

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

* Richard Field, Esquire (field@pipeline.com) chairs the Electronic Commerce Payment Committee of the American Bar Association, Section of Science and Technology. He is a co-author of the ABA's *Model EDI Payments Agreement* (1992) and its *Digital Signature Guidelines* (1996). Mr. Field has served as a U.S. delegate-advisor to the United Nations Commission on International Trade Law ("UNCITRAL"), Working Group on Electronic Commerce, and is an Affiliated Research Fellow of the Institute for Tele-Information ("C.I.T.I.") at Columbia Business School. He is a former in-house advanced technology and payment counsel at Manufacturers Hanover Trust Company, New York, and Morgan Guaranty Trust Company of New York. Mr. Field holds undergraduate degrees in Applied Mathematics and Engineering from *Brown University* and a J.D. from *New York University*.

3. Regulations CC, D, J, and operating circulars	978
4. Federal Deposit Insurance Corporation ("FDIC")	979
5. Comptroller of the Currency	981
6. Bank Secrecy Act regulations	981
C. Private Sector Rules	982
II. Recent Developments in Other Areas of Electronic Banking and Commerce	982
A. Electronic Contracting and Digital Signatures	982
B. Regulation of Cryptography	991
C. Intellectual Property Developments	999
1. Copyright	999
2. Trademarks	1000
3. Patents	1001
4. Trade secrets	1002
5. Web site links	1002
D. Privacy and Publicity	1003
1. Banking privacy	1003
2. Database protection	1004
3. Consumer database privacy	1005
4. Employee e-mail monitoring	1006
E. Telecommunications Act of 1996	1007
F. Taxation and the Internet	1011
G. Securities Industry On-line	1013
H. Government Benefits	1013
I. Advertising and Deceptive Practices	1015
J. Jurisdiction and Interstate Banking	1018
K. Criminal Conduct On-line	1019
L. Evidentiary Issues and Dispute Resolution	1020
M. Escheatment	1021
N. Antitrust	1021
O. Regulation Y	1022
P. Omnibus Appropriations Act	1023
Conclusion	1024
Appendix	1025

SYNOPSIS

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,¹ which governs commercial wire transfers. Others are much more specific in their objectives, such as Federal Reserve Regulation E,² which governs electronic funds transfer ("EFT") access to consumer bank accounts, and Federal Reserve Regulation Z,³ 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 3⁴ and 4,⁵ 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

1. U.C.C. art. 4A (1990).

2. Electronic Fund Transfers, 12 C.F.R. pt. 205 (1996).

3. Truth in Lending, 12 C.F.R. pt. 226.

4. U.C.C. art. 3 (1987).

5. *Id.* art. 4.

updated and revised frequently over the past forty years.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 truncation⁷ and electronic presentment.⁸ Although the majority of states have adopted these revisions,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,¹⁰ or unless he subsequently ratifies the instrument.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.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.¹³ This protection has permitted negotiable instruments to be accepted in trade without

6. See 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).

7. See, e.g., U.C.C. § 4-406(a) (amended 1990), 2B U.L.A. 65-66 (1991 & Supp. 1996) (facilitating truncation by streamlining banks' duties to customers).

8. See, e.g., U.C.C. § 4-110 (amended 1990), 2B U.L.A. 25 (1991 & Supp. 1996) (providing that transmission of an image may constitute presentment without delivery of item itself under agreement for electronic presentment).

9. See U.C.C. art. 3 (amended 1990), 2 U.L.A. 3-5 (Supp. 1996) (listing states that have adopted revised Article 3); 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).

10. See U.C.C. § 3-401(a) (1990).

11. See *id.* § 3-403(a).

12. See *id.* § 3-406 (precluding assertion of forgery by person whose negligence substantially contributes to instrument's alteration).

13. See *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.¹⁴ In part, this interpretation hinges on the requirement that negotiable instruments must be in writing.¹⁵ State legislatures are beginning to see the introduction of proposals to expand the definition of a writing to include electronic writings.¹⁶ 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 4A¹⁷ contains the U.S. rules for wholesale funds transfers. Between 1990 and 1996, it was enacted by forty-nine of fifty states.¹⁸ Article 4A was the first comprehensive legislation addressing

14. See, e.g., David Frisch & Henry D. Gabriel, *Much Ado About Nothing: Achieving Essential Negotiability in an Electronic Environment*, 31 IDAHO L. REV. 747, 747-51 (1995) (stating that electronic communication technologies are overlooked by U.C.C.). See generally *Department of Retirement Serv. v. Kralman*, 867 P.2d 643, 647 (Wash. Ct. App. 1994) (noting that federal courts uniformly have concluded that U.C.C. does not apply to electronic fund transfers (citing *Bradford Trust Co. v. Texas Am. Bank*, 790 F.2d 407, 409 (5th Cir. 1986); *Evra Corp. v. Swiss Bank Corp.*, 673 F.2d 951 (7th Cir. 1982); *Delbrueck & Co. v. Manufacturers Hanover Trust Co.*, 609 F.2d 1047 (2d Cir. 1979); *Shawmut Worcester County Bank v. First Am. Bank & Trust*, 731 F. Supp. 57, 62 (D. Mass. 1990); *Waler v. Texas Commerce Bank, N.A.*, 635 F. Supp. 678, 681 (S.D. Tex. 1986)).

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).

16. See, e.g., California Digital Signature Act, CAL. GOV'T CODE § 16.5 (West 1995); 46 UTAH CODE ANN. § 403 (1996); FLA. STAT. ANN. §§ 282.70 to .75 (West 1997); S.736, 143d Leg., Reg. Sess. (Ga. 1996); Draft Massachusetts Electronic Records & Signatures Act (Feb. 7, 1997) <<http://www.magnet.state.ma.us/itd/legal/mersa.htm>> (on file with *The American University Law Review*); Draft Illinois Electronic Commerce Security Act (Jan. 13, 1997) <http://www.mbc.com/ds_stat.htm> (on file with *The American University Law Review*).

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

18. See Mark Sneddon, *Symposium: Is the U.C.C. Dead, or Alive and Well? International Perspectives: The Effect of Uniform Commercial Code Article 4A on the Law of International Credit Transfers*, 29 LOY. L.A. L. REV. 1107, 1109 (1996).

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

19. See U.C.C. § 4A-202(b).

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).

23. See U.C.C. §§ 4A-103, -108.

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).

25. U.C.C. art. 5 (1995).

26. U.C.C. art. 7 (1987).

1994).²⁷ 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").²⁸

A noteworthy new Article 8 was approved by NCCUSL in 1994.²⁹ 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.³⁰ 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.³¹ It had its first NCCUSL "reading" during the summer of 1996.³² Currently, its scope covers all licenses of information, as well as all contracts involving software (including sales of mass-market software).³³ 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).

28. See Model Law on Electronic Commerce, UN Comm. on Int'l Trade Law ("UNCITRAL"), U.N. Doc. A/51/Supp. 17, Annex 1, arts. 16-17 (1996), available in <<http://www.un.or.at/uncitral/texts/electcom/english/ml-ec.htm>>.

29. See 2C U.L.A. 38 (Supp. 1996).

30. See 2C U.L.A. 41 (Supp. 1996) (citing need for legal rules for indirect holding systems).

31. See *Commercial Law Update Hits Rough Spot Over Licensing: Does UCC 2B Favor Software Vendors Over Users?*, INFO. L. ALERT: VORHEES REP., Oct. 11, 1996, available in 1996 WL 8913667 (remarking that timetable from Article 2B adoption is "rocket-fast in the glacial world of commercial code revision").

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 E³⁵ ("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).

35. Electronic Fund Transfers, 12 C.F.R. pt. 205 (1996).

36. 15 U.S.C. § 1693 (1994).

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).

financial institution.⁴⁰ This protection exists even if the account holder's negligence enabled the unauthorized person to access the account.⁴¹ 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.⁴²

On May 2, 1996, the FRB proposed amendments to Reg E.⁴³ These amendments would define, for the first time, the level of Reg E consumer protection for funds located on SVCs.⁴⁴ 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.⁴⁵

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;⁴⁶

(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;⁴⁷ and

(3) *On-line accountable*: the card is used only to request a transfer at the bank's central database.⁴⁸

In general, the FRB has proposed that off-line unaccountable cards would not be regulated by Reg E,⁴⁹ off-line accountable cards would be regulated minimally, with only a disclosure to consumers required,⁵⁰ and on-line accountable cards would be regulated under the current Reg E, with modifications.⁵¹ In addition, any card capable of storing a maximum of \$100 would be exempted from the regulation.⁵²

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).

43. See Electronic Fund Transfers, 61 Fed. Reg. 19,696 (1996) (to be codified at 12 C.F.R. § 205) (proposed May 2, 1996).

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).

46. See 61 Fed. Reg. 19,696, 19,701.

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).

54. See Omnibus Consolidated Appropriations Act, 1997, Pub. L. No. 104-208, § 2601, 1996 U.S.C.A.N. (110 Stat.) 3009 (1996).

55. See Commission Draft Recommendation Concerning Payments Effected Through a Payment Card, Including Pre-Paid Cards (Brussels, 1996) (working draft); Commission Draft Recommendation Concerning Payments by Means of an Electronic Payment Facility without a Payment Card (Brussels, 1996) (working draft).

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

56. Truth in Lending, 12 C.F.R. pt. 226 (1996).

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).

61. See MasterCard International, *Secure Electronic Transactions* (last modified Aug. 7, 1996) <<http://www.mastercard.com/set/set.htm>> (on file with *The American University Law Review*); Visa, *Secure Electronic Commerce* (visited Mar. 11, 1997) <<http://www.visa.com/cgi-bin/vee/sf/standard.html?2+0>> (on file with *The American University Law Review*).

62. 12 C.F.R. pt. 229.

63. See *id.* § 229.1 (stating that regulation contains rules to expedite collection and return of checks by banks).

collection and return of checks.⁶⁴ Reg CC establishes new legal and operational principles designed to expedite the collection and return of checks.⁶⁵ As a result, it preempts portions of U.C.C. Articles 3 and 4.⁶⁶

Regulation D ("Reg D"), Reserve Requirements of Depository Institutions,⁶⁷ requires that depository institutions set aside reserves to cover a percentage of their transaction account balances, such as checking accounts.⁶⁸ Non-transaction account balances, such as savings accounts, require little or no reserves.⁶⁹ Permitting remote access to an account, such as by computer or telephone, may require it to be classified as a transaction account.⁷⁰ A reserve requirement analysis pertaining to SVCs also may be forthcoming, although no proposal has been announced.⁷¹

Regulation J ("Reg J"), Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers through FedWire,⁷² describes the FRB's responsibilities in its check collecting and FedWire services.⁷³

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.⁷⁴

4. Federal Deposit Insurance Corporation ("FDIC")

On August 2, 1996, the FDIC published its General Counsel's Opinion No. 8.⁷⁵ 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.⁷⁶ Instead, for purposes of analyzing deposit insurance coverage, the General Counsel's Opinion

64. See Expedited Funds Availability Act, 12 U.S.C. §§ 4001-4010 (1994).

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).

71. See Richard L. Field, *Reserve Requirements: Implications for Stored Value Cards*, ELECTRONIC BANKING L. & COM. REP. (forthcoming 1997).

72. 12 C.F.R. pt. 210.

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.").

75. FDIC General Counsel's Opinion No. 8; Stored Value Cards, 61 Fed. Reg. 40,490 (1996).

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 categories⁷⁷ based on the statutory definition of "deposit" in the FDIA.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;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;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;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.⁸²

The General Counsel's Opinion concludes that in most cases SVCs are not protected by deposit insurance.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.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

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

78. See 61 Fed. Reg. at 40,490-91 (citing 12 U.S.C. § 1813(1) (1994)).

79. See *id.* at 40,490.

80. See *id.*

81. See *id.*

82. See *id.*

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.").

84. See *Stored Value Cards and Other Electronic Payment Systems*, 61 Fed. Reg. 40,494 (1996).

treated as insured deposits under general usage.⁸⁵ 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.⁸⁶

On September 10, 1996, the OCC issued Guidelines on SVCs.⁸⁷ The Guidelines emphasized adherence to the payment system risk factors previously identified by the OCC.⁸⁸

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.⁸⁹ 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.⁹⁰ Because fund transfers of under \$3000 are not covered by the rule,⁹¹ 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).

87. See Stored Value Card Systems, OCC Bulletin 96-48 (Sept. 10, 1996), available in LEXIS, BANKING Library, ALLOCC File.

88. See *id.*

89. See Amendment to the Bank Secrecy Act Regulations Relating to Record Keeping for Funds Transfers and Transmittals of Funds by Financial Institutions, 60 Fed. Reg. 220 (1995) (to be codified at 31 C.F.R. pt. 103). The rule became effective May 28, 1996.

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.⁹² MasterCard and Visa are in the process of finalizing their SET documents for secure Internet credit card payments and other transactions.⁹³

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.⁹⁴ These documents include: (1) contracts for the sale of goods in excess of \$500;⁹⁵ (2) contracts that, by their terms, cannot be completed within one year;⁹⁶ (3) contracts for the sale of land;⁹⁷ (4) contracts that guaran-

92. See generally BANKERS EDI COUNCIL, NAT'L AUTOMATED CLEARING HOUSE ASS'N, CORPORATE FINANCIAL EDI USER GUIDE (1993).

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).

94. See RESTATEMENT (SECOND) OF CONTRACTS § 110 (1981).

95. See *id.* § 110(2)(a).

96. See *id.* § 110(1)(e).

97. See *id.* § 110(1)(d).

ty the debts of another person;⁹⁸ and (5) certain other contracts, such as agreements made in contemplation of marriage.⁹⁹

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

Finally, there has been some confusion over how and when an electronic contract is created, as well as its enforceability.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.¹⁰⁵ Evidentiary and nonrepudiation issues have received substantial focus.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.¹⁰⁷ The laws of evidence, both at the state and federal levels, now permit the introduction of electronic records and documents.¹⁰⁸ The Federal Acquisition Regulations ("FAR") have been modified to permit electronic bidding and contracting in contracts with the federal government.¹⁰⁹ Most federal government agencies have addressed the use of electronic

98. See *id.* § 110(1)(b).

99. See *id.* § 110(1)(c).

100. See, e.g., U.C.C. § 2-201(1) (1990).

101. See, e.g., 15 C.F.R. § 762.4 (1996).

102. See MCCORMICK ON EVIDENCE §§ 288-290 (John William Strong et al. eds., 4th ed. 1992) (describing requirements for admissibility).

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).

104. See Thomas L. Lockhart & Patrick A. Miles, Jr., *No More Pulp Fiction: Proposed UCC Article 2 Revisions Embrace Paperless Electronic Transactions*, 75 MICH. B.J. 516, 516 (1996).

105. See INFORMATION SECURITY COMMITTEE, SECTION OF SCIENCE AND TECH., AMERICAN BAR ASS'N, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE (1996) [hereinafter DIGITAL SIGNATURE GUIDELINES]; Scott K. Pomeroy, Comment, *Promoting the Progress of Science and the Useful Arts in the Digital Domain: Copyright, Computer Bulletin Boards, and Liability for Infringement by Others*, 45 EMORY L.J. 1035, 1086 (1996).

106. See A. Michael Froomkin, *Symposium: Innovation and the Information Environment, The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 69 (1996).

107. See, e.g., U.C.C. § 4A-201 (1990).

108. See R. David Whitaker, *Letters of Credit and Electronic Commerce*, 31 IND. L. REV. 699, 708 (1995) (suggesting that Federal Rules of Evidence 803(6) and 1001 allow admission of electronic records kept in ordinary course of business).

109. See Federal Acquisition Regulations, 48 C.F.R. § 14.202-8 (1996) (authorizing contract officers to accept electronic bids).

records and documents.¹¹⁰ And states such as California have enacted legislation permitting the use of electronic signatures in communications with public entities.¹¹¹

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")¹¹² and digital signatures.¹¹³

There is increasing consensus that digital signatures are an appropriate solution for many problems in electronic commerce.¹¹⁴ They can be used to authenticate the accuracy of a message that has been transmitted via unsecure communication facilities, such as the Internet.¹¹⁵ 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. GOV'T 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).

114. See Jessica R. Friedman, *A Lawyer's Ramble Down the Information Superhighway: Copyright*, 64 *FORDHAM L. REV.* 705, 719 (1995) (advocating use of digital signatures for authentication and identification of copyrighted material transmitted over Internet); Byron F. Marchant, *On-Line on the Internet: First Amendment and Intellectual Property Uncertainties in the On-Line World*, 39 *HOW. L.J.* 477, 488-89 (1996) (supporting use of digital signatures as secure mechanism to authenticate electronic communications); see also A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 *J.L. & COM.* 395, 423 n.81 (1996) (arguing that digital signatures copied from one message have only a very slight chance of authenticating other messages because any slight variation in signatures will disrupt encryption algorithms and will render authentication nearly impossible).

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.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.¹¹⁷ Securing the message, instead of the entire communications system, is widely believed to be a natural and desirable evolutionary step.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 *Digital Signature Guidelines* on August 1, 1996.¹¹⁹ The *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 authorizing the use of digital signatures in commerce, making extensive reference to the *Guidelines*.¹²⁰ Early drafts of the proposed German digital signature law also cited the *Guidelines*.¹²¹

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

116. See generally Henry H. Perritt, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems*, 22 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., *President Clinton's National Information Infrastructure Initiative: Community Regained?*, 69 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).

117. See generally Theodore S. Barassi, *Cybernotary: Addressing Technical Problems with On-Line Commerce; A Brave New Area of Specialization for Lawyers?*, 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).

118. See generally DIGITAL SIGNATURE GUIDELINES, *supra* note 105.

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 *The American University Law Review*).

120. See 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).

121. See generally *Germany Drafts Multimedia Law Regulating Internet*, 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. See Terrence Gallagher, *Bonn Aims to Rein in Lawlessness in Cyberspace*, REUTERS 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).

123. See CONN. GEN. STAT. §§ 19a-25a (Supp. 1994) (enacting regulations regarding use of electronic signatures for medical records).

124. See FLA. STAT. chs. 282.70-74 (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, ALLCODE File (establishing legal framework for using digital signatures as a means of authenticating computer information).

126. See IOWA CODE § 48A.13 (Supp. 1997) (accepting electronic signatures on voter registration records).

127. See LA. REV. STAT. ANN. § 40:2145 (West Supp. 1996) (permitting health care providers to use electronic signatures on hospital records).

128. See H.J.R. 129, 1996 Sess. (Va.), available in LEXIS, LEGIS Library, TRCK96 File (addressing digital signature and electronic commerce issues).

129. See WASH. REV. CODE § 19.34.010 (Supp. 1997) (establishing uniform rules regarding authentication and reliability of electronic messages).

130. See GA. CODE ANN. § 21-2-221 (Supp. 1997) (authorizing Secretary of State and commissioner of public safety to promulgate regulations for acceptance of electronic signatures on voter registration applications); S.R. 621, 143d Leg., 1995-96 Reg. Sess. (Ga. 1996), available in LEXIS, LEGIS Library, TRCK96 File (creating Joint Digital Signatures Study Committee).

131. See H.B. 3394, 89th Leg., 1995-96 Reg. Sess. (Ill. 1996), available in LEXIS, STATES Library, ALLCODE File (encouraging use of digital signatures to authenticate electronic communications between state agencies and comptrollers).

132. See Draft Massachusetts Electronic Records & Signatures Act (Feb. 7, 1997) <<http://www.magnet.state.ma.us/itd/legal.mersa.htm>> (on file with *The American University Law Review*).

133. See S.B. 939, 88th Leg., Reg. Sess. (Mich. 1996), available in LEXIS, LEGIS Library, TRCK96 File (regulating computer communication and digital signatures); S.B. 1207, 88th Leg., Reg. Sess. (Mich. 1996), available in LEXIS, LEGIS Library, TRCK96 File (allowing digital signatures to be used at polling places).

134. See S.B. 7420, 219th Leg., 2d Reg. Sess. (N.Y. 1996).

135. See Brian Chin, *TechNotes: Marketers' Ability to Collect E-Mail Addresses Is Blocked*, PUGET SOUND BUS. J., Mar. 22, 1996, available in 1996 WL 10057248 (reporting that digital signature legislation failed to reach vote in Oregon legislature).

136. See H.B. 8125, 1996 Sess. (R.I.), available in LEXIS, LEGIS Library, TRCK96 File (establishing digital signature provisions).

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. 63, § 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).

142. See CHEMICAL BANK, CUSTOMER IDENTIFICATION STRATEGY: BIOMETRICS ARE THE FUTURE (1996).

143. See *id.*

identify securely gems, artwork, and other objects.¹⁴⁴ 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."¹⁴⁵ A cybernotary would be a person or firm with the capability to authenticate international electronic transactions.¹⁴⁶ 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.¹⁴⁷ Substantial assistance has been provided by the International Union of Latin Notaries, which is expanding the cybernotary concept internationally.¹⁴⁸

A federal PKI Steering Committee has been organized to coordinate efforts by executive agencies to use public key digital signature technology.¹⁴⁹ 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.¹⁵⁰

The United States Postal Service is developing "Postal Electronic Commerce Services" that will provide security and integrity to

144. See Suzanne Muchnic, *Have Forgers Finally Met Their Match? A New Digital Registration Process Could Discourage Forgery and Theft and Help Resolve Disputes About Authenticity and Ownership of Valuable Artworks*, L.A. TIMES, July 2, 1995, at 50. Verification Technologies, Inc., premises its digital registration process, promoted as ISIS (Intrinsic Signature Identification System) and named for the Egyptian goddess of secrets, on the idea that all objects contain "unique microscopic physical features and random anomalies that cannot be duplicated." *Id.* Using a high-powered video-microscope, ISIS can magnify details up to 2000 times their actual size. See *id.* These magnified images, known as "virtual fingerprints," then are encrypted onto a registration record using specially designed software. See *id.* Finally, the images are stored in the company's computer archive, along with a descriptive text. See *id.* For security purposes, Verification Technologies maintains back-up copies of its registration records and stores them on CD-Roms at various locations. See *id.*

145. See Barassi, *supra* note 117, at 1 (exploring function of cybernotaries, as proposed by CyberNotary Project at U.S. Council for International Business).

146. See *id.* (proposing that cybernotaries, with expertise in technical and legal security matters, serve as CAs for international notarial transactions).

147. See Victoria Slind-Flor, *Moving into Cyberspace as Notaries*, NAT'L L.J., Dec. 18, 1995, at 1; David Sommer, *New Legal Code: Sign It by Modem; Florida's Electronic Signature Act Has Become Law, But How It Will Be Implemented Isn't Clear Yet*, TAMPA TRIB., June 3, 1996, at 1.

148. See generally Theodore Sedgwick Barassi, *The Cybernotary: Public Key Registration and Certification and Authentication of International Legal Transactions* (visited Feb. 22, 1997) <<http://www.intermarket.com/eci/cybrnote.html>> (on file with *The American University Law Review*) (providing information about, and proposed role for, cybernotaries).

149. See generally PKI Technical Working Group (visited Feb. 24, 1996) <<http://csrc.nsl.nist.gov/pki/twg/twgindex.html>> (on file with *The American University Law Review*).

150. See *id.*

electronic correspondence and transactions, giving them attributes usually associated with first-class mail.¹⁵¹ 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.¹⁵² 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.¹⁵³ Commercial banks, the largest U.S. users of first-class mail, have the potential to become an important user of this type of service.¹⁵⁴

Notably, the Postal Service withdrew from its prior announcements its offer of general CA services.¹⁵⁵ It advised that it might offer general CA services at a later time if a market for such services developed.¹⁵⁶

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 1996.¹⁵⁷ 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.¹⁵⁸ It has been crafted carefully and is a valuable model for

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

152. See Jon Auerbach, *E-Mail Could Arrive with U.S. Postmark*, B. GLOBE, Sept. 19, 1996, at A1 (outlining Postal Service's plan to secure electronic messages by "postmarking" them as assurance against tampering); Barb Cole, *U.S. Postal Service to Lick E-Mail Security Problems*, NETWORK WORLD, Sept. 23, 1996, at 14 (same).

153. See Postal Electronic Commerce Service, 61 Fed. Reg. 42,219 (1996) (to be codified at 39 C.F.R. pt. 701). Comments on the proposal were accepted until September 13, 1996. See *id.*

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.

156. See 61 Fed. Reg. at 42,219.

157. See Model Law on Electronic Commerce, *supra* note 28.

158. See *id.* (covering validity of computer messages in commercial transactions, as well as special rules governing electronic bills of lading).

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.¹⁵⁹ 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,¹⁶⁰ and a Uniform International Authentication and Certification Practices working group that is developing practice guidelines.¹⁶¹ 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.¹⁶²

One additional barrier to the use of on-line contracts has been a continued question as to their enforceability.¹⁶³ This debate follows similar questions about the enforceability of "shrink-wrap" licenses, which are standard form licenses distributed inside a software or similar package.¹⁶⁴ 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*,¹⁶⁵ 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; (34) 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>>.

160. See International Chamber of Commerce, Status Report on ETERMS, Summary of Project Progress, Guidelines and Criteria, Meeting of Apr. 10, 1996, Annex I to Doc. No. E100/7; ETERMS Repository Guidebook, DRAFT Version 0.6, Sept. 23, 1996.

161. See ICC Document No. E100-26/1, Draft "Uniform International Authentication and Certification Practices" ("UIACP").

162. See *supra* note 160.

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

164. See Chad G. Asarch, Note, *Is Turnabout Fair Play? Copyright Law and the Fair Use of Computer Software Loaded into RAM*, 95 MICH. L. REV. 654, 668 n.62 (1996).

165. 86 F.3d 1447 (7th Cir. 1996).

of the trial court.¹⁶⁶ 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.¹⁶⁷

Finally, a clear validation of on-line contracts would be contained in U.C.C. Article 2B, as it currently is being drafted.¹⁶⁸

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.¹⁶⁹ 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.¹⁷⁰ 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"),¹⁷¹ which

166. See *ProCD v. Zeidenberg*, 86 F.3d 1447, 1454 (7th Cir.), *rev'g* 908 F. Supp. 640 (W.D. Wis. (1996)).

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").

168. See Michael Rustad & Lori E. Eischmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213, 278 (1995) (analyzing application of proposed Article 2B to intangible contracts and its validation of "electronic contract formation by exchange of records").

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 ("[S]ophisticated encryption technology has been used for years to protect electronic funds transfer.").

170. See Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189, 198 (1996) (outlining critics' arguments, but concluding that clipper chip does not threaten privacy).

171. 22 C.F.R. pts. 121-130 (1997).

contains a Munitions Control List of controlled military articles, including cryptography.¹⁷²

Items and technology that are not controlled by ITAR may be regulated under the Export Administration Regulations ("EAR"),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.¹⁷⁴ Recently, the regulations were restructured and reorganized.¹⁷⁵

The National Security Agency ("NSA"), branches of the U.S. military, and others advise regulators on cryptography export issues.¹⁷⁶ In practice, the NSA retains substantial control over U.S. cryptography export policy.¹⁷⁷ Enforcement of export policy is assigned to the U.S. Customs Service.¹⁷⁸ United States shipments, transmissions, and disclosures of hardware, software, and technical data to a location abroad are considered regulated exports.¹⁷⁹ Re-exports of U.S.-origin materials also are regulated,¹⁸⁰ as are disclosures to foreign nationals within the United States.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 *How to Make a Mint: The Cryptography of Anony-*

172. See The United States Munitions List, 22 C.F.R. pt. 121.

173. Export Administration Regulations, 15 C.F.R. ch. VII, subch. C (1997).

174. See *id.* pt. 774 cat. 5(11).

175. See *id.* § 730.5.

176. See David Banisar, *Roadblocks on the Information Superhighway*, 41 FED. B. NEWS & J. 495, 496 (1994) (noting concern Congress has with allowing NSA to control access of non-military computer systems).

177. See *id.* ("NSA plays a major role in determining rules for exporting US products with encryption capabilities.")

178. See Patricia A. Sherman, *Controls on the Export of Technical Data*, in COPING WITH U.S. EXPORT CONTROLS 1986, at 125, 127 (PLI Com. L. & Practice Course Handbook Series No. 398, 1986) ("[F]or unclassified controlled exports, Commerce and the Customs Service have the primary enforcement and counter-intelligence responsibility.")

179. See 15 C.F.R. § 730.5.

180. See *id.* § 730.5(a); see also Cecil Hunt, *Going International: Fundamentals of International Business Transactions*, ALI-ABA, Course of Study No. 4, July 8, 1996, at 431, 433 (noting that re-exports are regulated by Export Administration Regulations).

181. See 15 C.F.R. § 730.5(c) (requiring license for disclosure of technical data by "U.S. persons in connection with visits to foreign diplomatic missions and consular offices").

mous Electronic Cash.¹⁸² It reviews the basic cryptography of anonymous cash,¹⁸³ as well as the cryptography of optional features such as transferability,¹⁸⁴ divisibility,¹⁸⁵ and multiple spending prevention.¹⁸⁶

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.¹⁸⁷ The original Clipper proposal (informally called "Clipper I") used a government-provided undisclosed encryption algorithm.¹⁸⁸ Keys would be issued by the government, and two government agencies each would retain half of the key.¹⁸⁹ Complete keys were to be available to any government agency only with good cause, and only in accordance with proper judicial or agency process.¹⁹⁰ Use of other encryption systems was to be permitted domestically, but permission to export was likely to be denied.¹⁹¹

Clipper I received an extremely negative public reaction, and was withdrawn.¹⁹² 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.¹⁹³ As with Clipper I, the government would have access to keys (informally referred to as "GAK") in accordance with legal process.¹⁹⁴ No clear distinction was

182. Laurie Law et al., *How to Make a Mint: The Cryptography of Anonymous Electronic Cash*, 46 AM. U. L. REV. 1131 (1997).

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.

191. See, e.g., Stewart A. Baker, *Government Regulation of Encryption Technology: Frequently Asked Questions*, in, DOING BUSINESS ON THE INTERNET 287, 292 (PLI Pats., Copyrights, Trademarks, & Literary Prop. Course Handbook Series No. 452, 1996) (noting that United States, like most Western countries, does not control domestic use, but United States has focused keenly on controlling and monitoring export of strong encryption).

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).

193. See Howard S. Dakoff, *The Clipper Chip Proposal: Deciphering the Unfounded Fears that Are Wrongfully Derailing Its Implementation*, 29 J. MARSHALL L. REV. 475, 479 (1996).

194. See U.S. *Asked to Hold off on New Encryption Rules*, LAW PRAC. MGMT. COMPUTER & TECH. INDUSTRY NEWS, Jan. 7, 1997, available in 1997 WL 2913. "[T]he new rules allow companies to

made between keys used to sign documents and encryption keys. Public reaction to Clipper II was almost as negative as reaction to Clipper I.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, 1996.¹⁹⁶ The recommendations of the NRC Report are included as the Appendix of this article.¹⁹⁷

The NRC recommended a substantial shift in emphasis in favor of commercial use of cryptography, and a relaxation of cryptography export controls.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.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, 1996.²⁰⁰ Major features of the new policy include:

export software with encryption codes of 56 bits or longer, provided they agree to give the government computer 'keys' to allow enforcement of officials to decode protected transmissions." *Id.*

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, *Network 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.").

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.

197. See Appendix, *infra* pp. 1025-26.

198. See Appendix, *infra* pp. 1025-26.

199. See Charles R. Merrill, *A Cryptography Primer*, in DOING BUSINESS ON THE INTERNET 389, 401 (PLI Pats., Copyrights, Trademarks, & Literary Prop. Course Handbook Series No. 452, 1996) (noting that although current export laws allowed only 40 bits to be exported outside United States, NIST proposed in August 1995, to allow export of 64-bit software).

200. See *Statement by Vice President Al Gore*, U.S. Newswire, Oct. 1, 1996, reprinted in COPING WITH U.S. EXPORT CONTROLS 1996, at 717, 831 (PLI Comm. L. & Practice Handbook Series No. A-44512, 1996) [hereinafter *Statement by Vice President Gore*]; see also Mem. & Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996); Bureau of Administration Interim Rule, 61 Fed. Reg. 68,572, 68,587 (1996).

(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.*

205. Editorial, *A Flawed Encryption Policy*, N.Y. TIMES, Oct. 4, 1996, at A32.

206. See *Statement by Vice President Gore*, *supra* note 200, at 831.

207. See *Netscape to Distribute Highly Secure Versions of Netscape Software on the Internet*, M2 PRESSWIRE, July 18, 1996, available in 1996 WL 10348948; David Einstein, *Encrypted Software Shipped on Internet*, SAN FRAN. CHRON., July 16, 1996, at C3.

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.").

209. See *Encryption Law Change: Good News*, PC WK., Oct. 14, 1996, at 67E ("Observers believe that if the 56-bit experiment proves successful, relaxation of the restriction that still covers 128-bit key software will follow.").

introduced the Encrypted Communication Privacy Act of 1996²¹⁰ in March.²¹¹ Congressman Goodlatte (R-Va.) introduced the SAFE²¹² bill soon thereafter.²¹³ Senator Burns (R-Mont.) has introduced the Promotion of Commerce On-line in the Digital Era ("Pro-CODE") Act of 1996,²¹⁴ which would deregulate substantially encryption that is available in foreign markets,²¹⁵ and which was co-sponsored in the Senate by then-Senator Dole (R-Kan.) and enjoyed broad bi-partisan support.²¹⁶ Senator Burns has held open hearings on his bill that have been transmitted over the Internet.²¹⁷ He promised to re-introduce the bill when Congress reconvened in January 1997.²¹⁸ 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.²¹⁹

The Justice Department dropped its case against Phil Zimmerman, inventor of the cryptography program Pretty Good Privacy ("PGP") without comment on January 11, 1996.²²⁰ The program had been

210. S. 1587, 104th Cong. (1996).

211. See 142 CONG. REC. S1516 (daily ed. March 5, 1996) (statement of Sen. Leahy).

212. Security and Freedom Through Encryption (SAFE) Act of 1996, H.R. 3011, 104th Cong. (1996).

213. See 142 CONG. REC. E276 (daily ed. March 5, 1996) (statement by Rep. Goodlatte).

214. See *id.* S4619 (daily ed. May 2, 1996) (statement of Sen. Wellstone).

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).

216. See 142 CONG. REC. S4619, S4624 (daily ed. May 2, 1996) (statement of Sen. Burns (R-Mont.)). Cosponsors of the bill included Sen. Pressler (R-S.D.), Sen. Leahy (D-Vt.), Sen. Dole (R-Kan.), Sen. Faircloth (R-N.C.), Sen. Murray (D-Wash.), Sen. McCain (R-Ariz.), Sen. Wyden (D-Or.), and Sen. Ashcroft (R-Mo.).

217. For information on the bill, see Open Letter to the Internet from Senator Burns (last modified Feb. 27, 1997) <<http://www.senate.gov/~burns/open97.htm>> (on file with *The American University Law Review*).

218. See *Burns Introduces Internet-Friendly Bill* (Feb. 27, 1997) <<http://www.senate.gov/~burns/p-feb27.htm>> (on file with *The American University Law Review*) (announcing re-introduction of Pro-CODE bill).

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.

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.

placed on the Internet in the spring of 1991.²²¹ The Justice Department began its investigation in 1993.²²² 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.²²³ After the investigation was dropped, Mr. Zimmerman promised to continue working on technology that furthers privacy ends.²²⁴

Civil liberties advocates have begun to go on the offensive. In *Bernstein v. Department of State*,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.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.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.²²⁸ In *Junger v. Christopher*,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.²³⁰ Junger's challenge, like Bernstein's, is based on the

221. See *id.*

222. See *id.*

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.

224. See Sandy Shore, *Freedom Fighter Does Battle in Cyberspace; Boulderite's Encryption Software a Weapon?*, DENV. POST, Jan. 28, 1996, at B2.

225. Two reported district court opinions flow from this case. In *Bernstein v. Department of State*, 922 F. Supp. 1426, 1439 (N.D. Cal. 1996) [hereinafter *Bernstein I*], the court denied defendant's motion to dismiss and determined that plaintiff's claims were justiciable. In *Bernstein v. Department of State*, 945 F. Supp. 1279, 1290 (N.D. Cal. 1996) [hereinafter *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.*

226. See *Bernstein II*, 945 F. Supp. at 1282.

227. See *Bernstein I*, 922 F. Supp. at 1436.

228. A number of materials concerning the *Junger* lawsuit, including press releases and pleadings, can be found on the Internet at *Junger v. Christopher* (visited Jan. 28, 1997) <http://samsara.law.cwru.edu/comp_law/jvc> (on file with *The American University Law Review*).

229. No. 1:96 CV 1723 (N.D. Ohio Aug. 7, 1996). See *Junger v. Christopher Complaint* (filed Aug. 7, 1996) <http://samsara.law.cwru.edu/comp_law/jvc/complaint.html> (on file with *The American University Law Review*).

230. See *id.* ¶¶ 32-40.

unconstitutionality of requiring the permission of the government before one can communicate knowledge.²³¹ Earlier decisions have held that such a prior restraint, except in the most unusual of circumstances, is a violation of the First Amendment.²³² Oral argument in *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.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.²³⁴ Completion of the guidelines is expected by early 1997.²³⁵

Questions about the security of payment information were addressed internationally in 1996, with the release of the *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.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.²³⁷ The Smart Card Forum and other industry groups responded immediately with assurances that their architecture

231. See *id.*

232. See *Nebraska Press Assn. 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))).

233. See Michelle Slatalla, *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).

234. See Neil Munro, *Industry Split Forces a Global Encryption Skirmish*, WASH. TECH., May 15, 1996, available in 1996 WL 8827309.

235. See *id.* Working draft guidelines for the September and December, 1996, meetings can be located on the Internet at <<http://193.154.75.3/netzeil/oecd/>> (visited Jan. 28, 1997) (on file with *The American University Law Review*).

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).

237. See John Markoff, *Potential Security Flaw Discovered in "Smart Cards"*, DENV. POST, Sept. 26, 1996, at C3.

includes multiple levels of security, and that roll-out plans for smart cards will not be delayed.²³⁸

C. Intellectual Property Developments

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

238. Cf. David Bank, *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).

239. See 17 U.S.C. § 106 (1994).

240. See generally David M. Maiorana, Comment, *Privileged Use: Has Judge Boudin Suggested a Viable Means of Copyright Protection for the Nonliteral Aspects of Computer Software in Lotus Development Corp. v. Borland International?*, 46 AM. U. L. REV. 149, 157-61 (1996) (discussing application of copyright law to computer software).

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

242. See *Lotus Dev. Corp. v. Borland Int'l, Inc.*, 49 F.3d 807, 815 (1st Cir. 1995), *aff'd by an equally divided court*, 116 S. Ct. 804 (1996) (per curiam).

243. 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.²⁴⁴

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.²⁴⁵ The White Paper provided Congress with the Administration's official recommendations for tailoring federal intellectual property law to fit the growing digital marketplace.²⁴⁶ It concluded that existing copyright law was adequate, with a few minor adjustments.²⁴⁷

The National Information Infrastructure Copyright Protection Act²⁴⁸—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 1996.²⁴⁹ 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.²⁵⁰ The suits were filed against Internet service providers and individuals, alleging both direct and contributory copyright infringement.²⁵¹ The SPA also maintains a hotline where people can report suspected acts of piracy.²⁵²

2. Trademarks

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

244. See *Lotus Dev. Corp. v. Borland Int'l, Inc.*, 116 S. Ct. 804 (1996) (per curiam).

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.*

248. H.R. 2441, 104th Cong. (1995); S. 1284, 104th Cong. (1995).

249. See Mark Crawford, *Internet Copyright Protection: Not by Law Alone?*, NEW TECH. WK., Dec. 9, 1996, available in 1996 WL 12978756, at *3 (noting that House bill did not move out of Judiciary Committee).

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.²⁵³ NSI now has approximately 660,000 ".com" names registered in its InterNIC data base, representing 89% of NSI registrations.²⁵⁴ Claims that NSI's domain name policies are not neutral, but rather favor trademark owners over domain name owners are ongoing.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.²⁵⁶ Domain name owners have brought eighteen lawsuits against NSI and trademark claimants.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 1995²⁵⁸ that would expose an unauthorized user of another's trademark as a domain name or e-mail address to penalties under unfair competition laws.²⁵⁹ Some experts considered the bill alarmingly overbroad.²⁶⁰

3. 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.²⁶¹

253. See David J. Loundy, *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").

254. See generally Internet International Ad Hoc Committee, *Domain Name Surveys and Statistics* (last modified Dec. 11, 1996) <<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).

255. See Loundy, *supra* note 253, at 5.

256. See, e.g., David Hayes, *Site Rights: KC Group Says Its On-line Trademark Turf Has Been Infringed upon by California NonProfit*, KAN. CITY STAR, Feb. 19, 1997, at B1.

257. See Gabe Battista, *Our Approach Is Balanced*, USA TODAY, Jan. 15, 1997, at 10A.

258. Unauthorized Electronic Use of Trademark, S.B. 1034, 1995-96 Reg. Sess. (Cal. 1995).

259. See *id.* § 1.

260. See Ilana DeBare, *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.").

261. See Neil Gross & Amy Cortese, *E-Commerce: Who Owns the Right? E-Data's Patent Claims Are Causing an Outcry—and Raising Fears of an I-Way Full of Roadblocks*, BUS. WK., July 29, 1996, at 65 (discussing controversy surrounding patent protection for electronic commerce).

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.²⁶² 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 1997.²⁶³ 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 1996.²⁶⁴ The Act strengthens protections against theft or misuse of proprietary business information. It makes the theft of trade secrets a federal crime²⁶⁵ and provides financial penalties and prison sentences for specific acts of economic espionage.²⁶⁶ The Act also eliminates gaps in the criminal laws that address attacks against computers and the information they contain.²⁶⁷

5. Web site links

A much-criticized new Georgia law, known as the Georgia Computer Systems Protection Act,²⁶⁸ makes it illegal for organizations to use

262. See Brian Bremner et al., *Hold It Right There Citibank: Japan Could Hobble the Bank in the Race to Develop E-Cash*, BUS. WK., Mar. 25, 1996, at 176 (noting success of Citibank in gaining patent protection in United States); *Connected: The Way They Do Business in Cyberspace*, DAILY TELEGRAPH (LONDON), Nov. 19, 1996, at 8 (explaining that Amsterdam-based DigiCash holds patents to technology designed to guarantee anonymity of electronic payments); *CUs Must Stay Abreast of Tech Issues*, NCUA WATCH, Feb. 12, 1996, at 3, available in 1996 WL 5614347 (noting that Mondex owns patent on its version of encrypted electronic money).

263. See Eamonn Sullivan, *Pretty Good and Getting Better*, PC WK., Apr. 29, 1996, at N5.

264. Pub. L. No. 104-294, 1996 U.S.C.C.A.N. (110 Stat.) 3488 (to be codified at 18 U.S.C. §§ 1831-1839).

265. See *id.* § 101(a), 1996 U.S.C.C.A.N. (110 Stat.) at 3488-89 (to be codified at 18 U.S.C. §§ 1831-1832) (defining crimes of economic espionage, which includes theft of trade secrets, and also defining theft of trade secrets as separate crime).

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).

267. See *Clinton Approves Intelligence Spending Rise*, WASH. POST, Oct. 12, 1996, at A6.

268. 1996 Ga. Laws 1505 (to be codified at GA. CODE ANN. § 16-9-93.1).

trademarks and logos on the Internet without permission.²⁶⁹ The law also prohibits sending e-mail anonymously in some circumstances,²⁷⁰ as well as fraudulently representing one's Website as that of another organization.²⁷¹ The Georgia law imposes a penalty of as many as twelve months in prison and \$1000 in fines.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.²⁷³ The challenge is considered one of the first major assaults on state laws that seek to rein in the Internet.²⁷⁴

D. Privacy and Publicity

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.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 Act²⁷⁶ prohibits the government from obtaining certain types of banking information without due process of law.²⁷⁷ The EFTA²⁷⁸ and Reg E²⁷⁹ contain minimal restrictions on use or disclosure of customer information.²⁸⁰

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, *Suit Challenges State's Restraint of the Internet*, WALL ST. J., Sept. 25, 1996, at B1.

270. See 1995 Ga. Laws 1550 § 1 (1996).

271. See *id.*

272. See *id.* (classifying violation of provision as misdemeanor). Section 17-10-3 of the Georgia Code defines punishment for misdemeanors. See GA. CODE ANN. § 17-10-3 (Harrison 1990 & Supp. 1996).

273. See Sandberg, *supra* note 269, at B1.

274. See *id.*

275. See *United States v. Miller*, 425 U.S. 435, 441-42 (1976). But see *McDonough v. Widnall*, 891 F. Supp. 1439, 1437 (D. Col. 1995) (noting that Congress passed Right to Financial Privacy Act to provide some protection against unrestricted access to financial records and fill void left by *Miller*).

276. 12 U.S.C. §§ 3401-3422 (1994).

277. See *id.* § 3402.

278. 15 U.S.C. §§ 1693-1700 (1994).

279. 12 C.F.R. pt. 205 (1996).

280. See Jacqueline S. Akins, *Selected Statutes and Regulations Affecting Day to Day Bank Operations*, 48 CONSUMER FIN. L.Q. REP. 368, 373-74 (1995) (discussing protections and

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

limitations of Regulation E).

281. See *Feist Publications, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 349 (1991).

282. See Howard Fogt & Lisa Ann Smith, *An American View on the EU Database Directive*, 46 *MANAGING INTELL. PROP.* 33, 33-37 (1995) (summarizing provisions of EU's Database Directive).

283. H.R. 3531, 104th Cong. (1996).

284. See 142 CONG. REC. E890 (daily ed. May 23, 1996) (statement of Rep. Moorhead).

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.

287. See 15 U.S.C. §§ 1051-1072, 1091-1096, 1111-1127 (1994).

288. See Carol Levin & Don Willmott, *Is It Mine Online? International Panel Irons out Internet Policy*, PC MAG., 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.

289. See Council Directive 96/9/CE, 1996 J.O. (L77) 20.

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 Bill²⁹⁰ would regulate the use and dissemination of "personally identifiable information on consumers of computer information services."²⁹¹

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.²⁹² LEXIS-NEXIS, a respected provider of law and news databases, was caught off guard by the unprecedented groundswell of reaction.²⁹³ 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.²⁹⁴ 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.²⁹⁵

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-

290. See H.F. 2816, 79th Leg. Reg. Sess. (Minn. 1996).

291. *Id.*

292. See Tom Abate, *Rumormongers Spread Half Truths*, ARIZ. REPUBLIC/PHOENIX GAZETTE, Oct. 28, 1996, at E1 (detailing development of rumor regarding LEXIS-NEXIS and its database P-TRAK and noting "[e]xperts say the Lexis-Nexis episode is a case study in why the Internet is such a wonderful medium for spreading rumors"); Elizabeth Corcoran & John Schwartz, *On-Line Databases Draw Privacy Protests; Unfounded Lexis-Nexis Report Reflects Worry About Growing Files*, WASH. POST, Sept. 20, 1996, at A1 (reporting that LEXIS-NEXIS recently was bombarded with calls from consumers who were worried that personal consumer information was being sold by LEXIS-NEXIS without consumers' permission); Bruce Haring, *Internet Users Say Data Firm Violates Privacy*, USA TODAY, Sept. 20, 1996, at 3A (reporting on public's anger regarding firm's selling personal information without consent); Amy Harmon, *Public Outrage Hits Firm Selling Personal Data*, L.A. TIMES, Sept. 19, 1996, at A1 (describing rumor as "rapidly spreading—and apparently partially inaccurate—e-mail message").

293. See Corcoran & Schwartz, *supra* note 292, at A1 (stating that LEXIS-NEXIS was "bombarded with telephone calls" from consumers expressing their extreme displeasure that LEXIS-NEXIS was providing personal and confidential information on-line).

294. See Thomas E. Weber, *New Lexis Database of Names Sparks Outcry on Privacy: Episode Reflects the Power of Postings on the Internet to Spread the Confusion*, WALL ST. J., Sept. 19, 1996, at B7 (noting that LEXIS-NEXIS "permits individuals to request that they be removed from P-TRAK").

295. See Harmon, *supra* note 292, at A1 ("Lexis-Nexis spokesmen said in a statement that the information in question is 'readily available from public information sources such as telephone directories . . . and public records maintained by government agencies.'").

NEXIS.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.²⁹⁷ Specifically, the FTC recommended that the Fair Credit Reporting Act²⁹⁸ 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.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.³⁰⁰ The senators asked the FTC to provide a report within six months and to include recommendations for any new laws.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."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 Act³⁰³ prohibits a third party from intercepting or disclosing electronic communications.³⁰⁴ It also prohibits unlawful access to, and disclosure of, stored electron-

296. See Thomas E. Weber, *FTC Seeks New Consumer Protections in Wake of Flap over Lexis Database*, WALL ST. J., Sept. 24, 1996, at B7.

297. See *id.* (quoting letter written by FTC to Senate Subcommittee).

298. 15 U.S.C. §§ 1681-1681t (1994).

299. See Weber, *supra* note 296, at B7 (providing letter written by FTC to Senate Subcommittee).

300. See Lisa Fickenscher, *FTC: Self Regulate on Data Privacy or Deal with a Stirred-Up Congress*, AM. BANKER, Oct. 11, 1996, at 1 (stating that FTC Commissioner Varney received urgent request from three senators to investigate alleged privacy rights violations).

301. See Fickenscher, *supra* note 300, at 1 (noting that Congress has requested that FTC submit study in six months on "the collection, use, and public disclosure of identifying information by companies not covered by the Fair Credit Reporting Act").

302. *Id.*

303. 18 U.S.C. §§ 2510-2511 (1994).

304. See *id.* § 2511.

ic communications, including both voice and e-mail.³⁰⁵ Exceptions are available when there has been "prior consent"³⁰⁶ or when the access and disclosure is for "business use."³⁰⁷ Most states additionally have adopted wiretapping statutes that address unauthorized access to, and interception of, electronic communications.³⁰⁸ Laws and court interpretations vary widely among the states.³⁰⁹

In the case of *Smyth v. Pillsbury Co.*,³¹⁰ 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.³¹¹

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 1996³¹² 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;³¹³ broadcast services;³¹⁴ cable services;³¹⁵ regulatory re-

305. See *id.* § 2510(17).

306. See *id.* § 2511(2)(d).

307. See *id.* § 2511(2)(a).

308. See, e.g., CAL. PENAL CODE § 631 (West 1988 & Supp. 1997); MD. CODE ANN., CTS. & JUD. PROC. § 10-402 (1995 & Supp. 1996); MASS. ANN. LAWS ch. 272, § 99 (Law. Co-op. 1992 & Supp. 1996); MINN. STAT. ANN. § 626A (West 1983 & Supp. 1997); N.C. GEN. STAT. § 15A-287 (Supp. 1996); N.D. CENT. CODE § 12.1-15-02 (1985 & Supp. 1995).

309. See Annotation, *Validity, Construction, and Effect of State Legislation Making Wiretapping a Criminal Offense*, 74 A.L.R.2d 855, 855-60 (1960) (discussing rulings made in state prosecutions under wiretapping statutes).

310. 914 F. Supp. 97 (E.D. Pa. 1996).

311. See *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996).

312. Pub. L. No. 104-104, 1996 U.S.C.C.A.N. (110 Stat.) 56.

313. See Telecommunications Act of 1996, Pub. L. No. 104-104, tit. I, 1996 U.S.C.C.A.N. (110 Stat.) 56, 61-86 (to be codified at scattered sections of 47 U.S.C.).

314. See *id.* tit. II, 1996 U.S.C.C.A.N. (110 Stat.) at 107-14.

315. See *id.* tit. III, 1996 U.S.C.C.A.N. (110 Stat.) at 114-28.

form,³¹⁶ and obscenity and violence.³¹⁷ The Act directs the FCC to write more than eighty implementation rules in these areas.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 1997.³¹⁹ 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;³²⁰ (2) that access to advanced telecommunications and information services should be provided in all regions of the nation;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;³²² (4) that all providers of telecommunications services should make an equitable and nondiscriminatory contribution to the preservation and advancement of universal service;³²³ (5) that specific and predictable federal and state support mechanisms should be established to preserve and advance universal service;³²⁴ and (6) that access to advanced telecommunications services should be provided for schools, health care facilities, and libraries.³²⁵

Of particular interest to the Internet community are the provisions of Title V, known as the Communications Decency Act of 1996

316. *See id.* tit. IV, 1996 U.S.C.C.A.N. (110 Stat.) at 128-32.

317. *See id.* tit. V, 1996 U.S.C.C.A.N. (110 Stat.) at 133-43.

318. *See id.* § 101(a), 1996 U.S.C.C.A.N. (110 Stat.) 56.

319. *See id.*, 1996 U.S.C.C.A.N. (110 Stat.) at 71 (to be codified at 47 U.S.C. § 254(a)(1)).

320. *See id.*, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at 47 U.S.C. § 254(b)(1)).

321. *See id.*, 1996 U.S.C.C.A.N. (110 Stat.) at 72 (to be codified at 47 U.S.C. § 254(b)(2)).

322. *See id.*, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at 47 U.S.C. § 254(b)(3)).

323. *See id.*, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at 47 U.S.C. § 254(b)(4)).

324. *See id.*, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at 47 U.S.C. § 254(b)(5)).

325. *See id.*, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at 47 U.S.C. § 254(b)(6)).

("CDA").³²⁶ It criminalizes the sending of "obscene, lewd, lascivious, filthy, or indecent" communications through the Internet.³²⁷ 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.³²⁸ 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.³²⁹ After the decision in Philadelphia, a court in New York also declared the indecency sections unconstitutional in a similar case.³³⁰ The government has appealed both decisions directly to the U.S. Supreme Court,³³¹ in accordance with procedures specified in the Act.³³² 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,³³³ and nine others have considered taking action.³³⁴ 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."³³⁵ Virginia passed a bill in 1996 making it illegal for a state employee to use state-owned computers to access sexually explicit material.³³⁶ New York's governor has signed into law a bill to reinstitute prohibitions on disseminating indecent material to a minor,³³⁷ similar to those that were struck down at the federal level in *Shea v. Reno*.³³⁸ The New York law is effective November 1,

326. See *id.* tit. V, 1996 U.S.C.C.A.N. (110 Stat.) at 133-43.

327. *Id.* § 502(1), 1996 U.S.C.C.A.N. (110 Stat.) at 133 (to be codified at 47 U.S.C. 223(a)(1)(A)).

328. See *American Civil Liberties Union v. Reno*, 929 F. Supp. 824, 826-27 (E.D. Pa. 1996).

329. See *id.* at 849.

330. See *Shea ex rel. American Reporter v. Reno*, 930 F. Supp. 916, 942 (S.D.N.Y. 1996).

331. See *Shea ex rel. American Reporter v. Reno*, 930 F. Supp. 916 (S.D.N.Y. 1996), *petition for cert. filed*, 65 U.S.L.W. 3323 (U.S. Oct. 15, 1996) (No. 96-595); *American Civil Liberties Union v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996), *prob. juris. noted*, 65 U.S.L.W. 3414, No. 96-511 (Dec. 6, 1996).

332. See *Telecommunications Act of 1996*, Pub. L. No. 104-104, § 561(b), 1996 U.S.C.C.A.N. (110 Stat.) 56, 143 (to be codified at 47 U.S.C. § 223 note) (establishing right for direct appeal of federal district court final judgment to Supreme Court).

333. See Jared Sandberg, *Suit Challenges State's Restraint of the Internet*, WALL ST. J., Sept. 25, 1996, at B1.

334. See *id.*

335. See CONN. GEN. STAT. ANN. § 53a-183 (West 1994 & Supp. 1996).

336. See N.Y. PENAL LAW § 235.21 (McKinney 1989 & Supp. 1997).

337. See *id.*

338. See 930 F. Supp. 916, 942 (S.D.N.Y. 1996).

1996.³³⁹ 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.*,³⁴⁰ that an Internet service provider could be held liable for defamatory messages posted by users of its on-line service.³⁴¹ 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.³⁴² The court maintained that because Prodigy exercised editorial control over posted messages, it was a publisher rather than a mere distributor.³⁴³

The lawsuit itself eventually was dropped when Prodigy issued an apology to Stratton Oakmont;³⁴⁴ 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.³⁴⁵ 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.³⁴⁶

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

339. See N.Y. PENAL LAW § 235.21.

340. 23 Media L. Rep. (BNA) 1794 (N.Y. Sup. Ct. 1995).

341. See *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 23 Media L. Rep. (BNA) 1794, 1798 (N.Y. Sup. Ct. 1995).

342. See *id.*; see also *Cianci v. New Times Pub. Co.*, 639 F.2d 54, 61 (2d Cir. 1980) (holding publishers liable for reprinting libelous statements). But see *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 140 (S.D.N.Y. 1991) (comparing Internet provider CompuServe to bookstore and deciding that CompuServe has no editorial control over its content).

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).

344. See *Hiawatha Bray, Prodigy Loses Appeal in Libel Case; Ruling Finding Firm Liable for Material is Upheld*, B. GLOBE, Dec. 14, 1995, at 51 (discussing Prodigy's apology and subsequent failure to have New York court withdraw opinion).

345. See John Byczkowski, *Libel Decision Asks Too Much of On-Lines*, CINCINNATI ENQUIRER, June 6, 1995, at B7 (expressing concern that decision will censor Internet users); Elizabeth Corcoran, *\$200 Million Libel Suit Against Prodigy Dropped; On-Line Industry Had Worried About Case*, WASH. POST, Oct. 25, 1995, at F2 (discussing effect of court ruling and apology of on-line companies).

346. See Telecommunications Act of 1996, Pub. L. No. 104-104, § 502(2), 1996 U.S.C.A.N. (110 Stat.) 56, 134 (to be codified at 42 U.S.C. § 223(e) (exempting from liability violations of decency laws persons who solely provide access to "facility, system, or network not under that person's control").

confidentiality of proprietary information relating to other telecommunications carriers, equipment manufacturers, and customers.³⁴⁷

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.³⁴⁸ As a result, cities in Texas and Colorado reportedly are considering special on-line taxes.³⁴⁹

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.³⁵⁰ 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.³⁵¹

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.³⁵² It similarly notified customers in Pennsylvania, Illinois, and a number of other states.³⁵³ 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

347. See *id.* § 702, 1996 U.S.C.C.A.N. (110 Stat.) at 148-49 (to be codified at 42 U.S.C. § 222).

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).

349. See *Cities, States See Internet as Source of Tax Revenue*, HOUS. CHRON., Aug. 25, 1996, at 8 (surveying city and state on-line tax initiatives); Thomas E. Weber, *Taxing Net Commerce; Devil Is in the Details*, WALL ST. J., Nov. 21, 1996, at B10 (discussing local Internet taxation).

350. See Alisa LaPoit, *Internet Services May Face State Tax*, NASHVILLE BANNER, Jan. 3, 1997, at A1 (discussing legislators' struggle to determine which on-line communications are taxable); Paula Wade, *Expansion of Net Service Raises Taxing Questions*, COM. APPEAL, Jan. 23, 1997, at A11 (addressing Internet service providers' concerns over new Internet taxes).

351. See Editorial, *Tacoma's Failed Foray into Cyberspace Taxation*, SEATTLE TIMES, Sept. 7, 1996, at A9 (reporting Tacoma City Council's decision to lift much-criticized Internet tax).

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.³⁵⁴ Those who have not been paying, he said, could face audits, penalties, and demands for back taxes from up to seven years ago.³⁵⁵ Some service providers have argued that this would be unfair.³⁵⁶ 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.³⁵⁷

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.³⁵⁸ 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.³⁵⁹

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).

355. See MASS. REGS. CODE tit. 830, § 64H.1.6 (1996) (listing effective date of tax as Sept. 1, 1990).

356. See Hiawatha Bray, *Groups Urge Weld to Block Levy on Internet Services; Say On-Line Firms Already Taxed Using Phone Lines*, B. GLOBE, Oct. 15, 1996, at D2 (reiterating arguments of on-line services against Internet tax).

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 349, 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 on-line taxes in nation of "50 states and myriad counties").

358. See Ralph Vartabedian, *IRS Pulls Plug on Its Electronic Tax-Filing System*, L.A. TIMES, Sept. 11, 1996, at D1 (citing "undisciplined contracting" and "lack of technical expertise" as reasons for Cyberfile failure).

359. See *Filing Choices*, I.R.S. News Release, Jan. 1997, available in WESTLAW, FTX-NR Database.

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.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.³⁶¹ Spring Street subsequently said it planned to establish an on-line stock exchange.³⁶²

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

The SEC has indicated further, through a series of releases, that it is comfortable with expanding permissible securities activities to the Internet.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 1996³⁶⁶ requires federal agencies to convert from checks to EFTs in two phases.³⁶⁷ The

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").

361. See Interpretation Regarding Use of Electronic Media by Commodity Pool Operators and Commodity Trading Advisors, 61 Fed. Reg. 42,146, 42,148 (1996) (to be codified at 17 C.F.R. pt. 4) (describing preliminary requirements).

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

363. See Real Goods Trading Corp., SEC No-Action Letter, June 24, 1996, available in LEXIS, FEDSEC Library, NOACT File, 566, at *3 (allowing Real Goods to operate bulletin board on Internet that posts notices of purchases and sales of its stock).

364. See *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).

365. See Use of Electronic Media for Delivery Purposes, Securities Act Release No. 33-7233, 60 Fed. Reg. 53,458 (1995) (stating that SEC does not "disfavor" use of Internet for dissemination of information); Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisors for Delivery of Information, Advisers Act Release No. 33-7288, 61 Fed. Reg. 24,644 (1996) (to be codified at 17 C.F.R. pts. 231, 241, 271, 276) (expressing approval of use of electronic media, but urging users to follow regulations).

366. Pub. L. No. 104-134, 1996 U.S.C.A.N. (110 Stat.) 1321 (1996).

367. See Debt Collection Improvement Act of 1996, Pub. L. No. 104-134, § 31001, 1996 U.S.C.A.N. (110 Stat.) 1321 (to be codified at 31 U.S.C. § 3332) (requiring newly eligible recipients of federal payments to receive payments electronically as phase one and requiring

Financial Management Service of the U.S. Treasury has implemented these requirements.³⁶⁸ 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.³⁶⁹

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.³⁷⁰ These regulations "incorporate recent and significant changes in commercial law addressing the holdings of securities in book-entry form through financial intermediaries."³⁷¹

A question remains as to how electronic benefits transfer ("EBT") payments that utilize SVCs will be governed under the Federal Reserve's Reg E.³⁷²

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.³⁷³ Congress did not pass the so-called Fair ATM Fees for Consumers Act,³⁷⁴ 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).

368. See Management of Federal Agency Disbursements, 61 Fed. Reg. 39,254, 39,254 (1996) (to be codified at 31 C.F.R. pt. 208) (indicating that Financial Management Services implemented requirements are effective upon publication in Federal Register on July 26, 1996).

369. See *id.*; Debt Collection Improvement Act of 1996 § 31001, 1996 U.S.C.A.N. (110 Stat.).

370. See Regulations Governing Book-Entry Treasury Bonds, Notes and Bills, 61 Fed. Reg. 43,626, 43,626 (1996) (to be codified at 31 C.F.R. pt. 357) (finalizing and interpreting TRADES regulations).

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.

373. See 142 CONG. REC. S7784 (daily ed. July 11, 1996).

374. S. 1800, 104th Cong. § 2 (1996).

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

375. See *Transactive Corp. v. United States*, 91 F.3d 232, 241 (D.C. Cir. 1996).

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 Hoyer, *Spamming the Globe*, ARIZ. REPUBLIC, Dec. 30, 1996, at E1 (expressing frustration at plethora of junk e-mail and commercial advertising on Internet).

378. See Kim Girard, *Browser Interface Sets Atlanta Bank Apart*, COMPUTERWORLD, Nov. 4, 1996, at 67R (providing overview of banks that advertise on the Internet).

379. See 12 C.F.R. pt. 328 (1996) (imposing regulations on banks' ability to advertise).

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).

382. See Laura Fowlie, *Not a Vehicle for Unsolicited Sales Pitches*, FIN. POST, Oct. 26, 1996, at C12 (noting Internet users' disgust of "spam" and reviewing on-line industry's solutions).

383. See *id.* (discussing various ways in which spammers obtain e-mail address lists).

and vilified by other users, yet increased their spamming activities.³⁸⁴ Current spammers, such as Sanford Wallace of Philadelphia and his company, Cyber Promotions, Inc., aggressively have sought to protect their activities in court.³⁸⁵ 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.³⁸⁶

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.³⁸⁷ As a result, undeliverable return messages were flooding Concentric's system, preventing adequate service to its real customers.³⁸⁸ 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.³⁸⁹

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.³⁹⁰

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

384. See Yarden Arar, *Spotlighting the Computer World "Most Hated" Couple Beefs Up On-line "Spamming,"* L.A. DAILY NEWS, Nov. 28, 1994, at L5 (describing couple's efforts to advertise legal services on Internet despite threats of lawsuits).

385. See *Cyber Promotions, Inc. v. America Online, Inc.*, 24 Media L. Rep. (BNA) 2505 (E.D. Pa. 1996), request for reconsideration denied by No. 96-2486, 1996 WL 741974, at *10 (E.D. Pa. Dec. 20, 1996); see also Natalie Hopkinson, *E-debris Unwanted Advertisements Are Junking up Computers and It Won't Go Away*, FT. WORTH STAR-TELEGRAM, Jan. 4, 1997, at 5 (reporting mass e-mailing company official's defense of mass, yet responsible, e-mail).

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.*

390. See *Cyber Promotions*, 24 Media L. Rep. at 2505.

for deceptive advertising.³⁹¹ 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.³⁹² 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.³⁹³

Banking regulators also traditionally have reviewed bank advertisements with scrutiny. A number of banking regulations, such as Truth in Lending ("Regulation Z")³⁹⁴ and Truth in Savings ("Regulation DD")³⁹⁵ contain detailed interest rate disclosure requirements.³⁹⁶ 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.³⁹⁷

Many states have statutes prohibiting the use of an individual's likeness or name for commercial purposes without the person's written consent.³⁹⁸ Failure to obtain written consent (even of one's

391. See *FTC Tackles Fraud on the Information Superhighway, Charges Nine On-Line Scammers* (Mar. 14, 1996) <<http://www.ftc.gov/opa/9603/netsc.htm>> (on file with *The American University Law Review*).

392. See *In re Zygon Int'l, Inc.*, No. 942-3171 (Fed. Trade Comm'n Mar. 5, 1996), available in WESTLAW, FATR-FTC Database; *In re Larson*, No. 962-3016 (Fed. Trade Comm'n Mar. 1, 1996) available in WESTLAW, FATR-FTC Database; *In re Rahim*, No. 952-3441 (Fed. Trade Comm'n Feb. 29, 1996), available in WESTLAW, FATR-FTC Database; *In re Serviss*, No. 952-3436 (Fed. Trade Comm'n Feb. 28, 1996), available in WESTLAW, FATR-FTC Database; *In re Clark*, No. 962-3027 (Fed. Trade Comm'n Feb. 14, 1996), available in WESTLAW, FATR-FTC Database; *In re Smith*, No. 952-3436 (Fed. Trade Comm'n Feb. 9, 1996), available in WESTLAW, FATR-FTC Database; *In re Bean*, No. 952-3429 (Fed. Trade Comm'n Feb. 8, 1996), available in WESTLAW, FATR-FTC Database; *In re Coryat*, No. 962-3019 (Fed. Trade Comm'n Feb. 7, 1996), available in WESTLAW, FATR-FTC Database; *In re Albertson*, No. 952-3437 (Fed. Trade Comm'n Feb. 5, 1996), available in WESTLAW, FATR-FTC Database.

393. See *Virgin Atlantic Fined for Violations in Ads on Internet*, N.Y. TIMES, Nov. 22, 1995, at D3.

394. 12 C.F.R. pt. 226 (1996).

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 II.J (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).

own employees) makes such use a criminal violation in some states.³⁹⁹

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.*

402. See McFadden-Pepper Act, ch. 191, 44 Stat. 1224, 1224-34 (1927) (codified at scattered sections of 12 U.S.C.).

403. See *United States v. Thomas*, 74 F.3d 701, 705-06 (6th Cir.), *cert. denied*, 117 S. Ct. 74 (1996).

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,⁴⁰⁶ on October 7, 1996, the U.S. Supreme Court refused, without comment, to hear an appeal of the conviction.⁴⁰⁷

Similar cases are being heard in other states, with widely varying results. In *Maritz, Inc. v. CyberGold, Inc.*,⁴⁰⁸ 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.⁴⁰⁹ On the other hand, in *McDonough v. Fallon McElligott, Inc.*⁴¹⁰ and in *Bensusan Restaurant Corp. v. King*,⁴¹¹ intellectual property actions were dismissed under similar circumstances for lack of personal jurisdiction.⁴¹²

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 procedure⁴¹³ under the Bank Secrecy Act.⁴¹⁴

The White House issued an Executive Order on July 15, 1996, establishing a high-level President's Commission on Critical Infrastruc-

guideline in determining obscenity is "whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest" (quoting *Kois v. Wisconsin*, 408 U.S. 229, 230 (1972))).

406. See *Computer Porn Nets Prison Terms*, WASH. POST, Dec. 3, 1994, at C3 (noting defense contention that prosecutors had selected conservative venue in order to increase chance of conviction).

407. See *Thomas v. United States*, 117 S. Ct. 74 (1996).

408. 40 U.S.P.Q.2d (BNA) 1729 (E.D. Mo. 1996).

409. See *Maritz, Inc. v. CyberGold, Inc.*, 40 U.S.P.Q.2d (BNA) 1729, 1731, 1733-35 (E.D. Mo. 1996).

410. 40 U.S.P.Q.2d (BNA) 1826 (S.D. Cal. 1996).

411. 937 F. Supp. 295 (S.D.N.Y. 1996).

412. See *Bensusan Restaurant Corp. v. King*, 937 F. Supp. 295, 299-300 (S.D.N.Y. 1996) (concluding that New York's long-arm statute does not confer personal jurisdiction over Missouri defendant who operates Web site that is accessible in New York); *McDonough v. Fallon McElligott, Inc.*, 40 U.S.P.Q.2d (BNA) 1826, 1828 (S.D. Cal. 1996) (noting that creation of Web site used by Californians alone cannot establish California personal jurisdiction).

413. See 31 C.F.R. §§ 103.11(ii), .11(qq), .21 (1996) (streamlining reporting procedure through creation of uniform Suspicious Activities Report form).

414. 12 U.S.C. §§ 1829b, 1951-1959; 31 U.S.C. §§ 5311-5330.

ture Protection.⁴¹⁵ Critical infrastructures to be assessed include banking and finance.⁴¹⁶ 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."⁴¹⁷

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.⁴¹⁸ The result will be less powerful governments in relation to criminal organizations such as the Mafia and international drug cartels.⁴¹⁹ In addition, computer hackers will pose a more significant threat.⁴²⁰ 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.⁴²¹

L. Evidentiary Issues and Dispute Resolution

Although some considerations regarding computer evidence have been discussed previously in this Article,⁴²² one unique development in this area is the creation of on-line forms of dispute resolution. On-line 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.⁴²³ Another pilot project, funded by a grant from the National Center for Automated Information Research, was established at the University of Massachusetts.⁴²⁴ Called the Online Ombuds Office, the project is aimed at using on-line tools to resolve disputes

415. See Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (1996). The composition of the commission was changed subsequently by Exec. Order No. 13,025, 61 Fed. Reg. 58,623 (1996).

416. See Exec. Order No. 13,010, 61 Fed. Reg. at 37,347.

417. *Id.* at 37,348.

418. See Rory J. O'Connor, *Presidential Panel Warns of Cyberattack Threat: Critics Charge Danger Overstated Could Lead to Unwarranted Intrusion on Net*, MERCURY NEWS WASH. BUREAU, Jan. 31, 1997, available in <<http://www1.sjmercury.com/news/nation/threat0130.htm>>.

419. See *id.*

420. See *id.*

421. See *id.*

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

423. See *The Virtual Magistrate* (visited Jan. 30, 1997) <<http://vmag.law.vill.edu:8080>> (on file with *The American University Law Review*).

424. See *The Online Ombuds Office, Related Projects* (visited Jan. 30, 1997) <<http://www.ombuds.org/affil.html>> (on file with *The American University Law Review*).

arising out of both on-line and non-on-line activities.⁴²⁵ The project is targeted particularly to disputes involving copyrights, domain names, First Amendment, on-line service providers, and harassment.⁴²⁶

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.⁴²⁷ States have enacted detailed escheatment schedules and procedures for all types of property held by financial institutions.⁴²⁸ 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.⁴²⁹

No state has passed any rule on escheatment of unused value on a SVC yet, although New York has begun to study the issues.⁴³⁰ Commentators have recommended that stored value be escheatable only when it is redeemable for cash.⁴³¹ 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.⁴³² The problem of an issuer avoiding escheatment obligations by contractually limiting redemption options has been identified, but remains unresolved.⁴³³

N. Antitrust

Antitrust law sometimes is thought of as a counterweight to intellectual property protection. It is intended to promote competi-

425. See The Online Ombuds Office, *Online Ombuds FAQ* (visited Jan. 30, 1997) <<http://www.ombuds.org/faq.html>> (on file with *The American University Law Review*) (stating that office is "primarily interested in disputes arising out of some online activity").

426. See The Online Ombuds Office (last modified Aug. 21, 1996) <<http://www.ombuds.org/database.html>> (on file with *The American University Law Review*).

427. See CAL. CIV. PROC. CODE §§ 1500-1582 (West 1982 & Supp. 1997) (providing for uniform disposition of unclaimed property); GA. CODE ANN. §§ 44-12-190 to -235 (1982 & Supp. 1996) (setting forth procedures and standards for state's assumption of abandoned property); N.Y. ABAND. PROP. LAW §§ 101-1420 (McKinney 1991 & Supp. 1997) (governing escheat of property to state).

428. See CAL. CIV. PROC. CODE §§ 1513, 1513.5; GA. CODE ANN. §§ 44-12-196 to -197; N.Y. ABAND. PROP. LAW §§ 300-306.

429. See, e.g., CAL. CIV. PROC. CODE §§ 1511-1516; GA. CODE ANN. §§ 44-12-195 to -198, -201, -209; N.Y. ABAND. PROP. LAW § 300.

430. See Richard L. Field, *Forgotten But Not Gone: Escheatment of Stored Value Cards*, ELECTRONIC BANKING L. & COM. REP., June 1996, at 11.

431. See *id.* at 12.

432. See *id.*

433. See *id.* at 13.

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.⁴³⁴ In addition to the general antitrust laws, specific anti-tying laws apply directly to banks.⁴³⁵ Netscape openly has encouraged the Justice Department to investigate Microsoft for antitrust violations.⁴³⁶

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.⁴³⁷

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.⁴³⁸ The proposals would amend Federal Reserve Regulation Y.⁴³⁹ 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).

435. See 12 U.S.C. §§ 1971-1978 (1994).

436. See *Netscape Letter to Justice Department Accuses Microsoft of Antitrust Violations*, BNA ANTITRUST & TRADE REG. DAILY, Aug. 23, 1996, available in WESTLAW, BNA-ATD Database.

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 23, 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).

438. See Alan Yonan Jr., *Greenspan Applauds Effort*, CAP. MKT. REP., Aug. 23, 1996, available in WESTLAW, FINNEWS Database.

439. 12 C.F.R. pt. 225 (1996) (regulating bank holding companies and changes in control).

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

440. See Bank Holding Companies and Change in Bank Control (Regulation Y), 61 Fed. Reg. 47,242, 47,276 (1996) (to be codified at 12 C.F.R. § 225.28(b)(14)) (proposed Sept. 6, 1996).

441. See Statement on Signing the Omnibus Consolidated Appropriations Act, 1997, 32 WEEKLY COMP. PRES. DOC. 1935 (Sept. 30, 1996).

442. See H.R. 3540, 104th Cong. (1996); H.R. 3662, 104th Cong. (1996); H.R. 3755, 104th Cong. (1996); H.R. 3756, 104th Cong. (1996); H.R. 3814, 104th Cong. (1996); H.R. 4278, 104th Cong. (1996).

443. See Omnibus Consolidated Appropriations Act, 1997, Pub. L. No. 104-208, div. A, tit. II, § 2001(a), 1996 U.S.C.C.A.N. (110 Stat.) 3009 (1996) (to be codified in scattered sections of 12, 15, 26, 31, and 42 U.S.C.).

444. See *id.* §§ 2401-2422, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at 15 U.S.C. §§ 1681a-1681e, 1681g-1681j, 1681m-1681o, 1681q-1681s) (amending Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994)).

445. See *id.* §§ 2501-05, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at 42 U.S.C. §§ 6991b(h), 9601(20), 9607).

446. See *id.* § 2603, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at 18 U.S.C. §§ 474, 474A, 514).

447. See *id.* § 2608, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at 12 U.S.C. § 1811 note) (modifying content of Federal Reserve Board's required annual report to Congress so as to include trends in fees charged and pricing and availability of services on state-by-state and metropolitan area basis).

448. See *id.* §§ 2201-2244, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at scattered sections of 12 U.S.C.).

449. See *id.* § 2612, 1996 U.S.C.C.A.N. (110 Stat.) (to be codified at 12 U.S.C. § 1843(c)(8)).

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.

APPENDIX

Committee to Study National Cryptography Policy
National Research Council
CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY
May 30, 1996, Prepublication Copy

Recommendations

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.