UIC John Marshall Journal of Information Technology & Privacy Law

Volume 17
Issue 3 *Journal of Computer & Information Law - Spring 1999*

Article 12

Spring 1999

The Law of Electronic Commerce and Digital Signatures: An Annotated Bibliography, 17 J. Marshall J. Computer & Info. L. 1043 (1999)

John R. Austin

THE LAW OF ELECTRONIC COMMERCE AND DIGITAL SIGNATURES: AN ANNOTATED BIBLIOGRAPHY

by JOHN R. AUSTIN†

This bibliography consists of annotated references to periodical articles, books and book chapters, World Wide Web sites, and government documents that examine the law of electronic commerce and digital signatures. It does not include newspaper articles or books that are no longer in print. To facilitate access, the materials are grouped under the following subject headings:

I. ELECTRONIC COMMERCE (IN GENERAL): Materials cited offer a comprehensive overview of the subject or cover many subcategories.

II. DIGITAL SIGNATURES, CERTIFICATION AUTHORITIES, INFRASTRUCTURE MODELS, AND AUTHENTICATION TECHNIQUES: Some of the materials grouped under this category discuss digital or electronic signatures, often with an accompanying discussion of the law of signatures. Some discuss authentication issues in electronic commerce and the role that certification authorities or other trusted third parties might play. Others examine public key/private key infrastructure or other infrastructure models for electronic commerce. Often all of these subjects are discussed in a single piece.

III. UNIFORM COMMERCIAL CODE/STATUTE OF FRAUDS AND EVIDENTIARY ISSUES: Materials cited discuss applicability of the Statute of Frauds signed writing requirements to electronic contracts, problems of proof that arise in litigation, or the need for revisions to the Uniform Commercial Code to encompass electronic commerce.

IV. ENCRYPTION/CRYPTOGRAPHY AND SECURITY ISSUES: Cited materials describe cryptosystems used in electronic commerce, privacy and export control issues relating to such systems, and computer security concerns as they relate to commercial activity on computer networks.

† Director of the Law Library & Associate Professor, Northern Illinois University, College of Law, DeKalb, IL 60115-2890.

V. FOREIGN AND INTERNATIONAL ASPECTS: Materials in this category discuss the law of electronic commerce and digital signatures in foreign countries or international initiatives in this area.

I. ELECTRONIC COMMERCE (IN GENERAL)

Digital Signature Resource Center (visited Dec. 13, 1998) <http://www.ilpf.org/digsig/digsig2.htm>. This comprehensive site, maintained by the Internet Law and Policy Forum, includes the text of state, federal, international and model digital signature legislation, American and international documents relating to policy development, background information, and links to resources for electronic commerce, encryption/cryptography, and certificate authorities. For a description of the Internet Law and Policy Forum, visit its home page <http://www.ilpf.org/>.

The Law of Electronic Commerce, in DOING BUSINESS ON THE INTERNET (PLI Patents, Copyrights, Trademarks, & Literary Property Course Handbook Series No. G-452, 1996) (PLI Patents, Copyrights, Trademarks, & Literary Property Course Handbook Series No. G-491, 1997). Each of these Practicing Law Institute handbooks contains numerous short practice-oriented articles on all aspects of electronic commerce.

Electronic Commerce and Interoperability in the National Information Infrastructure: Hearing Before the Subcomm. On Technology, Environment, and Aviation of the House Comm. On Science, Space, and Technology, 103d Cong. (1994).(Available in Congressional Information Service microfiche, CIS 94-H701-77. Superintendent of Documents No. Y4.SCI2:103/134) (161 p.). Witnesses testify regarding the implications of electronic commercial activity for the National Information Infrastructure, the economy, and society.

Electronic Data Interchange: Key to Small Business Competitiveness: Joint Hearing Before the Subcomm. On Exports, Tax Policy, and Special Problems and the Subcomm. On Environment and Labor of the House Comm. On Small Business, 101st Cong. (1990). 344 p. (Available in Congressional Information Service microfiche, CIS 91-H721-19. Superintendent of Documents No. Y4.Sm1:101-28) (344 p.). Witnesses discuss the effects of electronic data interchange on the productivity of small and medium-sized businesses.

WARWICK FORD & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE: BUILDING THE INFRASTRUCTURE FOR DIGITAL SIGNATURES AND ENCRYPTION (1997) (Prentice-Hall, 470 p.). Mr. Ford, an engineer, and Mr. Baum, a lawyer, have written a book for lawyers, business professionals, and technologists that can serve both as an introduction to and basic reference for the emerging law and technology of electronic commerce. Introductory chapters provide basic information on the Internet, busi-

ness and legal principles relating to electronic commerce, Internet security, and information security technologies such as cryptography and digital signatures. More advanced chapters discuss certificates, public key infrastructures, non-repudiation, and certification practices. Appendices offer reprints of the United Nations Model Law on Electronic Commerce and the Internet Domain Name Dispute Resolution Policy, information on how to obtain copies of Standards cited in the text, and technical discussions of cryptographic mechanisms, the X.509 Standard for certificate formats, and Abstract Syntax Notation One that supports X.509.

Office of Tech. Assessment, Electronic Enterprises: Looking to the Future (Comm. Print. 1994). (Available in Congressional Information Service microfiche, CIS 94-J952-26. Superintendent of Documents No. Y3.T22/2:2EL2/13) (176 p.) This report, prepared for the Senate Commerce, Science, and Transportation Committee and the House Science, Space, and Technology Committee, examines the development of electronic networks for business purposes.

Summary of Electronic Commerce and Digital Signature Legislation (last modified Dec. 10, 1998) <http://www.mbc.com/ds_sum.html>. This comprehensive site, maintained by the Chicago law firm of McBride, Baker & Coles, includes legislation analysis tables, the text of proposed or enacted state and federal statutes, federal agency regulations, American Bar Association and National Conference of Commissioners on Uniform State Laws initiatives, international documents, and foreign law.

BENJAMIN WRIGHT & JANE K. WINN, THE LAW OF ELECTRONIC COMMERCE (3d ed. 1998) (Aspen Law & Business, looseleaf, approx. 600 p.). This third edition of a well-established text covers business, technological, security, and regulatory issues. Included are chapters on evidentiary issues, recordkeeping and control requirements, electronic contract issues, and network service provider issues relating to health care information, electronic funds transfer, confidentiality, and liability for inadequate service.

Electronic Messaging Services Task Force, American Bar Ass'n, *The Commercial Use of Electronic Data Interchange—A Report and Model Trading Partner Agreement,* 45 Bus. Law. 1645 (1990).

> The Model Trading Partner Agreement, along with its section-by-section Commentary, were prepared . . . to furnish a tool for counsel whose clients are integrating electronic data interchange into their contracting procedures. The Report . . . details the commercial practices which are evolving as the use of electronic data interchange increasingly becomes common and describes the Task Force's study of those practices and the preparation of the Model Trading Partner Agreement and Commentary. In addition the Report analyzes the implications of these practices for commercial law and offers suggestions for resolving the issues in light of

> existing law, as well as an agenda for future study. It and the Model Agreement offer a format and framework for counsel and parties seeking a workable, practical approach to existing problems.

Id. at 1647. The Model Agreement, not accompanied by the Report, is also published at 4 SOFTWARE L.J. 179 (1991) under the title *Model Electronic Data Interchange Trading Partners Agreement and Commentary.*

Information Sec. Comm., American Bar Ass'n, *Tutorial*, 38 JURIMETRICS J. 243 (1998). The article presents an overview of the basic concepts which provide the legal and scientific underpinnings of electronic commerce and digital signatures law. Terminology such as public key infrastructure, cryptography, asymmetric cryptosystem, private key, hash function, public key certificate, and certification authority are fully explained in the context of how a digital signature verification system works. Some attention is also paid to the costs and benefits of such systems and the role of standards. The *Tutorial* is based on an earlier version published in the American Bar Association's *Digital Signature Guidelines* (1996) (*See infra* Section II for annotation.)

Michael S. Baum, *Legal Issues in Electronic Data Interchange*, *in* 13TH ANNUAL COMPUTER LAW INSTITUTE, at 575 (PLI Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series No. 322, 1991). Written in outline format, the author offers brief introductions to basic electronic data interchange ("EDI") principles and to the following as they relate to EDI transactions: evidentiary, contract formation, and international legal issues, trading partner agreements, and third party service provider agreements.

President William J. Clinton & Vice President Al Gore, Jr., The Framework for Global Electronic Commerce (visited Dec. 13, 1998) <http://www.whitehouse.gov/WH/New/Commerce/>. Created by an interagency task force headed by the Vice President, the *Framework* establishes principles for U.S. government involvement in the development of the Internet as a tool for electronic commerce and makes recommendations regarding interational cooperation in this area.

Philip S. Corwin, *Electronic Authentication: The Emerging Federal Role*, 38 JURIMETRICS J. 261 (1998). Mr. Corwin briefly discusses the rationales offered for federal statutory control of cybercommerce and then examines the following bills pending in the 105th Congress: H.R. 2991 (mandating that all federal agencies be able to offer the public the opportunity to do business with them electronically and eliminating federal requirements for pen-and-ink signatures); H.R. 2676 (providing for electronic filing of tax and information returns and eliminating the requirement that a paper record of the transaction be concurrently filed); H.R. 2937 (providing a framework for the recognition of digital signatures as a valid alternative to written signatures for all purposes); and S. 1594

(providing for nationwide recognition of digital signatures in banking transactions).

Robert W. McKeon, Jr., *Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena*, 12 J. MARSHALL J. COMPUTER & INFO. L. 511 (1994). The author provides a description of the basic elements of electronic data interchange ("EDI") and then offers discussions of the unique evidentiary issues it poses, focusing on questions of authenticity, the best evidence and hearsay rules, and the application of contract law principles to EDI transactions, concentrating on Statute of Frauds, parol evidence rule, and battle of the forms issues.

Raymond T. Nimmer, *Electronic Contracting: Legal Issues*, 14 J. MARSHALL J. COMPUTER & INFO. L. 211 (1996). Professor Nimmer discusses basic principles of contract law and possible ways in which they may be adapted to the unique problems posed by utilizing electronic data interchange ("EDI") technology in the creation of contracts. Included are discussions of needed Uniform Commercial Code revisions relating to offer and acceptance, timing and revocation, terms and conditions, enforceability and the Statute of Frauds. Some attention is also paid to the legality of one party's requiring the use of EDI when another party does not wish to, data ownership and confidentiality issues, the law of mistake, the liability of the providers of electronic mail processing systems, and the content of EDI trading partner agreements.

Richard L. Ravin, *Tradesecrets and Digital Signatures*, 8 SETON HALL CONST. L.J. 751 (1998). This six-page, unfootnoted article has value in that the author is able, in three paragraphs (at 755), to succinctly and clearly outline the major legal issues involved in electronic contracting and authentication of digital signatures—a nice introduction to the subject for someone unacquainted with it. (The remainder of the article is principally devoted to the relationship of registered trademarks and Internet domain names.)

Public Key Infrastructure Symposium, 38 JURIMETRICS J. 241 (1998). The symposium includes a tutorial and fifteen articles. The tutorial and articles authored by Philip S. Corwin, Daniel J. Greenwood, Juan A. Avellan V, Stephen S. Wu, Charles R. Merrill (*The Accreditation Guidelines*), Michael S. Baum & Warwick Ford, Walter A. Effross, R.R. Jueneman & R.J. Robertson, Jr., Emily Frye & Randy V. Sabett, and Juan C. Cruellas are annotated elsewhere in this bibliography. Also included are articles by Veronique Wattiez LaRose (*Brief Essay on the Notion of and Rules Relating to Incorporation by Reference in Civil Law Systems,* at 295); B. Paul Cotter & John H. Messing (*Electronic Court Filing in Pima County Small Claims Court—Technical Parameters, Adopted Solutions, and Some of the Legal Issues Involved*, at 397); Arthur Purcell *et al.* (*Electronic Patent Application Filing System (EPAFS): A Demonstration Project of the U.S. Patent and Trademark Office*, at

407); Alexander Cavalli & Jane K. Winn (*Internet Security in the electric Utility Industry*, at 459) and Andreas Mitrakas & Janjaap Bos (*The ICC ETERMS Repository to Support Public Key Infrastructure*, at 473).

John C. Yates, *Electronic Commerce and Electronic Data Interchange, in* 18TH ANNUAL INSTITUTE ON COMPUTER LAW, at 147 (PLI Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series No. G-507, 1998). Mr. Yates presents an outline of "Practical Pointers" for the use of attorneys who advise clients who contract using electronic data interchange ("EDI"). Summaries of relevant case law are included. Of particular interest are a list of Web sites relating to EDI and digital signatures (at 163) and attachments which include the text of documents such as the *White House Report: A Framework for Global Electronic Commerce* July 1, 1997, at 179, the UNCITRAL Working Group on Electronic Commerce's *Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues* Dec. 3, 1996, at 199, The A.B.A. Electronic Messaging Services Task Force's *Model Electronic Data Interchange Trading Partner Agreement and Commentary* 45 Bus. Law. 1717 (1990); *Discussion Draft of Uniform Commercial Code, Article 2B - Licenses, with Comments* at 253 (Nov. 1, 1997).

John C. Yates, *Recent Legal Issues in Electronic Commerce and Electronic Data Interchange, in* 16TH ANNUAL INSTITUTE ON COMPUTER LAW at 271 (Mar. 1996) (PLI Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series No. G-430, 1996). This article, written in outline format, has four goals:

> To review the definition of electronic data interchange (EDI) and its role as a commercial subset of electronic commerce . . . . To understand the business and financial models driving the growth of EDI and electronic commerce . . . . To examine the dynamic legal principles impacting EDI, including the model EDI Trading Partner Agreement [prepared by the A.B.A.'s Electronic Messaging Services Task Force and reproduced as an Attachment at 305] and to review future legal trends.

Id. at 277.

II. DIGITAL SIGNATURES, CERTIFICATION AUTHORITIES, INFRASTRUCTURE

MODELS AND AUTHENTICATION TECHNIQUES

Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, 1996 A.B.A. SEC. INFO SECURITY COMMITTEE. As the subtitle implies, these *Guidelines* offer a set of legal principles that can be used to define the duties and liabilities of certification authorities (persons who issue certificates used to authenticate the content and/or the identities of the parties involved in an elec-

tronic transaction) and all other parties associated with an electronic agreement. Part I offers definitions, Part II general principles, and Parts III, IV, and V principles relating to certification authorities, subscribers, and other relying parties, respectively. Also included are a fifteen-page tutorial on digital signature technology and a one-page bibliography. The *Guidelines* may be purchased from the A.B.A. or downloaded at no charge from the A.B.A. Web site <http://www.abanet.org/scitech/ec/isc/dsgfree.html>. For an overview, *see* Charles R. Merrill, *An Attorney's Roadmap to the Digital Signature Guidelines*, DOING BUSINESS ON THE INTERNET, at 379 (1996) (PLI Patents, Copyrights, Trademarks, & Literary Property Course Handbook Series No. G-452).

Michael S. Baum, *Federal Certification Authority Liability and Policy—Law and Policy of Certificate-Based Public Key and Digital Signatures* (U.S. Dept. Of Commerce/NIST Publication No. NIST-GCR-94-654; National Technical Info. Serv. Publication No. PB94-191-202, 1994). (421 p.). This report, intended as an "issues-and-think piece," comprehensively examines legal issues that relate to the role of certification authorities in electronic commerce (trusted third parties who create certificates which authenticate transactions), the legal implications of certification authorities being operated by or on behalf of the United States government, and possible paradigms for a federal certification authority infrastructure. Extensively footnoted.

Do You Know Who You Are Doing Business With? Signatures in a Digital Age: Hearing Before the Subcomm. On Technology of the House Comm. on Science, 105th Cong. (1997). (Available in Congressional Information Service microfiche, CIS 98-H701-13. Superintendent of Documents No. Y4.SCI2:105/25) (131 p.) Witnesses testify regarding the need for secure environments for electronic commerce, the role that digital signature technology could play, U.S. Department of Commerce activity in this area, and the development of standards.

Federal Role in Electronic Authentication: Hearing Before the Subcomm. on Domestic and International Monetary Policy of the House Comm. on Banking and Financial Services, 105th Cong. (1997) (Available in Congressional Information Service microfiche, CIS 98-H241-1. Superintendent of Documents No. Y4.B22/1:105-21) (174 p.) Witnesses testify regarding the need for authentication of electronic commercial documents, the role of digital signatures, and whether electronic commerce should be regulated by private industry and/or the federal or state governments.

Public Forum on Certificate Authorities and Digital Signatures: Enhancing Global Electronic Commerce, July 24, 1997 (visited Dec. 13, 1998) <http://csrc.nist.gov/ecforum/>. This site, maintained by the U.S. Department of Commerce Technology Division, includes the meeting notice, agenda, text of public comments electronically submitted, and the

presentations made at the Forum, held at the National Institute of Standards and Technology, Gaithersburg, Maryland, July 24, 1997. Topics included are developments in the states and emerging trends, the new certificate authorities industry, digital signatures and other authentication technologies, international activities, and developments in foreign countries.

World Wide Web Consortium Digital Signature Initiative (visited Dec. 13, 1998) <http://www.w3.org/DSig/>. The World Wide Web Consortium, or W3C, is an international technical group jointly hosted by the Massachusetts Institute of Technology Laboratory for Computer Science and European and Japanese higher education centers. Its Digital Signature Initiative is a project to develop international technical standards for digital signatures. This home page provides links to technical data regarding the standards.

Michael S. Baum & Warwick Ford, *Public Key Infrastructure Interoperation*, 38 JURIMETRICS J. 359 (1998). The authors discuss the problems and opportunities presented by public key infrastructure ("PKI") interoperation, in which PKIs are linked to and interact with each other. Specific issues considered include the extent to which foreign certification authorities ("CAs") may offer services to domestic customers, the legal validity of certificates issued by foreign CAs and interdomain certificate chains. Options and strategies for developing and sustaining PKI interoperation are offered.

C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Market Place*, 34 SAN DIEGO L. REV. 1225 (1997). The author contrasts open public key infrastructures ("PKIs") (systems in which subscribers obtain certificates from independent third parties certifying that subscriber's identity and then use these certificates for any business purpose whatsoever) with closed PKI models (systems in which certificates may only be used in specific contexts contractually defined by the parties). He concludes that open PKI systems, such as those prescribed by the Utah Digital Signature Act or the American Bar Association's *Digital Signature Guidelines*, are not commercially viable in that they subject issuers of certificates or subscribers to unpredictable levels of risk if certificates are fraudulently obtained and used. Because of better risk management and other benefits, he believes that closed PKI systems are a better choice for business. However, he advocates that future digital signature legislation not be drafted to favor use of closed PKI systems but be neutral and permit market factors to determine which model is preferred. For a response to this article, *see* Thomas G. Melling, *Washington's Electronic Authentication Act: Eliminating Legal Uncertainties Through Default Rules*, 34 SAN DIEGO L. REV. 1247 (1997).

Michael L. Closen & R. Jason Richards, *Notaries Public—Lost in Cyberspace, or Key Business Professionals of the Future?*, 15 J. MARSHALL J. COMPUTER & INFO. L. 703 (1997).

> This paper will focus on the problems inherent in current notarial legislation and practice. It will discuss what problems loom ahead for both notaries and cybernotaries [persons who provide the professional service of certifying and authenticating electronic transactions] as states move to implement appropriate cyberlegislation. This paper will provide a brief historical view of the relevant facets of the office of notary public, including their qualifications, statutory authority, practices, and liabilities. We will discuss cybernotarial legislation and will analyze the role of cybernotaries and identify the inadequacies of current legislation in anticipating and regulating cybernotarial acts. This paper will include our suggestions to the states as they move to enact cybernotary legislation and as they seek to avoid the pitfalls of the past, as well as the problems of the current cybernotary laws. We will conclude by considering what the future holds for both notaries public in general and cybernotaries in particular.

Id. at 716.

Karen Coyle, *Digital Signatures: Identity in Cyberspace*, AALL SPECTRUM, Dec. 1997, at 8. This three-page article provides an easy-to-read introduction to digital signatures and underlying concepts such as encryption and certification authorities. Examples of digital signatures and citations to relevant World Wide Web sites are included.

Juan C. Cruellas et al., *EDI and Digital Signatures for Business to Business Electronic Commerce*, 38 JURIMETRICS J. 497 (1998). The authors present a technical discussion of EDIFACT (Electronic Data Interchange for Administration, Commerce and Trade), a "set of internationally agreed standards, directories and guidelines for the electronic interchange of structured data." *Id.* at 499. EDIFACT is currently being considered by the International Organization for Standardization ("ISO") as a possible international standard for electronic data interchange ("EDI") and, if approved, will become ISO 9735. Much attention is paid to EDIFACTs security features and the ways in which certificates of authenticity would be provided. A detailed comparison between the certificate structures of EDIFACT and the ISO X.509 Standard is also offered.

Maureen S. Dorney, *Digital Signature Legislation, in Doing Business on the Internet: The Law of Electronic Commerce*, at 141 (PLI Patents, Copyrights, Trademarks, & Literary Property Course Handbook Series No. G-491, 1997). The author discusses the law of signatures and its relation to digital signature technology, focusing on the role of certification authorities and liability considerations. She also offers a brief overview of state and federal legislative initiatives.

Walter A. Effross, *Notes on PKI and Digital Negotiability: Would the Cybercourier Carry Luggage?*, 38 JURIMETRICS J. 385 (1998).

> Part I of the Article provides a brief summary of the operation of PKI [public key infrastructure] and its use of certification authorities. Part II summarizes the relevant elements of negotiability and the forms of negotiable instruments under Article 3 of the Uniform Commercial Code. Part III examines the application of PKI technology to support a system of digital negotiability and raises the problem of the fraudulent computerized 'cloning' of such instruments.

Id. at 386.

Gary W. Fresen, *What Lawyers Should Know About Digital Signatures*, ILL. B.J., Apr. 1997, at 170. Mr. Fresen presents a short and nontechnical introduction to digital signature law and technology. Included are explanations of basic concepts such as public key encryption, hash function, and certificate authority as well as a brief discussion of emerging regulatory approaches in the United States.

A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996). The author offers a thorough introduction to the role of certification authorities ("CAs") in electronic commerce (CAs are trusted third parties who issue certificates of authenticity relating to the parties to the transaction and/or the integrity of the electronic document.). Included are considerations of the legal regulatory framework in which CAs should operate, what sorts of certificates they might issue, and the liability which a CA might incur for issuing an inaccurate certificate.

John Gibeaut, *Sign on the Dotted Screen: ABA Takes Lead in Developing Guidelines for Electronic Document Verification*, A.B.A. J., May 1997, at 100. This short article provides a brief, nontechnical introduction to major digital signature concepts as treated in the American Bar Association's *Digital Signature Guidelines* and alludes to actions relating to digital signatures or cybernotaries that the A.B.A. and other groups have taken.

Albert Gidari & John P. Morgan, *Survey of Electronic and Digital Signature Legislative Initiatives in the United States* (visited Sept. 12, 1997) <http://www.ilpf.org/digsig/digrep.pdf>. Commissioned by the Internet Law and Policy Forum to assist its Digital Signature Working Group to draft model state legislation, this report compares and contrasts all proposed and enacted state legislation regarding any form of electronic signature. For an executive summary, visit <http://www.ilpf.org/digsig/digrep.htm>. For a 1998 supplement, visit <http://www.ilpf.org/digsig/UPDATE.HTM>. The text of most documents cited is available at the Digital Signature Resource Center <http://ilpf.org/digsig/digsig2.htm> (*see supra* Section I for annotation).

Daniel J. Greenwood, *Risk and Trust Management Techniques for an "Open But Bounded" Public Key Infrastructure*, 38 JURIMETRICS J 277 (1998). Mr. Greenwood contrasts open and closed public key infrastructures ("PKIs"). (In open PKIs, subscribers obtain digital certificates which link their identities to their public keys for almost all purposes whereas in closed PKIs subscribers need to obtain different digital certificates for each type of transaction in which they engage.) He then advocates and describes an intermediate approach called the "open but bounded" PKI which, unlike the completely open PKI, requires advance agreements by known parties that define parameters for acceptable parties, uses, and processes for future transactions.

Digital Signature Working Group, Internet Law & Policy Forum, *Legislative Principles for Electronic Authentication and Electronic Commerce* (visited Dec. 13, 1998) <http://www.ilpf.org/digsig/principles.htm>. This draft, created by an Internet Law and Policy Forum working group convened in October, 1997, consists of eight core principles for which there was strong consensus and one principle still in need of further refinement. For a description of the Digital Signature Working Group's activities, visit its home page <http://www.ilpf.org/digsig/digsig.htm>.

Working Group on Certification Authority Practices, Internet Law & Policy Forum, *The Role of Certification Authorities in Consumer Transactions: Draft* (Apr. 14, 1997) <http://www.ilpf.org/work/ca/draft.htm>. This report focuses on the role of a certification authority ("CA") in an open system consumer setting in the United States, in which a consumer obtains an identity certificate from an independent CA and then uses it in dealing with many merchants. It does not address transactions between merchants. It suggests that the relationship between consumers and CAs is likely to be governed by contract law and, since the certificate will be like a service and not a good, common law principles should apply. Tort law would most likely govern the relationship of CAs and merchants who receive certificates from consumers.

R.R. Jueneman & R.J. Robertson, Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 JURIMETRICS J. 427 (1998). The authors argue that the use of identification techniques combined with cryptographic techniques associated with public key infrastructures can significantly elevate the levels of protection against an electronic document's having been tampered with or an electronic signature's having been forged. They review the law relating to written documents and pen-on-ink signatures and discuss modification needed to accomodate electronic documents. They conclude by analyzing the security risks associated with public key infrastructure cryptography and the ameliorative role that supplementation by biometric means might play.

Charles R. Merrill, *The Accreditation Guidelines—A Progress Report on a Work in Process of the ABA Information Security Committee*, 38

JURIMETRICS J. 345 (1998). The author offers an "interim glimpse of the major themes, methodology, and direction of the *Accreditation Guidelines*," a work-in-progress of the A.B.A.'s Information Security Committee that will offer standards to be used in accrediting digital signature certification authorities (trusted third parties whose function is to link the persons who are parties to an electronic transaction to specific public keys and thus verify their digital signatures as authentic).

Charles R. Merrill, *The Digital Notary (TM) Record Authentication System—A Practical Guide for Legal Counsel on Mitigation of Risk from Electronic Records* (June 22, 1995) <http://www.surety.com/in_news/legalgid.html>. This paper describes an electronic record authentication system, which does not rely on public key/private key encryption. Also included are considerations of the problems associated with cryptosystems that utilize keys and evidentiary and Statute of Frauds issues associated with electronic documents.

Richard Raysman, *Digital Signatures: Time-Saving Technology at Your Fingertips*, TR. & EST., Apr. 1996, at 22. This three-page, unfootnoted article offers a succinct, nontechnical introduction to digital signatures, discussing how they work, approaches to regulation as embodied in the Utah Digital Signature Act and the American Bar Association's *Digital Signature Guidelines*, and Statute of Frauds and security-related issues.

Brian W. Smith & Timothy E. Keehan, *Digital Signatures: The State of the Art and the Law*, 114 BANKING L.J. 506 (1997). This ten-page article describes public key/private key digital signature technology, state efforts at digital signature regulation (with particular emphasis on the Utah Digital Signature Act), Statute of Frauds issues (concluding that there are no Statute of Frauds problems concerning electronic contracts if evaluated using the criteria of U.C.C. Section 2-201), and alternatives to public key/private key authentication such as electronic handwritten signatures, off-line security, and smart cards.

Mike Tonsing, *The Digital Certificate Comes of Age*, FED. LAW., Oct. 1998, at 20. The author presents a two-page, unfootnoted description of digital certificates and certification authorities aimed at readers who want a nontechnical, easily read introduction to the subject.

Michael D. Wims, *Law and the Electronic Highway: Are Computer Signatures Legal?*, CRIM. JUST., Spring 1995, at 31. This three-page article provides a nontechnical, easy-to-read introduction to the underlying concepts essential for an understanding of the law of digital signatures. Basic terms such as encryption, public and private keys, and certification authority are simply explained. Included is an example of a digitally signed document.

Jane K. Winn, *Couriers Without Luggage: Negotiable Instruments and Digital Signatures*, 49 S.C. L. REV. 739 (1998). After a thorough description of the origins and development of negotiable instruments and digital signatures, the author discusses the risk allocation features of each, focusing on Uniform Commercial Code provisions and Federal Trade Commission rules relating to the former and the American Bar Association's *Digital Signature Guidelines* for the latter.

Jane K. Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177 (1998).

> This article will first describe the context in which digital signature applications are being developed . . . . At present, various groups are advancing different models of how Internet electronic commerce can be accomplished from technical and business perspectives; many of the competing models include digital signature technology administered in different forms. The second part of this Article examines how existing law treats signatures as evidence of intent to be legally bound and allocates the risk of loss due to forgeries or unauthorized signatures. This includes the law of signatures under contract law and negotiable instruments law, as well as the existing laws governing the use of authentication procedures in electronic funds transfers. This Article next reviews the ABA digital signature guidelines as a conceptual framework for technology specific legislation and the recent electronic commerce law passed in Rhode Island as a model of technology-neutral legislation. It compares those models to the existing law of signatures and authentication procedures. Finally, this Article reviews the policy issues raised by technology specific legislation, the rules for allocating fraud losses in commercial transactions, and the problem of market failure due to imperfect calculation of risk by consumers in complex transactions.

Id. at 1183-4.

Benjamin Wright, *Authenticating EDI: The Location of a Trusted Recordkeeper*, 4 SOFTWARE L.J. 173 (1991). The author argues that authentication of the contents of electronic contracts is best done by turning to separate "internal recordkeepers" employed by each contracting party rather than to independent third parties ("external recordkeepers"). His rationale is that "internal recordkeepers" would be "less expensive and administratively cumbersome," confidentiality of document contents would be better protected, and an "internal recordkeeper's" records would be under the control of only one contracting party, therebye simplifying issues of access and ownership.

Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures, in* DOING BUSINESS ON THE INTERNET: THE LAW OF ELECTRONIC COMMERCE, at 65 (PLI Patents, Copyrights, Trademarks, & Literary Property Course Handbook Series No. G-452, 1996). The author evaluates two methods of authenticating electronic signatures: public-key cryptography (as embodied in the Utah Digital Signature Act) and

pen biometrics (with emphasis on the PenOp system.). A slightly different version of this article appears at 15 J. MARSHALL J. COMPUTER & INFO. L. 303 (1996).

Stephen S. Wu, *Incorporation by Reference and Public Key Infrastructures: Moving the Law Beyond the Paper-Based World*, 38 JURIMETRICS J. 317 (1998). Incorporation by reference is defined as one document becoming part of another document by "referring to the former in the latter, and declaring that the former shall be taken and considered as a part of the latter the same as if it were fully set out therein." *Id.* at 317. This four-part article "describes the emerging patterns of incorporation by reference in electronic commerce . . ., explains [its] significance . . . and sets out a hypothetical demonstrating this significance . . ., describes the obstacles to electronic commerce . . . posed by the paper-based law on incorporation by reference . . . and presents principles to guide legal developments." *Id.* at 318. Particular attention is paid to the significance of incorporation by reference for certification authorities.

William E. Wyrough, Jr. & Ron Klein, *The Electronic Signature Act of 1996: Breaking Down Barriers to Widespread Electronic Commerce in Florida*, 24 FLA. ST. U. L. REV. 407 (1997).

> This Article examines the issues associated with making the transition to electronic commerce via the use of electronic signatures and discusses the [Florida] Electronic Signature Act of 1996. Part II discusses both electronic commerce and tis concomitant security issues to provide a better understanding of the significance of electronic signatures. Part III discusses the history of traditional signatures and their legal importance, and provides a brief introduction to electronic signatures. Part IV examines the development of a type of electronic signature called a 'digital signature.' Part V highlights the conclusions and recommendations of the Joint Committee that formed the basis of the electronic signature legislation. Part VI describes the Electronic Signature Act of 1996, discusses its enactment, and analyzes its possible effect.

Id. at 409.

C. Bradford Biddle, Comment, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L. REV. 1143 (1996).

> This Comment begins by presenting a brief overview of digital signature technology in Section II . . . . A summary of the Utah Digital Signature Act follows in Section III. Section IV describes the Utah Digital Signature Act's status as a putative Model Act, and suggest that this status may not be entirely appropriate. In Section V, the focus turns to a comparison of the liability allocations and evidentiary burdens imposed by the Utah Act to three analogous models: the credit card model, the notary model, and the telecommunications toll fraud model . . . . An alternative approach to the apportionment of liability in a public key infrastructure is proposed, based upon a proposed reform in the analo-

> gous arena of telecommunciations toll fraud. Ultimately, this Comment asserts that the liability allocations of the Utah Act inappropriately impose potentially unlimited risk on users of digital signatures, ignoring an important policy of consumer protection. This Comment additionally asserts that the provisions of the Utah Act which limit the liability of certification authorities undermine the economic integrity of the infrastructure implemented by the Act.

Id. at 1145.

Anthony M. Singer, Note, *Electronic Commerce: Digital Signatures and the Role of the Kansas Digital Signature Act*, 37 WASHBURN L.J. 725 (1998). The author provides an overview of the types of digital signature legislation that have been passed by state legislatures and then critically analyzes the Kansas Digital Signature Act. He concludes that the Kansas Act will make the use of digital signatures unattractive to merchants in that while it places the burden of proof on them in the typical consumer transaction, it does not provide them with any mechanism for the authentication of digital signatures.

Christy Tinnes, Student Work, *Digital Signatures Come to South Carolina: The Proposed Digital Signature Act of 1997*, 48 S.C. L. REV. 427 (1997). The author offers a nontechnical description of digital signature technology and the proposed South Carolina statute that would regulate it. She also briefly describes the Statute of Frauds provisions of U.C.C. Article 2 as they relate to electronic contracts, international efforts to regulate the use of digital signatures, and case law relating to electronic signatures in contracts created by telefacsimile, telegram, and computerized transmissions.

John P. Tomaszewski, Comment, *The Pandora's Box of Cyberspace: State Regulation of Digital Signatures and the Dormant Commerce Clause*, 33 GONZAGA L. REV. 417 (1997/98). The author discusses the law of electronic commerce, focusing on issues associated with verification and authentication. He examines approaches that the states have taken in regard to these issues and divides all of them into two categories: one in which the state regulates the duties, liabilities and standards for certification authorities (CAs) only as these relate to doing business with the state (the Massachusetts approach) and another in which the state regulates CAs for all commercial purposes, both public and private (the Washington State approach). He concludes that the Massachusetts approach is exempt from Commerce Clause review whereas the Washington State approach is not. He further concludes that the latter fails the strict scrutiny test regarding its requirement that a CA be Washington-licensed and also fails the *Pike* balancing test, in which the interests of the state are balanced against the burden placed on interstate commerce when that test is applied to the requirement that only Washington State-licensed CAs may operate certificate repositories (Pike v. Bruce Church,

Inc., 397 U.S. 137 (1970)). He notes that "the inherent nature of electronic commerce makes regulation and licensing of those entities who operate in cyberspace more appropriate for either the federal government or a national accreditation authority." *Id.* at 461.

III. UNIFORM COMMERCIAL CODE/STATUTE OF FRAUDS AND EVIDENTIARY ISSUES

U.C.C. Art. 2B: Software Contracts and Licenses of Information (Transactions in Computer Information) (visited Dec. 13, 1998) <http://www.law.upenn.edu/bll/ulc/ulc.htm#ucc2b>; *Unif. Electronic Transactions Act* (visited Dec. 13, 1998) <http://www.law.upenn.edu/bll/ulc/ulc.htm#ueccta>. Uniform Commercial Code Article 2B and the Uniform Electronic Transactions Act, when finally adopted by the National Conference of Commissioners on Uniform State Laws, will serve as models for state legislatures seeking to regulate electronic commerce. These Web sites, part of the official site of the National Conference, contain all draft versions and issued statements regarding the acts.

Amelia H. Boss & Jane K. Winn, *The Emerging Law of Electronic Commerce*, 52 BUS. LAW. 1469 (1997). The authors discuss proposed revisions to the Uniform Commercial Code necessitated by new business practices made possible by electronic data interchange and other new communications technologies. They describe provisions that deal with the Statute of Frauds, attributing electronic messages to particular senders, the role of electronic agents (computer programs which act on behalf of a party without any direct input from him or her), timing considerations relating to contract formation, and new Article 2B, which applies to licenses of information and software contracts.

Halina S. Dziewit et al., *The Quest for a Paperless Office—Electronic Contracting: State of the Art Possibility But Legal Impossibility?*, 5 SANTA CLARA COMPUTER & HIGH TECH. L.J. 75 (1989). The authors examine the enforceability of electronic contracts, focusing on the Statute of Frauds and Uniform Commercial Code requirements that there be a writing, that the document be signed, and that its authenticity be verifiable. They conclude that legal obstacles to enforceability will be overcome if appropriate technological authenticity safeguards, such as digital signatures or public key encryption, are utilized.

Stewart I. Edelstein, *Litigating in Cyberspace: Contracts on the Internet*, TRIAL, Oct. 1996, at 16. Mr. Edelstein discusses the application of the Statute of Frauds provisions of the Uniform Commercial Code (Section 2-201) to agreements created using electronic data interchange ("EDI"). He concludes that courts will find that the writing and signature requirements of the Statute have been met if the parties have taken

"commercially reasonable" security measures. He also suggests questions for discovery and evidentiary considerations for trial.

Raymond T. Nimmer, *UCC Revision: Information Age in Contracts, in 17th Annual Institute on Computer Law: The Evolving Law of the Internet: Commerce, Free Speech, Security, Obscenity and Entertainment,* at 377 (PLI Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series No. G-471, 1997). This paper offers a discussion of the commercial and policy considerations that influenced the development of draft Article 2B of the Uniform Commercial Code. Of particular interest is the discussion of the Article's treatment of electronic contracts (beginning at 408), which focuses on formation and attribution issues.

R.J. Robertson, Jr., *Electronic Commerce on the Internet and the Statute of Frauds*, 49 S.C. L. REV. 787 (1998). After briefly comparing the benefits and negatives associated with two forms of electronic commerce, electronic data interchange ("EDI") and forms of "open electronic commerce" such as electronic mail, the author discusses three alternative approaches legislatures might take to ensure that electronic contracts conform with the Statute of Frauds requirements that there be a signed writing: do nothing and allow the courts to decide (after analyzing judicial opinions involving application of the Statute of Frauds to contracts executed using earlier technologies such as the telegraph, telex, telefacsimile, tape recordings, and computer records, he concludes that courts may well find that electronic contracts do not meet Statute of Frauds requirements); repeal the Statute of Frauds (he rejects this approach because the Statute is "deeply engrained in the American legal culture" and there are "compelling policy reasons" why it should not be repealed); or, the preferred method, to amend the Statute of Frauds to include electronic contracts. He then compares three approaches to regulation undertaken by the states: the Utah approach, which he characterizes as being unduly restrictive because it provides that only messages that include digital signatures can satisfy the Statute of Frauds; the Georgia approach, which although less restrictive in that digital signatures are not the only form of electronic signature that is acceptable, is still too restrictive in that it posits too many criteria for an electronic signature to meet Statute of Frauds requirements; and the Florida/Illinois approach, which is preferred because it provides that any electronic signature executed by a party with the intent that it authenticate a document fulfills Statute of Frauds requirements.

Peter N. Weiss, *Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Toward Developing a Security Policy*, 12 J. MARSHALL J. COMPUTER & INFO. L. 425 (1993). Pointing out that issues of evidentiary admissibility of electronic data interchange ("EDI") "system outputs" and the reliability and integrity of EDI systems

for electronic commerce are the same, the author examines the Federal Rules of Evidence as they relate to admissibility of electronic records and the security requirements of both paper- and EDI-based commercial systems. He proposes a security classification scheme based on principles enumerated in the federal Computer Security Act of 1987 and suggests security techniques appropriate for non-sensitive or "low, medium or high sensitive" EDI transactions.

John Anecki, *Comment, Selling in Cyberspace: Electronic Commerce and the Uniform Commercial Code*, 33 GONZAGA L. REV. 395 (1997/98).

> This Comment explores . . . how the current UCC, and proposed provisions, might apply to the use of electronic commerce. Section II provides a brief overview of the UCC Article 2 and its inability to adequately address the rapidly growing electronic commerce. Section III discusses the evolution of electronic commerce, the scope of the current Article 2 as it applies to electronic commerce, and the scope of the proposed Articles 2 and 2b. Section IV discusses electronic contract formation, presents a model electronic contract, provides proposed provisions of Articles 2 and 2B which specifically address electronic contracts, and discusses changes and errors in electronic records. Finally, Section V discusses the use of electronic agents.

Id. at 396.

Sharon F. DiPaolo, Note, *The Application of the Uniform Commercial Code Section 2-201 Statute of Frauds to Electronic Commerce*, 13 J.L. & COM. 143 (1993). This short note discusses the writing and signature requirements of the Uniform Commercial Code Statute of Frauds provision and briefly describes methods of authentication commonly used for agreements made through electronic data interchange ("EDI") technology. It concludes that given the traditionally broad construction accorded the U.C.C. by the courts and the high degree of reliability that electronic authentication techniques have shown, contracts executed utilizing EDI will be found to be "signed writings," enforceable under the Statute of Frauds.

Gregory L. Johnson, Comment, *Electronic Contracts: Are They Enforceable Under Article 2 of the U.C.C.?*, 4 SOFTWARE L.J. 247 (1991).

> This Comment will focus on whether exchanges using EDI [electronic data interchange] become legal, enforceable, and binding contracts subject to Article 2 of the U.C.C. First, this Comment will discuss the development of EDI and its implementation. Second, this Comment will review the purpose and premises of traditional or 'paper' contract formation under the U.C.C. Third, this Comment will address whether EDI transactions satisfy U.C.C. Section 2-201, the Statute of Frauds writing requirement. Fourth, the Comment will discuss the relationship of the parole evidence rule, U.C.C. Section 2-202, with EDI transactions. Fifth, this Comment will focus on 'the battle of the forms,' U.C.C. Section 2-207, as it relates to EDI transactions. Finally, the Comment

> concludes that Article 2 of the U.C.C., although initially drafted prior to the advent of the commercial use of computer technology, was masterfully drafted and brings EDI transactions within its scope. This Comment suggest that in an effort to update the U.C.C., 'Official Comments' should be drafted to include EDI technology.

Id. at 251.

Douglas R. Morrisson, Comment, *The Statute of Frauds Online: Can a Computer Sign a Contract for the Sale of Goods?*, 14 GEO. MASON L. REV. 637 (1992). The author analogizes the use of the telegraph in business transactions to present-day contracting through electronic data interchange ("EDI"). After offering an introductory description of EDI, he thoroughly reviews the case law relating to the commercial use of the telegraph, noting that those cases that post-date the advent of the telephone are the most applicable because they discuss transmissions not accompanied by written orders (telephone calls became the usual means of ordering telegrams, replacing the written order forms previously used). He concludes that EDI, like the telegraph, fulfills both the writing and the signing requirements imposed by the Statute of Frauds.

Marc E. Szafran, Note, *A Neo-Institutional Paradigm for Contracts Formed in Cyberspace: Judgment Day for the Statute of Frauds*, 14 CARDOZO ARTS & ENT. L.J. 491 (1995-1996).

> Because of the absence of clear authority, doubt as to whether electronic transactions constitute signed writings persists. Consequently, the question arises whether electronic contracts are enforceable in light of section 2-201 . . . . Applying a neo-institutional microeconomic theory for procedural efficiency in legal rule formulation, this Note suggests transferring the concept of the Statute from its historical role as a basic principle of contract formation—applicable to all transactions that fall within the scope of Article 2—into an ancillary contract law rule, applicable only to particular types of transactions . . . . The second point proposes that in following this neo-institutional cost/benefit analysis, certain commercial transactions—particularly transactions conducted via electronic networks—should not be governed by the Statute.

Id. at 494-7.

John R. Thomas, Note, *Legal Responses to Commercial Transactions Employing Novel Communications Media*, 90 MICH. L. REV. 1145 (1992).

> This Note analyzes contemporary business practices and specific characteristics of the new media [telefacsimile and electronic mail], and suggests a judicial response consonant with courts' approaches to the earlier technologies of telegraphy and teletype. Part I examines the effect of the Statute of Frauds and rules of authentication upon contracts formed using these media. It concludes that documents produced by telefacsimile and electronic mail systems should be considered ordinary writings. Part II considers the Best Evidence Rule and argues that telefacsimiles and electronic mail transmissions should be considered the best evidence of the contract they memorialize. Part III evaluates

> doctrines of liability allocation in the event of a transmission error . . . . It concludes that these doctrines are based upon theories of agency, common carriage, and contract law, rather than characteristics of individual media, and that telefacsimile and electronic mail systems do not require reconsideration of these doctrines. This Note concludes that telefacsimile and electronic mail services, like earlier systems of telegraphy and teletype, should be recognized as legally acceptable media for contract formation.

Id. at 1148.

Deborah L. Wilkerson, Comment, *Electronic Commerce Under the U.C.C. Section 2-201 Statute of Frauds: Are Electronic Messages Enforceable?*, 41 KAN. L. REV. 403 (1992). The author's examination of whether electronic contracts meet the U.C.C. section 2-201 Statute of Frauds requirements that enforceable contracts be written and signed concludes that while it is likely that courts will conclude that they do, there would be less uncertainty if the U.C.C. provisions were redrafted to specifically include electronic agreements. Included are an examination of some of the case law involving contracts transmitted via telefacsimile, telex, and telegraph, evidentiary issues that might arise, and what are commercially reasonable security measures that might be used to protect the authenticity and integrity of electronic messages.

IV. ENCRYPTION/CRYPTOGRAPHY AND SECURITY ISSUES

Encryption: Individual Right to Privacy vs. National Security: Hearing Before the Subcomm. on International Economic Policy and Trade of the House Comm. on International Relations, 105th Cong. (1997). (Available in Congressional Information Service microfiche, CIS 98-H461-57. Superintendent of Documents No. Y4.IN8/16:R44/2) (116 p.). Witnesses discuss United States government encryption control and export policies and the development of encryption and key recovery technologies. The Security and Freedom Through Encryption Act, H.R. 695, which is concerned with decreasing export controls on encryption software, is also considered.

Office of Tech. Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information* (Comm. Print 1987). (Available in Congressional Information Service microfiche, CIS 87-J952-61. Superintendent of Documents No. Y3.T22/2:2D36) (186 p.). This report, prepared for the House Government Operations Committee and the House Judiciary Committee Subcommittee on Civil and Constitutional Rights, discusses the relationship of government agencies and the private sector in the development and implementation of computer security technologies.

Office of Tech. Assessment, *Information Security and Privacy in Network Environments* (Comm. Print 1994). (Available in Congressional In-

formation Service microfiche, CIS 94-J952-49. Superintendent of Documents No. Y3.T22/2:2SE2/2) (244 p.). This report, prepared for the Senate Governmental Affairs Committee and the House Energy and Commerce Committee Subcommittee on Telecommunications and Finance, discusses technical, legal, and policy issues relating to computer network security.

S. 1726, *Promotion of Commerce Online in the Digital Era Act of 1996, or Pro-CODE Act: Hearing Before the Subcomm. on Science, Technology, and Space of the Senate Comm. on Commerce, Science, and Transportation,* 104th Cong. (1996). (Available in Congressional Information Service microfiche, CIS 97-S261-1. Superintendent of Documents No. Y4.C73/7:S.HRG.104-624) (299 p.). Witnesses testify regarding the need for the federal government to loosen its export controls on encryption technology.

A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

> This is a long article. It is long because it addresses three complex issues. First, it outlines some of the promises and dangers of encryption. Second, it analyzes the constitutional implications of a major government proposal premised on the theory that it is reasonable for the government to request (and perhaps some day to require) private persons to communicate in a manner that makes governmental interception practical and preferably easy. Third, it speculates as to how the legal vacuum regarding encryption in cyberspace shortly will be, or should be, filled.

Id. at 713. The article also offers a good description of encryption technology.

Emily Frye & Randy V. Sabett, *Key Recovery in a Public Key Infrastructure*, 38 JURIMETRICS J. 485 (1998). The United States Government has argued that it must have access to all cryptographic keys (i.e., key recovery) as a crime prevention measure. Industry has argued that this would make electronic commerce less attractive because it would breach the confidentiality required for many transactions and also make the American cryptography industry less competitive internationally. This paper "explore[s] the merits of both government and industry arguments . . ., discusses ways that key recovery might fit into the emerging public key infrastructure . . . [and] recommend[s] that key recovery be a strictly voluntary endeavor." *Id.* at 487.

Charles R. Merrill, *A Cryptography Primer*, *in* THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES, at 13 (1996), *reprinted in* DOING BUSINESS ON THE INTERNET: THE LAW OF ELECTRONIC COMMERCE, at 395 (PLI Patents, Copyrights, Trademarks, & Literary Property Course Handbook Series No. G-452, 1996). This primer provides an eight-page introduction to public key encryption,

message security and its attendant problems in online networks, and government regulation of encryption technology.

Edward J. Radlo, *Legal Issues in Cryptography*, COMPUTER LAW., May 1996, at 1. The author offers a brief overview of existing types of cryptography (e.g., private key cryptographic systems such as the U.S. Data Encryption Standard (DES) and Skipjack, and public key cryptographic systems such as PGP) and then discusses the following legal issues: export control of cryptographic products by the U.S. Departments of State and Commerce, the Federal Information Processing Standards ("FIPS"), the significance of cryptography standards developed by nongovernmental groups and foreign governments, and patent issues.

David P. Vandagriff, *Who's Been Reading Your E-Mail? Two Easy-to-Use Tools Can Protect Privacy, Integrity of Documents*, A.B.A. J., May 1995, at 98. This one-page article provides a nontechnical introduction to PGP (Pretty Good Privacy) public key encryption technology and how a lawyer might use it to affix a digital signature to a document.

Peter N. Weiss, *Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Toward Developing a Security Policy*, 12 J. MARSHALL J. COMPUTER & INFO. L. 425 (1993). *See supra* Section III for annotation.

Mai-Tram B. Dinh, Note, *The U.S. Encryption Export Policy: Taking the Byte Out of the Debate*, 7 MINN. J. GLOBAL TRADE 375 (1998).

> This Note argues that while the U.S. encryption export policy may not be ideal, no alternative achieves a better balance of interests in privacy, economic growth, and national security. Section I explains the background of the Internet as a vehicle for electronic commerce (e-commerce) and outlines the U.S. policy statement concerning e-commerce. Section II describes the U.S. encryption export policy. Section III sets forth the effects of encryption technology on e-commerce and analyzes the export policy in the context of the United States' stated goals. Finally, Section IV explains why criticism of the current policy is unwarranted.

Id. at 375.

Ryan A. Murr, Comment, *Privacy and Encryption in Cyberspace: First Amendment Challenges to ITAR, EAR and Their Successors*, 34 SAN DIEGO L. REV. 1401 (1997). The author examines the constitutionality on First Amendment grounds of the export limitations imposed on encryption technology by the Export Administration Regulations ("EAR") and the International Trade in Arms Regulations ("ITAR") and concludes that they are unconstitutional in that they are content-based, do not meaningfully further the security interests of the United States, and unnecessarily interfere with the exercise of rights of privacy and freedom of expression.

Kenneth P. Weinberg, Note, *Cryptography: "Key Recovery" Shaping Cyberspace (Pragmatism and Theory)*, 5 J. INTELL. PROP. L. 667 (1998).

> The purpose of this Note is not only to summarize the encryption debate, but also to offer new insight into an issue that may very well shape the future of society . . . . Section II of the Note briefly describes cyberspace and the Internet. Section III sets the stage for the encryption debate by defining cryptography . . ., discussing the ways in which encryption is a necessary component of cyberspace, and describing the government's reasons for wanting to limit the use of encryption. Section IV begins the analysis of the encryption debate by introducing the government's *'key recovery'* proposals [Key recovery is the ability of a third party to covertly access the plaintext and digital signatures associated with an encrypted electronic document.] . . . . Section V offers a more theoretical critique of 'key recovery' by arguing that a key recovery system would result in the elimination of all physical limitations on the government's surveillance capabilities. A Fourth Amendment analysis of how courts have struggled with legal limitations when physical barriers are removed suggests that it would be extremely unwise to rely solely on legal limitations to protect the privacy of United States citizens.

Id. at 667-670. The author's description of cryptography technology is written in a nontechnical style intended for a lay audience.

V. FOREIGN AND INTERNATIONAL ASPECTS

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996) <http://www.un.or.at/uncitral/en-index.htm>. This Web site, the home page of the United Nations Commission on International Trade Law, includes the full text of the Model Law as adopted by the U.N. General Assembly in December 1996 as well as information about related activities sponsored by the Commission.

Towards a European Framework for Digital Signatures and Encryption (visited Dec. 1, 1998) <http://www.ispo.cec.be/eif/policy/#digital>. This Web site, hosted by the European Internet Forum, includes the text of this Communication from the Commission (of the European Communities) to the European Parliament, the Council, the Economic and Social Committee of the Regions on Ensuring Security and Trust in Electronic Communications, adopted by the Commission in October 1997, as well as the text of the Copenhagen Hearing on Digital Signatures and Encryption, held April 23-24, 1998, and documents, press releases, and speeches related to general Internet issues.

Juan A Avellan V, *John Hancock in Borderless Cyberspace: The Cross-Jurisdictional Validity of Electronic Signatures and Certificates in Recent Legislative Texts*, 38 JURIMETRICS 301 (1998). The author surveys approaches to electronic signature verification either under consideration or adopted around the world. Much attention is paid to the United

States (particularly the states of Hawaii, Mississippi, Utah, California, Washington, Massachusetts, and Illinois), the European Union, Germany, and the United Nations Conference on International Trade Law. Footnotes offer many URLs for Web sites containing both domestic and foreign documents.

Amelia H. Boss, *The Emerging Law of International Electronic Commerce*, 6 TEMP. INT'L & COMP. L.J. 293 (1992). This short article, based on a presentation given by the author at the Congress on Uniform Commercial Law in the 21st Century, sponsored by the United Nations Commission on International Trade Law in May, 1992, discusses how electronic communications technologies are modifying business practices and creating new related service industries, and what appropriate international forms of regulation might be.

Amelia H. Boss, *The International Commercial Use of Electronic Data Interchange and Electronic Communications Technologies*, 46 BUS. LAW. 1787 (1991). Professor Boss surveys the work of the following organizations on the legal implications of conducting business using electronic data interchange and other electronic messaging technologies: United Nations Commission on International Trade Law, United Nations Working Party on the Facilitation of International Trade Procedures, International Chamber of Commerce, Commission of the European Communities, and the American Bar Association's Section of Business Law.

Clive Davies, *Legal Aspects of Digital Signatures*, 11 COMPUTER L. & PRAC. 165 (1995). This four-page article offers an overview of the British law of electronic commerce and digital signatures. A brief discussion of French and German law is also included.

Richard Hill & Ian Walden, *The Draft UNCITRAL Model Law for Electronic Commerce: Issues and Solutions*, COMPUTER LAW., Mar. 1996, at 18. The authors offer a brief discussion of the general treatment of the following issues in Europe, the United States, and by the United Nations Commission on International Trade Law's *Model Law on Legal Aspects of Electronic Data Interchange and Related Means of Communication*: the requirement of writings and that they be signed, whether electronic transmissions constitute signed writings, and evidentiary considerations.

Chris Reed, *Authenticating Electronic Mail Messages—Some Evidential Problems*, 4 SOFTWARE L.J. 161 (1991). The author applies British law to issues relating to authentication and admissiblility of electronic documents. Included is a description of electronic mail and digital signature cryptography technologies.

Symposium, *Current Issues in Electronic Data Interchange*, 13 Nw. J. INT'l L. & Bus. 1 (1992). The symposium includes the following arti-

cles: Jeffrey B. Ritter, *Defining International Electronic Commerce*, at 3; Amelia H. Boss, *Electronic Data Interchange Agreements: Private Contracting Toward a Global Environment*, at 31; Aileen A. Pisciotta & James H. Barker, *Telecommunications Regulatory Implications for International EDI Transactions*, at 71; Judith Y. Gliniecki & Ceda G. Ogada, *The Legal Acceptance of Electronic Documents, Writings, Signatures, and Notices in International Transportation Conventions: A Challenge in the Age of Global Electronic Commerce*, at 117; and George B. Trubow, *The European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans Border Data Flow*, at 159.