ 36(j) and 1813(o)).
CONCLUSION

Just a year ago, it was fashionable to describe the Internet as a new "Wild West," and to classify the state of law on the Internet as chaotic. It would not be unreasonable to say that the Wild West has become populated by legislators seeking to pass a plethora of laws regulating electronic commerce and the Internet.

To some extent, one could view the current situation as a legislative laboratory in which one hopes the best laws will be copied and the worst will disappear. In the long term, that result likely will happen. For now, however, the rush to pass laws has created incredible confusion in some areas of electronic commerce, and the absence of standards has resulted in uncertainty in other areas. It is interesting in this situation how much reliance Americans put on the courts to produce fair and equitable results.

Some members of the banking industry have advocated the delay or avoidance of new legislation and regulation. Ultimately, this is an unlikely scenario, and not necessarily a desirable goal. Just as the presence of Reg E and Reg Z have promoted consumer acceptance of debit and credit cards, it is likely that new electronic forms of money will blossom only after suitable consumer protections are put into place.

National security, taxes, privacy, and the promotion of a feeling of confidence remain some of the more pressing legislative needs in electronic commerce. Banks will have to focus more on these new issues, as they reflect on the future of the industry. Experts have warned that those banks that do not do their homework today, and therefore fail to understand the new banking environment, will not exist to compete tomorrow. Internet branching, home banking, payment services, e-cash, advertising, securities offerings, information distribution, regulatory filings, electronic contracting, and EDI services are being offered today by forward-looking financial institutions. Institutions that can plan for the future also have a unique opportunity to add their voices to legal and social debates and to affect fundamental new legislation. The world has shown that it will move forward; whether banks continue to play a role is up to them today.

That role may involve completely new models of business as the PKI matures and creates a sizeable market for new products and services. Banks are logical offerors of some of these services, such as registration, certification, escrow, and data storage services. The future is still very much in doubt for many banks, but it is hopeful for those that seize today's opportunities.
Recommendation 1: No law should bar the manufacture, sale, or use of any form of encryption within the United States.

Recommendation 2: National cryptographic policy should be developed by the executive and legislative branches on the basis of open public discussion and governed by the rule of law.

Recommendation 3: National cryptographic policy affecting the development and use of commercial cryptography should be more closely aligned with market forces.

Recommendation 4: Export controls on cryptography should be progressively relaxed but not eliminated.

4.1—Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable. Today, products with encryption capabilities that incorporate 56-bit DES provide this level of confidentiality and should be easily exportable.

4.2—Products providing stronger confidentiality should be exportable on an expedited basis to a list of approved companies if the proposed product user is willing to provide access to decrypted information upon legally authorized request.

4.3—The U.S. government should streamline and increase the transparency of the export licensing for cryptography.

Recommendation 5: The U.S. government should take steps to assist law enforcement and national security to adjust to new technical realities of the information age.

5.1—The U.S. government should actively encourage the use of cryptography in nonconfidentiality applications such as user authentication and integrity checks.
5.2—The U.S. government should promote the security of the telecommunications networks more actively. At a minimum, the U.S. government should promote the link encryption of cellular communications and the improvement of security at telephone switches.

5.3—To better understand how escrowed encryption might operate, the U.S. government should explore escrowed encryption for its own uses. To address the critical international dimensions of escrowed communications, the U.S. government should work with other nations on this topic.

5.4—Congress should seriously consider legislation that would impose criminal penalties on the use of encrypted communications in interstate commerce with the intent to commit a federal crime.

5.5—High priority should be given to research, development, and deployment of additional technical capabilities for law enforcement and national security to cope with new technological challenges.

Recommendation 6: The U.S. government should develop a mechanism to promote information security in the private sector.