Nova Law Review

Volume 23, *Issue* 2 1999 *Article* 3

Searching for Security in the Law of Electronic Commerce

Amelia H. Boss*

*

Searching for Security in the Law of Electronic Commerce

Amelia H. Boss

TABLE OF CONTENTS

I. INTRODUCTION 585
II. THE NEED FOR SECURITY 590
III. THE DEBATE: A CONFLUENCE OF TWO STREAMS 596
IV. SURVEYING THE BATTLE FRONT 602
V. ENABLING VERSUS PROMOTING: THE DEBATE IN THE UNIFORM LAW PROCESS 608
VI. UNIFORM ELECTRONIC TRANSACTIONS ACT 608
VII. ARTICLE 2B OF THE UNIFORM COMMERCIAL CODE 611
VIII. INTO THE BREACH: LEGISLATING FOR SECURITY 615
IX. CONCLUSION 622

I. INTRODUCTION

Since before the time Gutenberg invented the printing press, centuries of jurisprudence have been devoted to and predicated upon paper-based systems of communication, particularly in the area of commercial law. With advances in technology and the implementation of electronic modes of communication in businesses and market places in general, however, the world has begun to move away from paper as the primary mode of communication and the primary method of doing business.[1] This continues the process begun with the introduction of the telegram and the telephone, both of which contributed to the elimination of paper in the conduct of business negotiations.

Electronic commerce, however, is fundamentally different from either telephonic or paper-based commerce. First, there is no tangible piece of paper that one can treat as the final expression of the parties' intent; reliance must be placed upon electronic messages, which are either stored in an electronic medium or, in the case of risk-averse business people, printed out at

1. According to the Organization for Economic Co-operation and Development ("OECD"), the volume of electronic commerce may rise to $1 trillion by 2005. Organization for Economic Co-operation and Development, *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda*, ch. 1 (1998) <http://www.oecd.org/subject/e_commerce/summary.htm>; *see generally Id.* at ch. 3. *See generally* U.S. Department of Commerce, *The Emerging Digital Economy* (1998) <www.doc.gov/ecommerce/EmergingDig.pdf>.

one end. Second, the electronic message is often generated by a computer and may not provide the typical indicia of trustworthiness. For example, with paper, we can recognize the handwriting, identify the stationery, check the postmark and address, and check for visible changes to the writing. On the telephone, we can recognize the voice and verify the number we are calling. Third, commercial transactions have traditionally required time and, frequently, additional verifiable information for completion. For example, in the sale of goods, the time between the execution of the sales agreement and the ultimate shipment or delivery of goods allows for verification of creditworthiness and of other information such as shipment details. Electronic transactions, on the other hand, are often executed online instantaneously between computers, and the ability to verify the identity of the parties and other information is radically reduced. Indeed, one emerging characteristic of much of electronic commerce, such as the web-based transaction, is the transitory nature of the relationship between the parties. Last, the tangible nature of the transaction, e.g., the sale of goods, has allowed for security measures such as the creation and potential enforcement of security interests in the property that was sold. By contrast, the subject matter of electronic commerce is increasingly intangible,[2] reducing the ability to monitor and enforce the obligations of the other party.[3]

---

2. Although tangible goods are frequently sold in electronic commerce, online transactions involving intangibles such as software and information are multiplying. On the emergence of a new species of property, information, as one important aspect of the development of electronic commerce, see Amelia H. Boss, *The Emerging Law of International Electronic Commerce*, 6 TEMP. INT'L & COMP. L.J. 293, 298–300 (1992); Katherine Mahoney, *Information as a Commodity: New Imperatives of Commercial Law*, 55 LAW & CONTEMP. PROBS. 77, 103 (1992); Raymond T. Nimmer & Patricia Ann Krauthaus, *Electronic Commerce: New Paradigms in Information Law*, 31 IDAHO L. REV. 937, 937 (1995); Margaret Jane Radin, *Property Evolving in Cyberspace*, 15 L.J. & COM. 509, 511–13 (1996). The increasing predominance of information as the subject matter of the deal has given rise to efforts to create legal structures accommodating these new transactions, the main one of which has been the drafting of a new article to the Uniform Commercial Code, Article 2B, to cover transactions in software and information, *see* U.C.C. art. 2B (Proposed Draft Dec. 1998), *available at* <http:www.law.upenn.edu/bll/ulc/ulc.htm#UCC2B>, or, alternatively, computer information transactions. *See* U.C.C. art. 2B (Proposed Draft Feb. 1, 1999), *available at* <http:www.law.upenn.edu/bll/ulc/ulc.htm#UCC2B>. Evolution of new types of transactions creates concern about the rules applicable to those transactions, and concomitantly, there is some desire for certainty and predictability in developing a legal framework. As with the case of electronic contracting, which is discussed in this article, there are instances where the demand for such rules may be misplaced, arising from the assumption that only positive law may create an environment where transactions may be trusted.

3. Traditional factors in commercial transactions that contribute to amicable and effective resolution of disputes, e.g., ongoing relationships between the parties, sufficient time to structure the transaction, and potential collateral, are often absent in online transactions.

The emergence of electronic commerce has raised a host of questions about our existing rules and legal system. One frequent plea is to remove the barriers to electronic commerce, barriers that are, to a great degree, the vestiges of a commercial law system based on paper. Legal requirements, such as those for a "writing," a "signature," and an "original" need to be reconsidered in the context of electronic commerce. Efforts are underway to respond to these demands in the following ways: in the domestic arena, the Uniform Commercial Code[4] and the proposed Uniform Electronic Transactions Act ("UETA");[5] and on the international level, the formulation of the United Nations Commission on International Trade Law ("UNCITRAL") Model Law on Electronic Commerce.[6]

---

4. Pending revisions to Article 2 of the Uniform Commercial Code, as well as the pending proposal to include computer information transactions in a new Article 2B, include provisions addressing the application of such requirements in an electronic environment. *See* Raymond T. Nimmer, *Article 2B: An Introduction*, 16 J. MARSHALL J. COMPUTER & INFO. L. 211, 227–37 (1997) (reviewing electronic and online commerce provisions of Article 2B); Raymond T. Nimmer, *Electronic Contracting: Legal Issues*, 14 J. MARSHALL J. COMPUTER & INFO. L. 211, 212 (1996); Amelia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform*, 72 TULANE L. REV. 1931, 1956–63 (1998) (reviewing the changes being made in Article 2B and the Uniform Electronic Transactions Act to accommodate electronic commerce). Other completed revisions to the Code do so through a variety of techniques. Article 5, for example, adopts terms such as "record" in place of "writing" and contemplates presentation of non-paper documents. *See* U.C.C. § 5-102 (a)(14) (1997) (defining record); *id.* § 5-102(a)(6) (defining document to include presentation in any media permitted by the letter of credit or standard practice); *id.* § 5-102 cmt. 2 (revised Article 5 "contemplates and facilitates the growing recognition of electronic and other nonpaper media as 'documents'"). *See also* R. David Whitaker, *Letters of Credit and Electronic Commerce*, 31 IDAHO L. REV. 699, 699–701 (1995). Article 8 eliminates any statute of frauds writing requirement for contracts transferring interests in securities. *See* James S. Rogers, *An Essay on Horseless Carriages and Paperless Negotiable Instruments: Some Lessons From the Article 8 Revision*, 31 IDAHO L. REV. 689, 691 (1995); U.C.C. § 8-113 (1997). Completed in 1999, revised article 9 also uses the terms "record" and "authenticate" in place of "writing" and "signed." U.C.C. § 9-102(a)(7) (authenticate); *id.* § 9-102(a)(69) (record).

5. Currently scheduled for completion in August of 1999, the Act contains electronic contracting rules for transactions outside the scope of the Uniform Commercial Code. *See Uniform Law Commissioners Drafts* <http://www.law.upenn.edu/bll/ulc/ulc.htm> (for drafts of the UETA).

6. The United Nations Commission on International Trade Law ("UNCITRAL") has taken the lead at the international level in formulating the law governing electronic commerce, and in 1996, it gave its final approval to a new Model Law on Electronic Commerce which contains many provisions adapting the formalities of the law to an electronic environment. *See* REPORT OF THE UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW ON THE WORK OF ITS TWENTY-NINTH SESSION, U.N. GAOR, 51st Sess., Supp. No. 17, U.N.Doc. A/51/17 Annex I (1996), *reprinted in* 36 I.L.M. 200 (1997). *See* Amelia H. Boss & Jane

In many arenas, however, demands are being made on legislators and lawmakers to go beyond mere removal of legal barriers and to "support" the development of electronic commerce by the establishment of a legal framework that encourages and promotes its use. The argument is that the law should build confidence in the system by providing rules that support and promote these new ways of doing business.

In many respects, these demands are quite understandable, as they combine two needs. The first is the perceived need for rules to guide conduct on the Internet. The public and the press have in recent years become so enamored of technology that they use phrases such as "revolutionary" to describe it. The characterization of cyberspace as something new and alien creates in people a fear that it is indeed unknown and unknowable, and people distrust the unknown. The result is concern about what will govern this unknown and uncharted territory. Some have argued that the Internet as a unique jurisdiction should be subject to its own body of rules,[7] while others have attempted to resolve issues on the Internet by analogizing it to other areas of law.[8] The real challenge is to examine the

---

Kaufmann Winn, *The Emerging Law of Electronic Commerce*, 52 BUS. LAW. 1469, 1469 (1997); 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*, 13 NW. J. INT'L L. & BUS. 117 (1992); Daniel J. Greenwood & Ray A. Campbell, *Electronic Commerce Legislation: From Written on Paper and Signed in Ink to Electronic Records and Online Authentication*, 53 BUS. LAW. 307, 307–09 (1997) (comparing provisions of the UNCITRAL Model Law with domestic legislation). For an overview of the relationship between the domestic efforts and the international efforts, see *supra* note 4. There are, of course, other efforts both within UNCITRAL and other international organizations to consider other aspects of electronic commerce.

7. *See, e.g.*, David G. Post & David R. Johnson, *Chaos Prevailing on Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI. KENT L. REV. 4 (forthcoming 1999). In other contexts, the tendency to see the Internet as a separate place necessitating different legal rules has been criticized. Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703, 703 (1998) (concluding that the Internet is simply an alternative communications technology, and that there is no more a need for the 'law of cyberspace' than there ever was for the "law of the alphabet.").

8. One scholar surveyed the evolution of "Internet law," tracing it through two stages. In the first stage, the Internet was analogized to other areas where the legal doctrine was well established. In the second stage, a more advanced analysis focused on the nature and quality of the activity taking place. *See* Michael A. Geist, *The Reality of Bytes: Regulating Economic Activity in the Age of the Internet*, 73 WASH. L. REV. 521 (1998). Professor Geist's analysis was limited to developments in the area of jurisdiction and did not encompass the area of security and electronic commerce. Similarly, others trying to find trends in the law applicable to the Internet have focused on First Amendment issues. *See, e.g.*, Clay Calvert, *Regulating*

need for rules *in context* and determine whether the issue under consideration is sufficiently different in an Internet or online context to justify a different set of rules than would otherwise exist.[9]

The second need is security. In large part, the newness of the technology, unfamiliarity with the operation of the Internet, and the potential for fraud and error have given rise to concerns about the "trustworthiness" of the system. Indeed, "security" is one of the key words that is often bandied about in the context of electronic commerce; that is, the need for security and trustworthiness in online transactions.[10] Concerns about "security" are heard in all venues: legal,[11] technological,[12] business,[13] and theoretical.[14]

Cyberspace: Metaphor, Rhetoric, Reality and the Framing of Legal Options, 20 HASTINGS COMM. & ENT. L.J. 541, 554 (1998). Each area is distinguishable, however, from the concerns of the present Article. For example, in the area of jurisdiction, the primary forum for the development of "Internet law" has been the courts, not the legislature. By contrast, to date, the primary forum for the development of Internet law in the commercial context has been the private sector, and there have been few judicial decisions. Only recently have the legislatures become involved.

9. *See, e.g.*, Allan R. Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INT'L LAW 1167, 1167 (1998) (arguing that "there is nothing about legal relations over computer networks that in any way challenges our conventional notions about how sovereign authority is allocated in the world"); Amelia H. Boss, *The Jurisdiction of Commercial Law: Party Autonomy in Choosing Applicable Law and Forum Under Proposed Revisions to the Uniform Commercial Code*, 32 INT'L LAW 1067, 1068 (1998) (nothing about electronic commerce requires different rules on enforceability of choice of law and forum clauses). In Canada, a study for the federal government reached the same conclusion. Industry Canada (1998), *The Internet is not a No-Law Land*, *available at* <http://strategis.ic.gc.ca/>. *See also* John D. Gregory, *Solving Legal Issues in Electronic Commerce*, CAN. BUS. L.J. (forthcoming 1999) (some legal issues in electronic commerce can be and are being resolved by application of existing rules, once people become familiar with the new medium).

10. A sampling of the legal literature in the area of electronic commerce demonstrates the currency of the theme of "security." *See Public Key Infrastructure Symposium*, 38 JURIMETRICS J. 241 (1998).

11. Frequently, the legal arguments concerning security focus on restrictions on cryptography. *See* STEWART A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST: CRYPTOGRAPHY, GOVERNMENTS, AND ELECTRONIC COMMERCE (The Hague, London & Boston, 1998).

12. Recently, there has been an extensive amount of writing on concepts of trust from a technological perspective. *See, e.g.*, COMMITTEE ON INFO. SYS. TRUSTWORTHINESS, TRUST IN CYBERSPACE (Fred B. Schneider ed. 1999), *available at* <http://www.nap.edu/readingroom/>.

13. *See* Dan Greer, *Risk Management Is Where the Money Is*, THE RISKS DIG., Col. 20, Issue 6 (Nov. 12, 1998) <http://catless.ncl.ac.uk/risks/20.06/htm>: "The focus of 'security' research today is the study of 'trust management'—how trust is defined, created, annotated, propagated, circumscribed, stored, exchanged, accounted for, recalled and adjudicated in our electronic world." *Id.*

The need to provide "security" or "secure systems" for electronic commerce is being expressed not just at the technical and implementation levels but in legislatures as well.[15]

Combined with this is the reality that many legislators also want to be seen as at the cutting edge of technology and have introduced legislation at both the state and the federal levels.[16] State legislators, in particular, want to be the first to enact "electronic commerce" statutes, thereby attracting businesses into their region and appearing to be global leaders to their constituents. There might be, however, a problematic result: the passage of "technology" legislation that is premature and potentially counter-productive.[17]

II. THE NEED FOR SECURITY

Concerns about security, whether real or perceived,[18] need to be put into perspective. Security cannot be "legislated." It is a combination of factors: the technology utilized,[19] its business implementation and state of development, and the legal structure. Doing business "securely" on the information highway is not a simple matter of developing the right technologies to "lock up" information sent electronically to protect it against

14. Ed Gerck, *Towards Real-World Models of Trust: Reliance on Received Information* <http://www.mcg.org.br/trustdef.htm> (presenting an abstract definition of trust derived from different application areas, including communication systems, digital certificates, cryptography, law, linguistics, social sciences, etc.).

15. The United Kingdom has framed the issue as "building confidence in electronic commerce." *See Building Confidence in Electronic Commerce* (Mar. 5, 1999) <http://www.dti.gov.uk/cii/elec/elec_com.html>.

16. *See, e.g.*, Philip S. Corwin, *Electronic Authentication: The Emerging Federal Role*, 38 JURIMETRICS J. 261 (1998) (discussing federal bills during the 105th Congress).

17. Australian Electronic Commerce Expert Group, *Electronic Commerce: Building the Legal Framework*, Executive Summary <http://www.law.gov.au/aghome/advisory/eceg/welcome.html> ("There is the risk, particularly given the lack of any internationally uniform legislative approach, that an inappropriate legislative regime may be adopted without regard to market-oriented solutions.").

18. There is a view, generally accepted by persons familiar with technology, that in certain areas technology has the capability of offering *more* security in commercial transactions than paper-based systems. *See* WARWICK FORD & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE: BUILDING THE INFRASTRUCTURE FOR DIGITAL SIGNATURES AND ENCRYPTION (Upper Saddle River, NJ 1997); MICHAEL S. BAUM & HENRY H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING, AND EDI LAW (John Wiley & Sons, Inc. 1991).

19. *See* Raymond T. Nimmer & Patricia Krauthaus, *Electronic Commerce: New Paradigms in Information Law*, 31 IDAHO L. REV. 937, 945 (1995) ("the creation of system-based assurances of authenticity constitutes a condition precedent for continued expansion in the modern use of the systems in important marketplaces").

theft or alteration, nor is it a simple matter of developing authentication techniques that allow us to determine with extreme accuracy the actual originator or creator of a given message. "Secure" electronic commerce cannot be achieved merely by legislating those circumstances when requisite "security" is present. Rather, the "security" which business people seek when they begin doing business electronically requires the creation of an entire infrastructure—legal, social, economic, and political—one that is based on practice which recognizes, validates, and supports electronic commerce.

By comparison, many of us feel secure in our homes. This security does not necessarily flow from the existence of technological devices to keep out unwarranted intrusions: fences, burglar alarms, bolts, locks, or caller identification on the telephone. To a great degree, the availability of those devices does contribute to our sense of security, but the relationship is not necessarily a direct correlation. Indeed, the more such technological security devices there are in a home, the less likely it is that the inhabitant feels "secure." While some locks or keys may be necessary, the strongest feelings of security flow from the knowledge that locks and bolts are not needed, that one can leave the house unlocked with the expectation that upon return, things will be as they were upon departure.

Security is more than the technological exclusion of others from our premises and more than mere legislation. Security flows in large part from the ability to predict, with a fair degree of certainty, what lies ahead in our daily lives, the ability to control it, and the ability to identify, again with a fair degree of certainty, the risks that we may face so that we can take protective measures. It also comes from the knowledge that there is a social, political, economic, and legal system that protects us and recognizes our rights. It is the overall structure, not any particular technology or law, that creates that security. In our society, that overall structure includes the right to use and control property, the ability to acquire and hold that property, the knowledge that ownership of the property is free and clear of the claims of others, the ability to exclude others from one's property, the ability to move freely about the property and come and go as desired, the ability to allow others access to one's property as desired, the ability to sell or otherwise dispose of one's property, and the right to enforce that sale or transfer. Security flows from the knowledge that the economic, social, and legal systems recognize these rights, and that redress is available from those who violate or infringe them.[20]

20. Security in the home also flows from the knowledge that there is an economic, social, political, and legal structure out there that protects our home that sends firemen and police as needed, arrests trespassers or thieves and brings them to justice through the court system, and provides us with the services needed to use and enjoy our property.

Similarly, for businesses involved in electronic commerce, "doing business securely" means an entire complex of things. It encompasses the ability to enter into a commercial transaction that proposes an exchange on terms beneficial to each party, whether a sales, services, or commodities agreement, with the reasonable expectation that it will be performed. Contracts are performed because our economic, social, and legal structures support these types of transactions and provide incentives for performance as well as disincentives for breach. These economic, social, and legal consequences of breach are the main reasons contracts are performed. Thus, security in transactions means the knowledge that transactions will be performed as expected and the stability and certainty that come with that knowledge. Risk management, the ability to assess the possibilities and risks of non-performance and to take the steps necessary and appropriate to encourage performance or guard against breach, is a key ingredient.[21]

In the electronic environment, what is arguably lacking at the moment is a discernable legal and social structure that allows the parties to adequately assess the risks of electronic commerce and to respond by making intelligent choices concerning their own rights and liabilities, including allocation of risks in transactions with others. For example, without an appropriate legal structure that recognizes and validates electronic commerce, the presence of all the encryption or authentication devices in the world will not give businesses the security they need to conduct business in the electronic environment. The legal structure must include laws recognizing the ability to contract electronically, enforcing deals entered into electronically, and setting forth the rules applicable to the transaction while recognizing the power of the parties, within reason, to set the terms as between themselves and choose the applicable law. This type of security—"legal security"—flows from a legal framework, one that may, to a large extent, already exist, but to the extent the application of that framework in the online environment is less than clear, the resulting sense of security may be impaired. It must be recognized, however, that "legal security" is only part of the overall "security" picture.

21. A companion to the concept of "security" is that of "trust": the argument is that systems, both legal and technological, need to be created which people may trust. Again, trust has many meanings. To some, "trust" in electronic transactions may mean "I can count on this transaction being enforced." Alternatively, the trust issue may be expressed as "I can count on that this transaction will be carried out." A third possible phrasing: "I can trust the parties to and persons involved in the transaction." And last: "I can trust that the systems themselves are 'trustworthy.'" Thus, you may have trust in the legal structure supporting the transaction, trust in the parties to the transactions, trust in the performance of the transactions themselves, without regard to legal enforcement, and trust in the systems. There are, additionally, a variety of sources for "trust:" knowledge, experience, familiarity, and authority.

The desire for "security" has manifested itself in online commerce in somewhat traditional ways. Early on, in the absence of legislative and judicial recognition and validation of electronic commerce and the corresponding lack of industry-wide standards, customs, or standards to guide conduct, attempts were made to set the rules for electronic commerce through "trading partner agreements" between the parties doing business electronically.[22] Numerous regional and national model trading partner agreements, or interchange agreements, were developed to provide commerce with a contractual framework for facilitating the adoption and use of electronic commercial practices, thereby providing the parties with some degree of certainty as to the terms applicable to their transactions. Although there are differences between the various proposed interchange agreements, a key ingredient of virtually all of them was the parties' articulation of the technological security measures to be employed in transacting business electronically, and delineation of the circumstances under which each party would be bound by messages purportedly originated by that party.[23]

In situations where the parties were not in prior contact or direct contact, or where the transactions were such that prior negotiation of such agreements was impossible or impractical, alternative contractual models were adopted. One tactic is the articulation by one of the parties to the contract of the applicable terms, e.g., by posting of the terms on the relevant

22. "The idea of a model interchange agreement was first raised at the international level by the Nordic Legal Community in the early 1980s." Amelia H. Boss, *Electronic Data Interchange Agreements: Private Contracting Toward a Global Environment,* 13 NW. J. INT'L L. & BUS. 31, 38 (1992). In turn, the idea spread, and during the 1980s and early 1990s, there was a proliferation of "model interchange agreements" produced by EDI user groups representing specific industries by electronic data interchange associations, attorney groups, government agencies, and international organizations. *Id. See also* Amelia H. Boss & Jeffrey B. Ritter, ELECTRONIC DATA INTERCHANGE AGREEMENTS: A GUIDE AND SOURCEBOOK (1993). In the United States, such a model interchange agreement was proposed by a group within the American Bar Association. *See* The Electronic Messaging Services Task Force, *The Commercial Use of Electronic Data Interchange—A Report and Model Trading Partner Agreement,* 45 BUS. LAW. 1645 (1990).

23. Many of the following issues are addressed in those agreements: selection of EDI messages, message standards, and methods of communication; responsibilities for ensuring that the equipment, software, and services are operated and maintained effectively; procedures for making any systems changes which impair the ability of trading partners to communicate; security procedures and services; the points at which electronic messages have legal effect; the roles and contracts with any third party service providers; procedures for dealing with technical errors; the needs, if any, of confidentiality; liabilities in the event of any delay or failure to meet agreed EDI communications requirements; the laws governing the interchange of EDI messages and the arrangements of the parties; and methods for resolving any potential disputes. *See* Boss, *supra* note 22; Boss and Ritter, *supra* note 22.

website [24] or by postings stating that any transactions were to be governed by a given set of practices.[25] A variation of this type of contract was the development of operating rules within defined systems that purport to bind all participants in the system.[26] Establishment of voluntary "codes of conduct"[27] and the development of industry standards[28] are two other options

24. The desires of commercial parties to govern online transactions by posting, or having available on a website, the terms and conditions that purport to cover the transactions entered into on the website have led to the use of what have been called "click-wrap" or "shrink-wrap" licenses. Questions as to the enforceability of such terms and conditions have in turn given rise to litigation. Step-Saver Data Sys. v. Wyse Tech., 939 F.2d 91, 103 (3d Cir. 1991); ProCD Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996); Vault Corp. v. Quaid Software Let., 847 F.2d 255, 258 (5th Cir. 1988). They have also stimulated efforts to address such terms on the state level, the national level, and the international level, amidst considerable controversy. For an overview of the range of reactions to these issues, see Symposium, *Intellectual Property and Contract Law in the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Transactions in Information and Electronic Commerce*, 13 BERKELEY TECH. L.J. 809 (1998); Symposium, *Intellectual Property and Contract Law for the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Information and Commerce*, 87 CAL. L. REV. 1 (1999). *See also* Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239 (1995); Apik Minassian, *The Death of Copyright: Enforceability of Shrinkwrap Licensing Agreements*, 45 UCLA L. REV. 569 (1997); Jennett M. Hill, Note, *The State of Copyright Protection for Electronic Databases Beyond ProCD v. Zeidenberg: Are Shrinkwrap Licenses A Viable Alternative for Database Protection?*, 31 IND. L. REV. 143 (1998); Joseph C. Wang, Note, *ProCD, Inc. v. Zeidenberg and Article 2B: Finally, the Validation of Shrink-Wrap Licenses*, 16 J. MARSHALL J. COMPUTER & INFO. L. 439 (1997); Christopher L. Pitet, Note and Comment, *The Problem With "Money Now, Terms Later": ProCD, Inc. v. Zeidenberg and the Enforceability of "Shrinkwrap" Software Licenses*, 31 LOY. L.A. L. REV. 325 (1997); Thomas Finkelstein & Douglas C. Wyatt, Note, *Shrinkwrap Licenses: Consequences of Breaking the Seal*, 71 ST. JOHN'S L. REV. 839 (1997).

25. In the case of providers of certain services, this was accomplished through the development of statements of practice, such as the certification practice statements used by certification authorities in the context of digital signatures. *See, e.g.*, the certification practice statements published on the Internet by GTEI–CyberTrust, <http://www.bbnplanet.com/products/security/cytrust/cps.htm>; True Trust Limited <http://fw4.iti.salford.ac.uk/truetrust/cps/>; and Verisign http://www.verisign.com/ repository/CPS/>.

26. An example is the system rules for international inter-bank transfers, established by the Society for Worldwide Interbank Funds Transfers ("SWIFT").

27. In 1987, the International Chamber of Commerce took the first step by developing and producing the Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission (ICC Publication no. 452). The UNCID rules, the first product in this area, were aimed at facilitating the interchange of trade data effected by teletransmission through the establishment of agreed rules of conduct between parties engaged in such transactions. The UNCID rules were not self-executing but voluntary, requiring the agreement of the parties to incorporate its terms in their own relationship. *See* The Working Party on Facilitation of

that have been explored. One current project proposes to establish a common set of legal "Eterms" which can be incorporated by parties into their electronic messages, thereby providing the private legal structure to guide the transaction.[29] In addition, there has been a move to provide certainty through the use of choice of law and forum clauses and a corresponding desire to strengthen the enforceability of such clauses in electronic commerce[30]

In 1997, the White House issued its report, A Framework for Global Electronic Commerce,[31] which set forth the administration's policies with regard to the law of the Internet. The administration firmly emphasized that in the area of electronic commerce, the private sector should lead, and government regulation should be discouraged. Governments were urged to avoid undue restrictions on electronic commerce and at the same time encouraged to allow new business models and products to evolve. If and when government intervention is deemed necessary to facilitate electronic commerce, the administration cautioned that the government's "aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce."[32]

The White House recognized that despite the preferability of private sector leadership, there might be a need to draft rules governing global electronic commerce. In that regard, it urged the elimination of administrative and regulatory barriers to commerce and the recognition of certain fundamental principles. The primary principle is, of course, freedom of contract, the ability of "fully informed buyers and sellers" to set their own rules. Equally important, the administration urged that any legislation or rules be "technology neutral," i.e., the rules should neither require nor

---

International Trade Procedures, *UN/ECE Trade Facilitation Recommendation No. 26* (March 1995) <http://www.unece.org/trade/rec/rec26en.htm>.

28. *E.g.*, in the context of digital signatures, concerns about certification services and the fear that the public would be misled has led to exploration of the establishment of private systems for accreditation of certification authorities according to preestablished industry standards. Charles R. Merrill, *The Accreditation Guidelines-A Progress Report on a Work in Progress of the ABA Information Security Committee*, 38 JURIMETRICS J. 345, 347–48 (1998) (detailing accreditation guidelines' project and need for developing standards of trustworthiness).

29. *See* Andreas Mitrakas & Janjaap Bos, *The ICC ETERMS Repository to Support Public Key Infrastructure*, 38 JURIMETRICS J. 473 (1998).

30. *See* Boss, *supra* note 9.

31. *See* William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* <http://www.iitf.nist.gov/eleccomm/ecomm.htm>.

32. *Id.* Two other principles were also iterated: that governments should recognize the unique qualities of the Internet and that electronic commerce should be facilitated on a global basis.

assume a particular technology and be flexible enough to permit the development of new technologies in the future.[33]

In recognizing the need for legislation, and at the same time urging a minimalist approach, the White House report reflected discussions in business, academic, and political circles over the past several years. These discussions, however, revealed two distinct approaches, with distinct policy recommendations and legislative proposals flowing from them. These need to be examined in more detail.

III. THE DEBATE: A CONFLUENCE OF TWO STREAMS

The advent of electronic communications technologies and electronic commerce has, over the years, given rise to two distinct movements with regard to law reform, each with its own set of adherents.

Initially, concerns about electronic commerce focused on existing legal structures and principles. The main concern was the application of existing law to transactions entered into electronically. Attempts were made to identify existing barriers to electronic commerce and to determine the extent to which modification of these and other general transactional rules were required in an electronic environment. On the international level, the notion that governments should review legal requirements governing trade and commerce to determine their suitability for electronic commerce surfaced over fifteen years ago.[34] Domestically, the need to review existing laws has been recognized on both the federal[35] and state levels. Those approaching these issues tended to view the question as follows: what changes are

33. A concept related to that of "technology neutrality" is that of "implementation neutrality," the recognition that any rules or laws neither assume nor require the implementation of certain technology in preset ways. A third concept is neutrality, seeking an equivalence between transactions regardless of the medium used for communication. The basic goal of all these efforts is that the law should not discriminate between information on paper and information in electronic form.

34. The removal of legal barriers to electronic commerce became an international issue as early as 1985, when the United Nations Commission on International Trade Law ("UNCITRAL") called upon all governments to "review legal requirements of a handwritten signature or other paper-based methods of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication." U.N. GAOR, 40 th Sess., Supp. No. 17, at 72, U.N. Doc. (A/40/17).

35. *See, e.g.*, Matter of National Institute of Standards and Technology-Use of Electronic Data Interchange Technology to Create Valid Obligations, Dec. of the Comp. Gen. Of the U.S., File B-245714 (Dec. 13, 1991) <http://www.softwareindustry.org/issues/docs-org/cg-opinion.pdf> ("Contracts formed using Electronic Data Interchange Technologies may constitute valid obligations of the government for purposes of 31 U.S.C. § 1501, so long as the technology used provides the same degree of assurance and certainty as traditional 'paper and ink' methods of contract formation.").

necessary, in the area of commercial law, evidence, etc., to accommodate electronic commerce. Attempts to accommodate electronic commerce focused on the adaptation of the traditional transactional rules. The goal was to assure that electronic commerce was not discriminated against solely because of the medium in which it occurred.

For example, the law has traditionally required "writings" and "signatures" as a prerequisite for the enforcement of many transactions,[36] and the application of those requirements to electronic commerce has been problematic. The legislative response, at least within the context of commercial law,[37] was twofold: either to eschew the terms "writing" and "signature" in new legislation in favor of terms such as "record" and "authentication,"[38] or to provide affirmatively that existing writing and signature requirements could be met by electronic messages.[39] Most of these changes occurred within the context of more generalized substantive revisions of commercial law aimed at updating and modernizing commercial law to accommodate electronic commerce.

By contrast, a second movement started *not* with a focus on existing law, but rather with a focus on technology and its implementation. Concerns about security motivated members of the digital community to begin

---

36. This, of course, is the notion behind our statute of frauds, which dates back to the adoption by the British Parliament of the first such statute in 1677. Since then, the writing requirement of the statute of frauds has been adopted with some modification in nearly all of the United States. Subject to several exceptions, the statute provides that no suit or action may be instituted under certain categories of contracts unless that contract is written and signed by the party to be charged. *See generally* James J. White & Robert S. Summers, UNIFORM COMMERCIAL CODE §§ 2-1 to 2-12 (3d ed. 1988). However, the British Parliament repealed its statute of frauds in 1954. *Id. See also* R. J. Robertson, *Electronic Commerce on the Internet and the Statute of Frauds*, 49 S.C. L. REV. 787 (1998).

37. The legislative response was actually preceded by a contractual response by the parties to the transaction. *See supra* notes 21–29 and accompanying text.

38. The term "record" was developed over time expressly to deal with electronic records and had been developed and refined by the American Bar Association and the National Conference of Commissioners on Uniform State Laws as a generic term for use throughout proposed legislation. It has since become standard language in products of the National Conference of Commissioners on Uniform State Laws. *See* Patricia B. Fry, *X Marks the Spot: New Technologies Compel New Concepts for Commercial Law*, 26 LOY. L.A. L. REV. 607 (1993) (detailing history of the concept of "record"). *See also* U.C.C. §§ 5-102(14), 5-104, & 8-113 (using the term "record"); §§ 5-104, 8-113 (using the term "authenticate").

39. *See, e.g.*, Uniform Electronic Transactions Act § 106(c) (Proposed Draft Jan. 29, 1999) ("If a rule of law requires a record to be in writing . . . an electronic record satisfies the rule of law."); *id.* § 106(d) (Proposed Draft Jan. 29, 1999) ("[i]f a rule of law requires a signature. . ., the rule of law is satisfied with respect to an electronic record if the electronic record included an electronic signature."). *Compare* UNCITRAL Model Law on Electronic Commerce, Articles 6 (writing), and 7 (signature).

exploration of technological means of providing security to participants in electronic commerce. Three issues were identified as "security" risks: 1) authenticity—the problem of identifying the source or sender of a message and authenticating that it did indeed come from that sender; 2) integrity—the problem of proving that the message is complete and has not been altered since it was sent; and 3) non-repudiation—the risk that the sender may repudiate it after receipt.[40]

One technology, digital signatures, quickly became the "favorite" among many technology afficionados, who claimed it offered a technology-based cure for many of the security risks encountered in online commerce. In many regards, the description of the technology as "digital signatures" is a misnomer. In essence, what is being advanced is a method of encryption—or more appropriately, dual key encryption using two mathematically related numbers, or keys.[41] Each key pair consists of two keys: a person's private key, which is kept private, and the public key which can be made publicly available. When the private key is applied to a message, the message is transformed or encrypted, and a string of numbers is created, the "digital signature" for that message, which is unique to both the key used to encrypt and to the message itself. The recipient of that message can, by using the public key corresponding to the key used by the sender, determine whether the message was sent by the person holding that corresponding private key and determine whether the message had been altered since it was made.[42]

---

40. Although "non-repudiation" is often referred to as a desirable attribute of security procedures, a persuasive argument has been made that whether a person may repudiate a message is actually a legal construct related to the question of the message's authenticity. John D. Gregory, *Solving Legal Issues in Electronic Commerce*, CAN. BUS. L.J. (forthcoming 1999).

41. Although the two numbers are mathematically related, in theory it is computationally infeasible to ascertain what is known as the "private key" of the sender using the "public key" applied by the recipient to unlock the message. If the key utilized is sufficiently long, it would apparently take "extremely powerful computers [many] years and millions of dollars, to crack a single public/private key pair." Greenwood & Campbell, *supra* note 6, at n.14.

42. Thus, "digital signatures" have been defined as:

> [A] transformation of a message using an asymmetric cryptosystem such that a person having the intitial message and the signer's public key can accurately determine whether:
>
> (a) the transformation was created using the private key that corresponds to the signer's public key; and
>
> (b) the message has been altered since the transformation was made.

UTAH CODE ANN. § 46-3-103(10) (1998). For a good tutorial on digital signatures, see <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>. *See also* Information Security Committee, Section of Science and Technology, American Bar Association, *Public Key Infrastructure Symposium-Tutorial*, 38 JURIMETRICS J. 243 (1998).

One major obstacle to the easy use of this technology is assuring the potential recipient of a message, and user of one-half of the key pair, of the identity of the holder of the other key. In situations where the two parties know one another and can directly exchange keys, there is no problem. In systems such as on the Internet where the parties do not necessarily know each other, identity of the holder of a private key is an issue. To resolve this problem, industry has proposed an implementation of dual key encryption which involves the creation of a "public key infrastructure," or PKI, under which a third party, known as a certification authority, or CA, has the task of verifying the identity of the holder of a key and that the key being used by the recipient is the reciprocal of the key used by the sender.[43]

Supporters of the technology began to develop various models—public key infrastructures—for the use of digital signatures in commerce.[44] In large part, the development of these models involved decisions as to the appropriate business structures to use for electronic commerce. Moreover, the creation of new public key infrastructures raised interesting issues about the relationship between the various parties in the structure. In attempts to resolve these relationship issues and to encourage use of the technology, supporters began to advance the notion that a new legal structure was necessary to promote and facilitate the development of public key infrastructures. As a result, the proponents, concerned primarily with advancing the technology and its business implementations, are now advancing a legal construct to support and promote their specific implementation models.[45]

---

43. This explanation is obviously very simplified. Assume that a message purports to come from Bill Gates and is "digitally signed." The recipient will first want to know that the key it applies to the message is indeed the reciprocal to one held by Bill Gates. Second, it will want to know that the person who obtained the key using the name "Bill Gates" was indeed Bill Gates. Third, the recipient will want to know that the person who actually *used* the key was either Bill Gates or someone acting with authority for Bill Gates.

44. Interestingly, the implementation models that have been advanced have changed over time. Initially, for example, it was contemplated that certification authorities would provide "certificates" directly to the holders of private keys and that the key holders would then use these certificates in communications with others. As the various models have developed over time, however, it appears to be more common for the certification authority to supply the certificate *not* to the key holder but to the relying party, the recipient of the message who wants to verify the identity of the key holder.

45. As one proponent of such legislation has stated:

> [I]t is our desire to make current technology more available and more useful for real-world applications. This can be done by objectively reviewing what the various available technologies can do, grouping them according to their attributes of security, reliability, scalability, and so on, *and creating legislative constructs (including for self-regulation) appropriate to each technology.*

In 1995, Utah, the home to high technology companies with an interest in the topic, followed by Minnesota[46] and Washington,[47] became the first to enact a digital signature statute setting forth specific rules governing digital signatures and public key infrastructures.[48] The main characteristic of this legislation is its regulatory nature, providing for a licensing scheme for certification authorities.[49] Licensed certificate authorities under the statutes are given significant limitations on their liability to other parties within the public key infrastructure.[50] Indeed, it can be argued that the primary purpose behind the legislation is this limitation of liability, and that the licensing regime serves that limitation. The liability scheme was seen as necessary to assure commercial developers "that the risks of potential liability to users of the system could be kept within tolerable limits."[51] Although the statutes also attempted to address the rights and responsibilities of other participants in the public key infrastructure, only a small portion of the digital signature statutes pertains to the *legal effect* to be given to the use of the digital signature. These statutes frequently went further than saying that a person may use a digital signature and effectively meet any writing or signature requirements. Consistent with the philosophy of attempting to provide a comprehensive scheme to apportion all liability of the parties, these laws provided that where a digital signature was accompanied by a verifiable certificate issued from a certification authority licensed under the statute, it was entitled to the presumption that it was affixed by the holder of the

---

Michael S. Baum, *Technology Neutrality and Secure Electronic Commerce: Rule Making in the Age of "Equivalence"* at 4, n.5 (1998) <http://www.verisign.com/repository/pubs/tech_neutral/> (emphasis added). Reviewing and grouping may perform wonderful services to businesses attempting to implement electronic commerce, allowing parties to choose the attributes of security important to them. Whether legislation and new legal constructs are needed to facilitate those choices is a different issue.

46. *See* UTAH CODE ANN. tit. 46, Ch. 3 (1996).

47. Minnesota Electronic Authentications Act, MINN. STAT. ANN. § 325 (West 1998) <http://www.revisor.leg.state.mn.us/stats/325K/>.

48. Washington Electronic Authentications Act, WASH. REV. CODE ANN. § 19.34 (West 1998) <http://www.wa.gov/sec/dsrcq.htm>.

49. For example, the Utah statute confers authority on a state agency to license certificate authorities that operate within their jurisdiction. UTAH CODE ANN. §§ 46-3-201–204 (1998).

50. *See, e.g., id.* § 46-3-309 (limiting liability of certification authority to amount it includes in its certificate and specifically excluding consequential damages).

51. Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1241 (1998). "This limit on the potential liability of the [Certificate Authority] to subscribers and relying parties, above and beyond any liability that it has expressly undertaken and set forth in its certification practice statement, is a pivotal risk allocation rule." *Id.* at 1242.

private key and was therefore attributable to it.[52] Although these signing and attribution provisions were only a part of a larger digital signature statutory scheme, they overlapped with the efforts begun earlier to define signing and attribution in the commercial context.

In effect, these two separate movements, one with its origins in the law, the other with its origins in the technology, represent two philosophies. The first, which began with a concentration on commercial law issues, has focused on keeping commercial laws generic and supportive. The goals have been to remove barriers to electronic commerce, treat electronic communications on a par with paper communications, and not to favor one technology over another (technology neutrality) nor one business model over another (implementation neutrality). As between different technologies or implementation schemes, the choice was to be that of the parties. This approach exhibits a degree of confidence in the marketplace to make suitable options available to parties, allowing them to make intelligent choices. The second movement has the philosophy—and the express goal—of supporting and promoting specific technologies, or, more correctly, one specific technology and one implementation model. The theory is that the technology and implementation offer such benefits to the users of the Internet that legislation should recognize those benefits and enshrine them in the law. Despite their different orientations, both movements ended up dealing with the same issue: the satisfaction of legal requirements of writings and signatures through technological means in an electronic environment.

At the outset, the two movements were relatively separate; those revising the commercial laws and those building PKI infrastructures represented two different constituencies: law revisionists and technology supporters. To a large extent, however, the "digital signature" movement was the more visible of the two. Commercial law does not tend to have inherent appeal to either the public or to legislators. On the other hand, mere mention of certain buzzwords, such as "Internet," "security," or "technology," immediately piques the interest of both the public and the legislature. Among the public, the digital signature movement quickly gained two distinct bodies of followers. The first consisted of those who saw digital signatures as the answer for Internet security.[53] Because of their belief in the security aspects of digital signatures, the desire was to build a structure, a business structure as well as a legal structure, to support the technology. The second body of followers were those business people attracted to the digital signature movement not because of any interest in the

52. UTAH CODE ANN. § 46-3-406 (1998).

53. Some of these participants were in fact representing businesses that were marketing digital signature technology; others were simply focused on the merits of the technology.

technology itself but because of concerns about the ability of the law in its current state to recognize and validate online business transactions. Their desire to gain legal recognition of electronic communications contributed to their support for digital signature legislation. That support, driven out of a desire to establish the validity of electronic commerce, was given in the absence of a recognition that other efforts would establish that validity without the need for a complicated, legal, and regulatory structure for digital signatures.

Ultimately, the law revision and technology "movements" joined issue on the question of the legal effects to be given to certain uses of the technology to "sign" or otherwise authenticate messages. In one regard, the dispute is between the "removal" of barriers to electronic commerce through the development of generic rules and the "support and promotion" of electronic commerce through the creation of rules geared to promoting its use. In another regard, the dispute is whether specific types of technology implementations should be given special treatment under the law.

IV. SURVEYING THE BATTLE FRONT

The war between the law revision and technology movements is being waged on many simultaneous fronts: within the individual states, at the federal level in Congress, at the uniform law level within the United States, at the national level abroad, and on the international level as well. On the individual state level, state legislatures have acted in a variety of ways to accommodate electronic commerce, but four patterns of statutes have emerged over time, reflecting the influence of the two movements. Initially, Utah was the first state to adopt a full-fledged digital signature statute supporting a public key infrastructure,[54] legislation which was based on efforts of the American Bar Association's Information Security Committee, which published a set of *Digital Signature Guidelines*.[55] The approach used by Utah and the *Digital Signature Guidelines*, however, of setting forth a highly structured, prescriptive, regulatory environment only for digital signatures, has not been widely followed by the states.[56] California quickly

54. *See* UTAH CODE ANN. § 46-3-101 (1996). The 1996 legislation was a revision of legislation which originally became effective in 1995.

55. ABA COMM. ON INFORMATION SECURITY, *Digital Signature Guidelines* (1996). It is interesting to note that, while the *Guidelines* were developed within a committee of the American Bar Association, that committee consisted of a substantial number of individuals who were not lawyers but were drawn from various segments of the technology industry.

56. For an excellent survey, see Internet Law and Policy Forum, *Survey of State Electronic & Digital Legislative Signature Initiatives*, submitted Sept. 12, 1997 <http://www.ilpf.org/digsig/digrep.htm>, *updated*, Internet Law and Policy Forum, *UPDATE: Survey of State Electronic & Digital Signature Legislative Initiatives*

followed on the heels of Utah by enacting legislation that did not follow the Utah statute in its adhesion to public key cryptography. Rather, it drafted a technology-neutral law.[57] It provided that an electronic signature[58] would have the same legal effect as a manual signature if it has these attributes: it is unique to the person using it, it is capable of verification, it is under the sole control of the person using it, it is linked to the data in such a manner that, if the data are changed, the electronic signature is invalidated, and it conforms to regulations adopted by the Secretary of State.[59] Later regulations permitted either digital signature using a certification authority or signature dynamics.[60] The California approach has proven to be more popular in the United States than the Utah focus on digital signatures alone.[61] While it is more generalized, a person using a certain security procedure must demonstrate that either it fits within the regulations or within the generalized criteria set forth in the statute before the digital signature is given effect.

Florida followed a third approach when, in 1996, it enacted the Electronic Signature Act.[62] Florida represents the enabling approach, emphasizing the elimination of artificial barriers to electronic commerce. Under the Act, the term "writing" is defined to include information created or stored in any electronic medium that is also retrievable in perceivable form.[63] Any such writing containing an electronic signature, defined to include any letters, characters, or symbols, manifested by electronic or

---

<http://www.ilpf.org/digsig/UPDATE.HTM>. Another source of current information on state and other legislation is the McBride Baker Coles site, <http://www.mbc. com/>.

57. California was influenced, in part, by international legislation, the Model Law on Electronic Commerce, being drafted by the United Nations Commission on International Trade Law. *See supra* note 6.

58. California used the expression "digital signature" to cover more than just signatures using public key cryptography. To avoid confusion in the text, the term "electronic signature" is used to emphasize that the legislation applies to any signatures in electronic form, whether or not they are technically dual key encryption "digital" signatures.

59. *See* CAL. GOV'T CODE § 16.5 (West 1995). The first four criteria were first established in a decision of the Comptroller General of the United States in *Matter of National Institute of Standards and Technology (NIST)—Use of Electronic Data Interchange Technology to Create Valid Obligations*, Comp. Gen. File VB-245714 (Dec. 13, 1991) <http://www.softwareindustry.org/issues/docs-org/cg-opinion.pdf>.

60. Signature dynamics is associated with PenOp, a system of signing manually using computer-recorded strokes. *See* PenOp, *Welcome to PenOp, the World's Leading Electronic Handwritten Signature* <http://www.penop.com/>.

61. *See* ILPF Survey, *supra* note 57.

62. Electronic Signature Act of 1996, 1996 Fla. Laws ch. 96-224 (codified as amended at FLA. STAT. § 282.72 (1996)).

63. This formulation tracks the definition of a "record" in uniform legislation proposed by the National Conference of Commissioners on Uniform State Laws. *See supra* note 39.

similar means, with intent to authenticate a writing, may be used to sign a writing and is given the same force and effect as a written signature. This enabling approach has become increasingly popular among the states that have considered the question.[64] It does not require an extensive set of regulations, does not set forth specific technologies and implementations that it sanctions, nor does it set forth "criteria" for judging whether electronic signatures will be given legal effect.

A fourth approach developed in Illinois as a "middle ground" between digital specific statutes and mere enabling statutes: the concept of a hybrid statute that enabled the use of electronic signatures by validating their use, but at the same time recognized a category of "secure electronic signatures."[65] Anyone may use an electronic signature in electronic commerce and be assured that legal writing and signature requirements are no obstacle. However, if a signature qualifies as a secure electronic signature by meeting criteria similar to that found in the California statute, rebuttable evidentiary presumptions arise as to the authenticity and integrity of the signature.

The lack of uniformity among the various state enactments has led to activity on two fronts. Pressure is being placed on Congress to take action, both from the fear that states will delay in responding to the needs of electronic commerce and from the fear that their responses will be non-uniform in character. Thus, the push is on to: 1) develop standards for use of electronic and digital signatures in transactions with the government; 2) develop a federal standard for recognition of electronic and digital signatures; and 3) preempt state law. Several bills have been introduced over the past few years to deal with electronic commerce, although none have yet been enacted. The scope and approach of the proposed legislation has differed drastically. At one end of the spectrum is proposed legislation merely giving effect to "electronic signatures" as a method of signing;[66] this type of legislation would best be characterized as enabling legislation. Other proposed legislation, within the banking context, proposed to validate "secure" electronic techniques of authentication adopted pursuant to agreement or system rules;[67] to the extent this legislation would merely

64. ILPF Survey, *supra* note 57.

65. The Illinois statute was enacted in 1998. 205 ILL. COMP. STAT. § 705/10 (West 1998).

66. *See* Government Paperwork Elimination Act of 1998, S. 2107, 105th Cong. (1998) (sanctioning electronic signing of forms submitted to federal agencies); Paperwork Elimination Act of 1999, H.R. 439, 106th Cong. (1999) (following Government Paperwork Elimination Act); Millennium Digital Commerce Act, S. 761, 106th Cong. (1999).

67. The Digital Signature and Electronic Authentication Law of 1998, S. 1594, 105th Cong. (1998) (validating electronic authentication under relevant "agreements" or "system

reinforce the ability of the parties to govern their transactions by agreement, it would be consistent with an enabling and validating approach. A bit further down on the scale is proposed legislation providing that close-up electronic signatures meeting certain criteria are acceptable as signatures.[68] To the extent that legislation begins to set additional hurdles for electronic commerce, it begins to move from merely enabling and starts to introduce a channeling function—that of telling businesses what technologies they should adopt. One piece of proposed federal legislation, in the context of federal tax filings, would create a presumption that the person on whose behalf a return was filed did indeed subscribe to and submit the return.[69] As will be discussed below, presumptions have become a fertile battleground on the uniform law level; this proposed federal legislation, however, deals solely with communications, i.e., tax filings, with the government and relieves the Internal Revenue Service of proving in each instance that a particular taxpayer did indeed file the return under consideration. The proposed bill that goes the furthest in establishing a more regulatory approach would establish a federal panel to develop a national digital signature infrastructure.[70]

The primary thrust of the federal push is the need for immediate uniform national legislation. There are other efforts on a state-by-state basis that should fill that need. The National Conference of Commissioners on Uniform State Laws will be taking final action in July 1999 on two pieces of proposed uniform legislation that will address the concerns of at least those who want to validate and enforce electronic transactions by removing

---

rules" and authorizing their use by financial institutions pursuant to agreement or pursuant to a "banking, financial, or transactional system using electronic authentication").

68. Electronic Financial Services Efficiency Act of 1997, H.R. 2937, 105th Cong. (1997) (stating all forms of electronic authentication meeting certain standards "shall have standing equal to paper-based, written signatures"). Those standards are: 1) the identification method be unique to the person sending the communication; 2) the identification technology be capable of verification; 3) the identification method be under the sole control of the person using it; and 4) that the identification method be linked to the data in such a way that if the data is altered, the authentication becomes invalid. *Id.* This follows the approach begun in the California legislation—borrowing the standards from NIST, *supra* note 36, and subsequently picked up in several states.

69. Internal Revenue Restructuring and Reform Bill of 1997, H.R. 2676, 105th Cong. (1997) (sanctioning tax returns filed electronically and stating that any return filed electronically shall be presumed to have been submitted and subscribed to by the person on whose behalf it was filed).

70. Computer Security Enhancement Act of 1997, H.R. 1903, 105th Congress (1997) (also authorizing National Institute of Standards and Technology to assist private sector in developing voluntary standards and guidelines for a public key infrastructure).

barriers to electronic commerce.[71] Driven in large part by concerns about nonuniformity among the states, these efforts have benefitted greatly from the "experimentation" that has already occurred on the state level. The need for uniformity should be achieved, without federal preemption, if either of these measures gain sufficient enactment by the states.[72]

On the international scale, a similar pattern is beginning to emerge, although developments internationally are lagging somewhat behind those in the United States. Following the lead of Utah, and inspired in large part by the *Digital Signature Guidelines,* several countries, including Germany,[73] Italy,[74] Malaysia,[75] and Argentina,[76] have enacted legislation relating to electronic authentication and adopting to some degree the approach pioneered by Utah. By contrast, Singapore has adopted an approach loosely based on the Illinois hybrid approach, drawing a distinction between electronic signatures on the one hand, which it enables, and secure electronic records and signatures on the other, including digital signatures.[77] Similarly taking a hybrid approach is the recently released EU Directive on Digital Signatures[78] and several drafts considered by the United Nations Commission on International Trade Law.[79]

---

71. *See supra* note 5 and accompanying text.

72. Indeed, recent federal legislation would *not* preempt state laws in those states that have enacted uniform state law such as the Uniform Electronic Transactions Act. *See* Millennium Digital Conference Act, 1999 S. 761 (Mar. 26, 1999), section 6(c).

73. German Digital Signature Law (Aug. 1, 1997) <http://www.iid.de/rahmen /iukdgbt.html>, *available in English at* <http://www.kuner.com/data/sig/digsig4.htm>.

74. *See* Italian Law N. 59, Art. 15, c. 2 (enacted Mar. 15, 1997), *available in Italian at* <http://www.interlex.com/testi/attielet.htm>, and regulations promulgated Nov. 10, 1997 (Presidential Decree No. 513), *available in Italian at* <http://www. notariato.it/forum/dpr_513.htm> .

75. *See* Malaysia Digital Signature Act, Law No. 59 of 15 Mar. 1997 <http://www.mycert.mimasmy/digital.html.>.

76. Legislation has also been passed in Italy. Argentina has also adopted digital signature legislation by presidential decree. Presidential Decree No. 427/98 <http://www.sfp. gov.ar/firma.html>, *available in English at* <http://www.sfp.gov.ar/decree427.html>.

77. Singapore Electronic Transaction Act (adopted June 29, 1998), *available at* <http://www.ech.ncb.gov.sg/>.

78. European Commission, *Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures* (May 13, 1998) <http://www.ispo. cec.be/eif/policy/com98297.html>. The articulated goal of the directive was to "[ensure] the proper functioning of the Internal Market in the field of electronic signatures by creating a harmonized and appropriate legal framework for the use of electronic signatures within the [European] Community and establishing a set of criteria which form the basis for legal recognition of electronic signatures." *Id.*

79. *See* the Preparatory Documents for the UNCITRAL Working Group on Electronic Commerce <http://www.un.or.at/uncitral/>. For many years, UNCITRAL adhered to the

Several other nations, however, have refused to legislate detailed standards for the use of different authentication techniques or one particular technique, urging instead a simple enabling approach. In March 1998, the Australian Electronic Commerce Expert Group issued its report on the laws of electronic commerce, in which it concluded:

> It is our view that the enactment of legislation which creates a detailed legislative regime for electronic signatures needs to be considered with caution. There is the risk, particularly given the lack of any internationally uniform legislative approach, that an inappropriate legislative regime may be adopted without regard to market-oriented solutions. Given the pace of technological development and change in this area, it is more appropriate for the market to determine issues other than legal effect, such as the levels of security and reliability required for electronic signatures. Accordingly, we have recommended that legislation should deal simply with the legal effect of electronic signatures. While a number of articles in the Model Law deal with electronic signature issues that go beyond legal effect, it is our view that these issues should be left to the existing law in Australia. Whether the existing Australian law deals with these issues adequately or not, the same situation should apply to both paper based commerce and electronic commerce. At this stage we are not persuaded of the need to give a legislative advantage to electronic commerce not available to traditional means of communication. If a clear need to deal with these issues appears in the future the recommended legislation can be amended.[80]

Similarly, the New Zealand Law Commission, in its October 1998 report on Electronic Commerce, rejected the approach of technology specific legislation as found in Utah and Germany and adopted as one of its guiding

---

notion that it was important to maintain technology in its rules, and therefore pursued the dual approach. At its February 1999 meeting, however, the Working Group backed away from the attempts to develop a "media neutral" set of rules and opted for the moment to pursue development of public key infrastructure ("PKI") or digital signature specific rules.

80. Australian Electronic Commerce Expert Group, *Electronic Commerce: Building the Legal Framework*, Executive Summary <http://www.law.gov.au/aghome/advisory/eceg /summary.html>. Legislation has since been proposed which would follow the provisions of the UNCITRAL Model Law and therefore have no special recognition given to digital signatures nor any presumptions attaching beyond those provided for in the Model Law. *See Australian Draft Electronic Transactions Bill* <http://law.gov.au/ ecommerce/>.

principles "technological neutrality."[81] The Law Commission recommended merely that legislation be passed to ensure that electronic signatures would be acceptable under law.[82]

V. ENABLING VERSUS PROMOTING: THE DEBATE IN THE UNIFORM LAW PROCESS

The debate within the uniform law process, as it is currently proceeding, highlights the controversy between those who view the appropriate role of law revision as simply removing barriers to electronic commerce—with the marketplace providing other necessary incentives and support—and those who feel that security on the Internet is and should be promoted by legislation that gives advantages to those who adopt the appropriate technology. In August of 1999, the National Conference of Commissioners on Uniform State Laws will be presented with two pieces of proposed uniform legislation: a new Uniform Electronic Transactions Act ("UETA")[83] and an addition to the Uniform Commercial Code, Article 2B, that deals with computer information transactions.[84] Despite the worthy goal of uniformity and the original mandate to the drafting committees to be consistent, these two products are not uniform in their treatment of security procedures and their use. Indeed, their lack of uniformity exemplifies the tension between those dedicated to removing barriers to electronic commerce and those wishing to support and promote by creating confidence in the systems themselves.

VI. UNIFORM ELECTRONIC TRANSACTIONS ACT

The Uniform Electronic Transactions Act Drafting Committee, created in 1997 by the National Conference of Commissioners on Uniform State Laws, initially explored various means of providing security in electronic commerce, offering strong presumptions where certified digital signatures

81. New Zealand Law Commission, Report 50, *Electronic Commerce Part One: A Guide for the Legal and Business Community*, at ¶¶ 334–335 (Mar. 15, 1999) <http://www.lawcom.govt.nz/pub_index.html>.

82. "In our view, the needs of the market can be met by making a change to the proposed Interpretation Act by including a definition of the term 'signature' to ensure that electronic signatures are acceptable. This could follow the intent of article 7 of the UNCITRAL Model Law on Electronic Commerce." *Id.* at ¶ 344.

83. *See supra* note 5 and accompanying text.

84. *See supra* note 2. On April 7, 1999, after this article went to press, the National Conference of Commissioners on Uniform State Laws announce that the final form of these rules would be in the Uniform Computer Information Transactions Act, and not a part of the Uniform Commercial Code.

were involved.[85] Thus, in the beginning of the UETA deliberations, the philosophy of the digital signature legislation was pursued: identifying certain technological implementations and giving them special legal effect. Serious skepticism was expressed at the first meetings, however, about the appropriateness of this approach, and in particular about presumptions, for many reasons, ranging from concerns about the implementation of digital signature technology,[86] to the lack of acknowledged standards of care of a private key, to uncertain certification practices by CAs, and to unfairness of the presumptions to less sophisticated parties. On the theory that market practices were not sufficiently developed to permit evaluation of the presumptions, the presumptions were weakened drastically,[87] and the special treatment for digital signatures was replaced with special treatment for secure signatures. By July of 1998, however, the presumption language was eliminated.[88] No heightened effect was given to a message or record because of its status as either a digital or "secure" signature.

There was, however, special treatment given where security procedures were implemented. Under the provisions dealing with attribution, an electronic message would be attributed to a person if another person, through the application of a commercially reasonable security procedure, concluded that it was that of the purported sender.[89] Gone was any reference to specific technologies, or criteria those technologies need to satisfy; as long as the procedures were commercially reasonable, they were given special legal effect. In essence, what started as a technological construct (specified security procedures) evolved into a semi-technological construct (security procedures satisfying specified criteria) and eventually into a commercial law construct (commercially reasonable security procedure). Even that

85. The preliminary draft of the UETA was prepared in the spring of 1997 and considered at an organizing meeting of the drafting committee in Dallas in May. *See* Uniform Law Commissioners, *Drafts of Uniform and Model Acts Official Site*, <http://www.law.upenn.edu/bll/ulc/uecicta/ecomm.htm>. It reflected some of the thinking in both UNCITRAL's deliberation and the Utah Act, offering strong presumptions that certified digital signatures bound the purported signer (the person named in the certificate) to the electronic record. Similar provisions appeared in the August 1997 draft.

86. *See* Cem Kaner, *The Insecurity of the Digital Signature* <http://www.badsoftware.com/digsig.htm>.

87. The November 1997 draft of the UETA weakened the presumptions drastically; it had borrowed concepts from Illinois, as had UNCITRAL at about the same time. Continued concern about the presumptions led to the inclusion in the March 1998 draft of the UETA three alternative definitions of a presumption, ranging from a "bursting bubble" approach, where the proffering of any credible evidence destroys the presumption, to a shifting of the burden of persuasion. *See* UETA § 102(a)(15) (Revised Draft Mar. 1998).

88. *See* Uniform Electronic Transactions Act (Proposed Draft July 1998).

89. *See id.* § 202. In turn, a security procedure was defined as a procedure required by law, established by agreement, or knowingly adopted by each party. *See id.* § 102(a)(17).

provision raised concerns, in large part for the same reasons that the presumption language did, but in addition because of the vagueness and uncertainty inherent in a "commercially reasonable" standard. Eventually, this special treatment for commercially reasonable security procedures was also eliminated by the February 1999 draft.[90]

Although, generally, the UETA eliminated presumptions, the February 1999 draft did contain one vestige of presumptions arising in the security procedure context that proved to be controversial and was ultimately eliminated. Under that provision, if one party required the use of a security procedure, that "requiring party" would be precluded from denying any messages sent pursuant to that security procedure. In other words, an irrebuttable presumption was created that the message came from the requiring party.[91] The other party, however, would not be precluded from denying any messages under similar circumstances and would retain the right to deny the message as its own.[92] The theory of the section was to "cast[ ] the risk of misattribution, and informational error on the party that is responsible for a particular security procedure being used in a transaction."[93] The unintended consequence of this provision, however, was to *discourage* a party from resorting to security procedures: it would appear to a party's advantage *never* to require a security procedure—a result fundamentally at odds with the type of behavior, i.e., the use of security procedures, one would otherwise want to encourage. Even if a party were acting reasonably, prudently, and in good faith in setting out security procedures, it could not

90. A memorandum prepared by the Chair and Reporter of the UETA Drafting Committee outlined the reasons for eliminating the presumptions: "certainty and stability regarding the predicate facts giving rise to the presumption" inherent in creation of statutory presumptions is lacking; the vague formation of "commercially reasonable procedures" led to uncertainty; and uncertainty was inherent in the development of the technologies. Memorandum from Patricia Brumfield Fry and D. Benjamin Beard to NCCUSL Commissioners (July 18, 1998) <http://www.webcom.com/legaled/ETAForum>. Technology changes so rapidly that it is difficult to say, two years after a given transaction occurred, what procedures were "commercially reasonable" at the time. Other considerations that were cited include: the relative weakness and therefore meaninglessness of the "bursting bubble" presumption (the presumption exists until denied by the other party), the concern about creating a regime in which parties selected the medium for their transaction based on their differing legal effects; the fact that presumptions would operate against the interests of consumers and other unsophisticated parties; and the fact that presumptions might become a rationale for other governments to regulate. *Id.* For a summary of the discussions at the Uniform Electronic Transactions Act Drafting Committee meetings, see *id.*

91. UETA § 107(a) [Alternative 1] (Proposed Draft Feb. 1999). The other party must have relied upon that message to trigger the presumption. *Id.*

92. *Id.* An alternative proposal would provide simply that "an agreement to be bound by the results of a security procedure is unenforceable." *Id.* § 107(a) [Alternative 2].

93. *Id.* Reporter's Note.

escape liability under this provision, even by contract.[94] Consequently, a provision intended to encourage the use of security procedures arguably did just the opposite, and it was eliminated by the UETA Drafting Committee at its February 1999 meeting.

The current draft of the UETA, as it may be expected to be presented to the National Conference, treats attribution in a very simple, straightforward manner. An electronic message is attributed to a person "if the electronic record resulted from the act of the person, or its electronic agent."[95] Once it is found that a message or record is attributable to a person, attribution "has the effect provided for by law, regulation, or agreement regarding the security procedure."[96] Under this approach, attribution clearly is a factual matter;[97] no preference is given to any particular method of authentication or any particular security procedures, and at the same time, freedom of contract is recognized. Thus, at least within the context of the UETA, the view that there should not be any rule which would provide a specific effect for any security procedure,[98] whether it be an identified security procedure, e.g., digital signatures, a security procedure agreed to by the parties, or a security procedure which meets some predefined criteria, has carried the day with regards to attribution.[99]

VII. ARTICLE 2B OF THE UNIFORM COMMERCIAL CODE

The proposed new Article 2B to the Uniform Commercial Code, whose scope is limited to computer information transactions, was intended to forge

94. UETA § 107(b) (Proposed Draft Jan. 29, 1999) (stating the "provisions of this section may not be varied by agreement"). *Id.*

95. *Id.* § 109(a).

96. *See id.* § 109(b). "'Security procedure' means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person." *Id.* § 102(a)(18).

97. As a result, a certain security procedure may be effective to prove attribution at a given point in time but will lose its efficacy with advances in technology, or with the ability of hackers to demonstrate the vulnerability of systems.

98. *See* Letter from the Bank Working Group to D. Benjamin Beard and Patricia Brumfield Fry (Feb. 12, 1999) (on file with the author). The Bank Working Group includes Citigroup, The Chase Manhattan Bank, Visa International, Independent Bankers Association of America, Consumer Bankers Association, The New York Clearing House Association, L.L.C., and the Keybank National Association.

99. Under a parallel provision, § 111, an electronic signature "may be proven in any manner, including by showing that the electronic signature was signed in conformity with a security procedure for validating electronic signatures, or that a procedure existed by which the person . . . must have engaged in conduct or operations that signed the record or item in order to proceed further in the processing of the transaction." UETA § 111 (Proposed Draft Jan. 1999). Again, any presumptions arising from the use of a particular security method are removed. *Id.*

the rules for electronic contracting that would provide the base for the remaining articles of the Code.[100] Although the UETA has gone to great lengths to eliminate presumptions and to eliminate any special treatment arising from the use of security procedures, the Article 2B Drafting Committee has taken the position that such treatment is important and that if security procedures are present, that treatment encourages the use of security procedures and promotes electronic commerce.

Article 2B begins with the traditional rule that the person asserting that a record is that of another person has the burden of proof of attribution.[101] Special legal effect is given, however, to the implementation of security procedures, or what Article 2B calls an "attribution procedure."[102] If the parties agree to, *or otherwise adopt,* an attribution procedure[103] which is used by the parties, the attribution procedure is commercially reasonable, and the recipient "relies on or accepts" the message, then the recipient has met its burden of attributing the message to the sender.[104] The only way the purported sender may avoid attribution is to prove the message was not caused by: 1) someone entrusted by the sender with the right to act on its behalf; 2) someone who gained access to the transmitting facilities of the sender; or 3) someone who obtained, from a source controlled by the purported sender, information facilitating breach of the attribution procedure.[105] Even if the purported sender is able to overcome this hurdle, it might still be held liable under negligence-type principles.[106]

The foundation, then, of Article 2B's rules is the presence of a "commercially reasonable"[107] attribution procedure, a concept that had its

100. Although that was the intent, the Article 2 Drafting Committee voted at its February 1999 meeting to adopt a minimalist approach, more akin to Article 2B, rather than following Article 2B's approach. That decision was ratified by the Article 2 Drafting Committee at its last meeting in March of 1999. Thus, the Article 2 Drafting Committee has stopped short of adopting the Article 2B provisions discussed above.

101. *See* U.C.C. art. 2B-116(c) (Proposed Draft Feb. 1, 1999), *available at* <http:www.law.upenn.edu/bll/ulc/ulc.htm>.

102. An attribution procedure is defined as "a procedure established by law, regulation, or agreement, or a procedure otherwise adopted by the parties, [to verify] that an electronic message . . . is that of a specific person." *See id.* at § 2B-102(a)(3).

103. *See id.* at § 2B-116(c). At its February meeting, the Article 2B Drafting Committee discussed a clarification that the attribution procedure must have been "knowingly" adopted. *Id.*

104. *Id.*

105. *See id.* at § 2B-116(c)(3) (Proposed Draft Feb. 1, 1999) *available at* <http:www.law.upenn.edu/bll/ulc/ulc.htm>.

106. Under U.C.C. § 2B-116(e), a purported sender is liable for reliance losses if those losses occurred as a result of the purported sender's failure to exercise reasonable care with regard to the attribution procedures. U.C.C. § 2B-116(e).

107. *See, e.g., id.*

genesis in the "security procedure" provisions of Article 4A on funds transfers.[108] Once the presence of such a procedure is established, then the recipient of the message has carried its burden of establishing that the message originated with the identified sender. The theory is that such a standard makes it easier for recipients of messages to "prove up" those messages in court, and as a result, more people will implement commercially reasonable security procedures, and confidence in the systems will increase.

Those favoring presumptions[109] of this nature frequently invoke the precedent of Article 4A and its treatment of commercially reasonable security procedures. Crucial differences exist between the two formulations, however. First, Article 4A applies only where there has been an "agreed" security procedure. Indeed, under Article 4A, the notion of a "commercially reasonable security procedure" acts as a limitation on the ability of the parties to alter traditional rules governing proof of attribution: a contractual agreement will be recognized only if the agreed procedure is commercially reasonable. Thus, Article 4A is *not* a recognition that certain security procedures should be given special legal effect, but a recognition that the ability of the parties to agree—and, in particular, the ability of a bank to shift the liability for an unauthorized message to its customer—is limited.

While Article 4A only applies where there has been an "agreed" security procedure, Article 2B applies to any attribution procedure "otherwise [knowingly] adopted by the parties."[110] According to the drafters of Article 2B, the provision on attribution "enables electronic commerce in an open environment, while stating reasonable standards to allocate risk."[111]

---

108. *See* Boss, *supra* note 4. Article 4A on funds transfers defines a security procedure as "a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or canceling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication." U.C.C. § 4A-201. For the definition of an "attribution procedure," see *supra* note 102. The relevance of Article 4A as a precedent in other areas of electronic commerce has, however, been called into question in large part because of distinctions between the types of transactions subject to Article 4A and those subject to the provisions of either Article 2B or the UETA. *See* Boss, *supra* note 9, at 1079–80, 1083.

109. The February 1999 draft of § 2B-116 spoke in terms of use of attribution procedures "creat[ing] a presumption" of attribution. U.C.C. § 2B-116 (Proposed Draft Feb. 1, 1999). At its February meeting, the Drafting Committee accepted a proposal put forward by Chair Carlyle C. Ring, Jr. and Reporter Raymond Nimmer to modify the language to speak in terms of who has the burden of establishing attribution or non-attribution. *See* <http://www.2Bguide.com/docs/299t4.html>. The effect of the proposal was to remove the problem of characterizing the type of presumption (bursting bubble, burden of going forward, burden of persuasion), but in effect, the language utilizes the strongest of rebuttable presumptions: the burden is that of establishing the negative.

110. U.C.C. § 2B-102(a)(3) (Proposed Draft Feb. 1, 1999).

111. *Id.* § 2B-116, Reporter's Note 1.

It is clear that the Article 2B drafters were concerned about parties who were not otherwise in privity with each other: "Electronic commerce is anonymous in character and depends upon such procedures and their recognition in law and practice."[112] The absence of any requirement of an agreement has important ramifications. At least where there is an agreement between the parties as to the relevant procedures to be followed, a party is arguably on notice that all parties to the transaction will rely on those procedures. Because of the vague reference in Article 2B to procedures "otherwise adopted by the parties,"[113] such notice is arguably lacking. Moreover, under the required agreement under Article 4A, the customer unwilling to assume fraud risks had the ability to protect itself by shifting the burden back to the bank or requiring the bank to take additional procedures,[114] an ability lacking under Article 2B.

A second crucial difference is the practical ability of the alleged sender of a message to overcome the presumption in light of the nature of the transaction and in light of the state of technology. If a person adopts a PIN or other attribution method for doing business on the Internet, it will find that if a message is sent utilizing that PIN, the person will be liable for that message unless it can invoke the provisions setting forth how the presumption is overcome. Consequently, rather than the burden being on the recipient to prove who sent the message, the burden is now on the alleged sender to prove it did not send the message and that the message did not originate from anyone who gained access through the alleged sender.

Proving a negative is difficult. In the context of Article 4A, however, the rationale was explained as follows:

> Because of bank regulation requirements, in this kind of case [wire transfer fraud,] there will always be a criminal investigation as well as an internal investigation of the bank to determine the probable explanation for the breach of security. Because a funds transfer fraud usually will involve a very large amount of money, both the criminal investigation and the internal investigation are likely to be thorough. In some cases there may be an investigation by bank examiners as well. Frequently, these investigations will develop evidence of who is at fault and the cause of the loss. The customer will have access to evidence developed in these

112. *Id.* § 2B-102, Reporter's Note 2.

113. *Id.* § 2B-102(a)(3).

114. *See* U.C.C. § 4A-203, cmt. 3 ("A customer may want to protect itself by imposing limitations on acceptance of payment orders by the bank"). *Id.* "Some customers may be unwilling to take all or part of the risk of loss with respect to unauthorized payment orders even if all of the requirements of Section 4A-202(b) are met." *Id.* § 4A-203, cmt. 6.

> investigations and that evidence can be used by the customer in meeting its burden of proof.[115]

Unfortunately, access to such rigorous investigation and proof will be lacking in the typical transactions covered by Article 2B.[116]

Third, Article 2B adopts an additional ground for shifting risks: if the person alleged to have sent the message can nonetheless prove that it did not send the message—a somewhat difficult task to begin with—that person may still be liable for losses "in the nature of the cost of performance of the other party"[117] if the loss occurred because: 1) the purported sender failed to exercise reasonable care; 2) the other party reasonably relied on the belief that the purported sender sent the message; and 3) the fraudulent third party who used the attribution procedure gained access to it from a source under the control of the purported sender.[118] The net result is that it may well be impossible for an alleged sender to avoid attribution under Article 2B.[119]

VIII. INTO THE BREACH: LEGISLATING FOR SECURITY

When the UETA Drafting Committee was first established, the assumption, and, indeed, the mandate given to that committee, was to avoid inconsistency with the revisions being proposed to the Uniform Commercial Code, and, in particular, Article 2B. Theory, however, has diverged from practice, as illustrated by Article 2B's adoption of a presumption approach, and its not-so-hidden desire to go beyond mere removal of barriers to

115. U.C.C. § 4A-203, cmt. 5.

116. The difficulties in proving a negative raise another issue: the burden on the party attempting to avoid liability arguably is the same (to prove the message did not come from a source controlled by that party) regardless of the security procedure at issue. Yet not all technological security procedures are created equal; what they involve, what they prove, and the strength of their proof vary. Even "digital signatures" come in different strengths: the longer the number used to generate the key pair, the harder it is to crack the code, and the shorter the number, the easier it is. Yet all commercially reasonable security procedures are treated equally with respect to the presumption.

117. U.C.C. § 2B-116 (Proposed Draft Feb. 1, 1999).

118. *Id.* For a history of the evolution of this provision and its source in both Article 4A and the UNCITRAL Model Law on Electronic Commerce, see Boss, *supra* note 4, at 1961–63.

119. Take the situation of a person who has attribution procedures resident on an office computer and locks the office to attend a weekend meeting, where there are ample witnesses to confirm that it was physically impossible to send the message at issue. Proof that it was physically impossible for that person to send the message would not be sufficient to satisfy the burden of establishing that the electronic message was not caused by anyone entrusted by that person with the office, someone who gained access to the office, or someone who gained information facilitating breach from that person.

actively supporting electronic commerce, and the rejection of that approach in the UETA. According to the Chair and the Reporter for the UETA, "perhaps the most significant difference between the UETA and Article 2B relate[s] to the creation of presumptions when security procedures are employed by parties to an agreement."[120]

These differences continue despite attempts to harmonize the approaches between those two drafts; the only agreement is continued disagreement.[121] "In light of the different character and scope of the respective drafts, it was agreed that the different approach in the two drafts can be justified."[122] What is far from evident[123] is what differences in character and scope justify the difference in approach to presumptions. Although it is true that Article 2B has a narrower scope than the UETA in that it applies only to certain informational contracts while the UETA potentially applies to any contracts entered into online, the reality is that under both, there is a wide range of sophistication in the parties potentially subject to their provisions, and under both, identical arguments may be made about the need to support electronic commerce. The only conclusion that can be drawn is that each Drafting Committee has a different view about the relationship between the law and security.

On one hand, the philosophy of the UETA is the minimalist approach: as long as the law recognizes and enforces electronic transactions, businesses gain some "security" in their commercial dealings. The role of law in technology is enabling, not promotional of certain technologies, nor channeling, encouraging certain procedures. This approach recognizes that "technological security" is not monolithic: there are many technological methods of security, with different strengths and weaknesses, and technology is in a constant stage of development.[124] Thus, promoting certain technologies or certain implementations would be counterproductive. This approach also recognizes that the law is of limited utility in encouraging

120. Memorandum, *supra* note 90.

121. Each Drafting Committee reaffirmed its own approach, and rejected that of the other, in its last meeting in February 1999.

122. Memorandum from Patricia B. Fry, UETA Drafting Committee Chair, and Carlyle C. Ring, Jr., U.C.C. Article 2B Drafting Committee Chair, to the UETA and Article 2B Drafting Committees (Jan. 29, 1999) <http://www.2Bguide.com/docs/199pfcr.html>.

123. This is true even to one who is both on the Article 2B Drafting Committee and the official American Bar Association Advisor to the UETA Drafting Committee. The statement may simply be a recognition that different drafting committees, dealing with different subject matters, came up with different solutions.

124. "While a number of participants argued that *fairly strong presumptions are necessary to promote electronic commerce*, others felt that the state of technology and current market are still too underdeveloped to warrant the creation of any presumptions." Memorandum, *supra* note 90.

certain types of behavior: people will use security procedures because it is good business, not because the law gives special legal effects if they are used. The marketplace, rather than the legislature, provides the incentives and support. The UETA does not view the law as the sole or even primary source of security; instead, it recognizes that the entire technological, legal, and social structure contributes to that security.

On the other hand is the view that the law has an important role in providing "security" in electronic commerce; that the law can indeed "legislate" security by providing certain benefits to those who use the available technology. Article 2B, following the lead of Article 4A,[125] represents the position that statutory provisions that recognize those security procedures can encourage use of security procedures.[126] By assuring parties involved in "electronic commerce" of the ability to enforce transactions in which reasonable security procedures are used, the law creates user confidence and ultimately supports and promotes the use of electronic commerce.

Each approach has its critics. The minimalist approach, limited to the removal of barriers, has been criticized as not giving the user of technology the degree of assurance necessary. Critics emphasize that simply saying electronic messages "may" suffice or are equivalent to writings and signatures is insufficient; users want to know what *will* suffice. Consequently, it is asserted that the legislation must lay out the indicia of assurance and certainty necessary for the electronic messages to be deemed reliable.[127]

The question, however, is whether the Article 2B approach gives any greater certainty or any greater assurances than the minimalist approach. In giving special effect when commercially reasonable security procedures are present, what must be asked is whether Article 2B has met the goals of

---

125. Article 4A theorized that losses due to fradulent payment orders can best be avoided by the use of commercially reasonable security procedures, and that the use of such procedures should be encouraged. U.C.C. § 4A-203, cmt. 3. The rules designed to "protect both the customer and the receiving bank," were aimed at providing such encouragement. *Id.* Thus, the customer may not be held liable *unless* commercially reasonable security procedures are agreed to, and the bank is protected if they are agreed to and are implemented. *Id.*

126. As one letter put it: "Given the limited experience with electronic commerce, NCCUSL should gravitate towards general legal principles that provide incentives for, and reward the use of, *commercially reasonable* and *agreed* procedures that give courts a basis to select and adjust to the facts of individual cases." Memorandum from Business Software Alliance to Article 2B Drafting Committee (Jan. 20, 1999) <http://www.2Bguide.com/docs/0119bsa.html>. Of course, as discussed, Article 2B goes well beyond agreement.

127. *See* Michael S. Baum, *Linking Security and the Law of Computer-Based Commerce* <http://www.verisign.com>.

"security:" more certainty and predictability in the application of the law; greater assurances of the validity of the transaction; encouragement of the use of security procedures; and more faith or trust in the systems.

It is questionable whether, as currently articulated, Article 2B contributes to the certainty and predictability in the application of the law. The factual nature of the commercially reasonable standard[128] renders it vague and subjective in nature,[129] a result which "could hardly have been more inconsistent with the drafters' statement that 'the parties . . . transfer need to be able to predict risk with certainty.'"[130] It is true that in the context of funds transfers, the same test has been used, but the funds transfer situation differs.[131] Determining what is "commercially reasonable" in an industry where there is a developed body of commercial practices, where the

128. U.C.C. § 2B-114 (Proposed Draft Feb. 1, 1999) ("commercial reasonableness is [to be] determined in light of the purposes of the procedure and the commercial circumstances at the time the parties agree to or adopt the procedure."); *id* ("How one gauges commercial reasonableness depends on a variety of factors, including the agreement, the choices of the parties, the then current technology, the types of transactions affected by the procedure, sophistication of the parties, volume of similar transactions engaged in, availability of feasible alternatives, cost and difficulty of utilizing alternative procedures, and procedures in general use for similar types of transaction."). *Id.*, Reporter's Note 4.

129. This objection has been made on both the domestic level as well as on the international level (where the concepts of "reasonableness" and "commercial reasonableness" generally do not have the same level of acceptance as they do within the United States). *See* letter from Paul Shupack, Paul S. Turner, and Jane K. Winn (Jan. 20, 1999) <http://www.2Bguide.com/>.

130. *Id.* (citing Official Comment to Section 4A-102).

131. In the Article 4A context, the use of the phrase was justified on the grounds that to the extent one goal of Article 4A was to shield banks from potential catastrophic losses by shifting some wire fraud risks to customers, the "commercially reasonable security procedure" requirement was one way of achieving a balance by limiting the bank's ability to shift the risk in egregious circumstances. According to that line of argument, the national interest of protecting recipients of messages from catastrophic losses (which was present in the bank regulation arena) is absent in the more generic area of electronic commerce. Thus, a device (the requirement of a commercially reasonable security procedure) which was originally adopted to protect customers from a rule of absolute liability is now being invoked to impose liability. *See* Letter from Shupack, Turner, & Winn, *supra* note 126.

This description of the intent of the "reasonable security procedure" requirement of Article 4A has been disputed by the Chair of the Article 2B Drafting Committee, who also chaired the Article 4A Drafting Committee. Memorandum of Carlyle C. Ring, Jr. (Jan. 25, 1999) <http://www.2Bguide.com/>. His account points out that, in its application, Article 4A places the risk of unauthorized orders on the bank; the bank is only able to shift that risk to the customer if it finds that commercially reasonable security procedures are used. While his argument correctly interprets the language and structure of Article 4A as it currently existed, it does not respond to the argument that the alternative in Article 4A was to shield banks from liability by placing all risks on the customer.

parties belong to a relatively closed community of players, and where the major participants are either large, sophisticated commercial parties or banks subject to strict regulatory oversight[132] is a different burden than proving what is "commercially reasonable" when such factors are absent. In other words, although benefits are intended to flow from the use of "commercially reasonble" security procedures, the introduction of notions of "commercial reasonableness" is a serious qualification on the legal construct that weakens its usefulness as a guiding beacon for business.[133] Thus, according benefits when "commercially reasonable" security procedures are used may not provide the type of "security" that the industry is seeking, given the vagueness and uncertainty inherent in the formulation and the difficulty in determining whether a particular procedure may be commercially reasonable under the circumstances.

Just as it is questionable whether the goal of "certainty" is met, it is also questionable whether Article 2B gives the user any greater assurances than would exist under the UETA. To get the benefit of the beneficial treatment accorded by the statute, the proponent would still have to prove that there was a method adopted by the parties to authenticate the message as that of the sender, that the method adopted did operate as an authentication device, and that under the circumstances of the transaction, it in fact operated reasonably as an authentication device. In other words, to get the benefit of the statute, the recipient would have to prove essentially the same set of facts one would normally need to prove attribution directly.[134] Thus, it is doubtful

---

132. Boss, *supra* note 9, at 1079–80, 1083.

133. Of course, to the extent a vague standard of "commercial reasonableness" falls far short of laying out the indicia of assurance and certainty necessary for reliability, one could argue for more specificity in the type of security procedures sanctioned by the law. To the extent a specific technological implementation does indeed provide assurances of reliability, it is argued that implementation should be given greater efficacy under the law. This can be accomplished through statutory or legal provisions treating these more secure methods as conclusively satisfying signature and writing requirements and as providing evidence of source and identity of the sender, as well as the integrity of the content of the message. The more detail and "indicia," however, one lays out in a statute, the more regulatory and binding the scheme becomes. Also, there is less flexibility with respect to emerging technologies and implementations and the needs of the parties.

134. That is not the case where there is an agreement: then all the recipient would need to prove was the agreement itself and compliance with its procedures. Similarly, where there is a specific statute or regulation validating a specific technological method of authentication, all that the recipient would need to prove is that the specified method was used. The proof issues become complicated when the recipient must prove "commercially reasonable attribution procedures," as is the case with Article 2B, or when it must prove that the method used qualifies as a "secure electronic signature," the approach followed in Illinois and in the proposed UNCITRAL legislation.

whether the "commercially reasonable security procedure" standard at all helps the litigant with her burden of proof.

The goal of encouraging the use of security procedures is also troublesome, and the risk exists that the statutory scheme may actually operate as a disincentive. As was observed in the context of the UETA, a rule placing the risk of loss on the person requiring use of a specified security procedure might indeed discourage people from designating certain procedures;[135] a variation of this provision in Article 2B[136] was deleted at the Drafting Committee's last meeting for this very reason. The same question can be raised about the other provisions in Article 2B with regard to attribution: does adopting presumptions that make it easier for one party to prove a transaction in court, while at the same time making it difficult, if not impossible, for the other party to disprove the transaction, result in encouraging or discouraging the use of security procedures? No special proof rules exist, for example, in the context of phone orders or mail orders, yet those businesses thrive. Article 2B's rule encourages recipients of messages to use "commercially reasonable attribution procedures" by giving them statutory incentives, but it does not provide similar incentives to potential senders of electronic messages. Indeed, the rules may arguably discourage potential senders from adopting certain methods of communication for fear of having liability imposed, in actions with strangers, where the alleged sender did not send the message.[137] If, indeed, part of the problem is that people are concerned about the "unknown" and the potential of unintended liability, rules such as this feed rather than assuage their fears.

Additionally, Article 2B takes the view that by providing those benefits, one in turn *increases* the confidence of those doing business electronically because they can now reasonably rely on receipt of electronic messages from strangers. This view of security and its relationship to the law assumes that the value and security added to electronic commerce in this manner is both appropriate and acceptable. As noted above, however, that security may be illusory. First, to the extent that potential users of the technology are discouraged from its use because of fear of potential liability, their confidence in the system is *decreased.* More importantly, however, whatever confidence flows from the use of security procedures in electronic commerce arguably comes *not* from the knowledge that the law gives the

135. *See supra* notes 91–94 and accompanying text.

136. U.C.C. § 2B-115 (Proposed Draft Feb. 1, 1999).

137. Consumer representatives, for example, have pointed out that the credit card scheme that currently exists protects consumers in the case of fraud or unauthorized use of their cards, while in contrast, an Article 2B approach in the consumer context would protect the merchant. The UETA approach is to favor neither party.

users benefits but from the knowledge that the technological implementations themselves are trustworthy.

On the federal level, several agencies have noted the need to avoid allocations of risk at a time when electronic commerce is still evolving. Thus, the Federal Reserve Board, considering the question of stored value cards, noted:

> Economic theory and empirical evidence suggest that government regulation has the potential to foster or hinder technological progress and the development of new products by influencing private sector incentives to invest in research and development activities and private sector choices among alternative technologies. In deciding whether and, if so, how to regulate . . . policymakers must carefully assess the potential effect of their decisions on the evolution of these new products and the extent to which they achieve market acceptance.[138]

In similar words, the White House, which had previously urged governments to avoid undue regulation of the market,[139] urged flexibility in the drafting of electronic commerce laws, in large part to prevent unwarranted market distortion. This is expressed in the following:

> The market is very much in the early stages of experimentation with respect to business models for electronic commerce. The United States believes it is not wise at this time to attempt to identify a single model that these transactions will use or to develop a legal environment using a single model. Indeed, such an approach would prevent the market from testing different possible approaches and prematurely impose a particular model on all electronic commerce, inevitably limiting its growth. Therefore, at the current state of development, the legal framework should support a variety of business models so that the market is able to experiment and select the models that best fit particular types of electronic commerce.[140]

---

138. Board of Governors of the Federal Reserve System, *Report to the Congress on the Application of the Electronic Funds Transfer Act to Electronic Stored-Value Products* (Mar. 1997) <http://www.bog.frb.fed.us/boarddocs/RptCongress/efta_rpt.pdf>.

139. *See supra* note 30.

140. U.S Government Working Group on Electronic Commerce, First Annual Report (Nov. 1998) <http://www.doc.gov/ecommerce/E-comm.pdf>.

IX. CONCLUSION

No one disputes the fact that security issues in electronic commerce, both of the technological and non-technological kind, are extremely important. This is true even of those who adhere to the notion that the law should, at this stage, simply *remove* barriers but otherwise stay neutral on the subject. Indeed, security is one of the primary concerns that should be addressed by businesses migrating to electronic communication and businesses online.[141] Thus, in the case of agreements between businesses doing electronic commerce, it makes sense to go beyond merely requiring "reasonable security procedures" to explain in specific detail what procedures are required,[142] and where the agreement is specific as to the effects to be given to the use of those procedures, it makes sense to give deference to that agreement. Similarly, the development of industry standards and codes of conduct addressing security is of extreme importance.[143] Industry codes and standards operate to inform business people as to the variety of technological security means at their disposal, thereby empowering them to make intelligent choices. This type of education clearly gives the businesses a sense of security.

The real questions go to the relationship between the law and these "security" issues: what type of "legal security" is necessary? Should the law set forth a legal regime specific to certain technologies or implementations, providing certain benefits when that technology is used? While it may be true that certain technological security procedures are "uniquely suited to the needs of secure e-commerce,"[144] two key points

141. *See supra* note 21, cmt. 1 (1990) ("Adequate security procedures are recognized . . . as critical to the efficacy of electronic communication. . . . The use of adequate security enhances the reliability of those records and enhances the ability to prove the substantive terms of any underlying commercial transaction.").

142. *See, e.g., Model Electronic Payments Agreement and Commentary* at § 7, cmt. 5; 32 JURIMETRICS J. 601, 654 (1992) ("in certain situations a lack of specificity in defining 'reasonable' security procedures may provide inadequate guidance causing such security procedures to fail in their intended purpose. Specificity may help the parties implement and comply decisively and unambiguously with security procedures, reduce confusion and offer better expectations of reliability and certainty. Security procedures should be sufficiently precise so that they are not subject to discretionary, self-serving interpretation").

143. *See* Information Security Committee, Section of Science and Technology, *American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (1996) <http://www.abanet.org/scitech/ec/isc/home.html/ >.

144. This claim, often made of digital signatures within a public key infrastructure, *see* Baum, *supra* note 46, has been disputed both because it assumes all implementations of the technology are the same when they are not, and it ignores other technological security procedures such as biometrics.

remain. First, while certain types of technology today may be considered sufficiently secure to merit special treatment, future technological advances raise the possibility that: 1) methods of security currently used may cease to be secure in the future; and 2) other methods of security and other modes of technological implementation will provide comparable or even better means of security. Given the time lags inherent in the updating of laws,[145] drafting a technology-specific or implementation-specific body of rules may not be prudent.[146] Drafting a more general body of rules that depend upon such concepts as "commercially reasonable security procedures" or that set out criteria that security procedures must satisfy present a different problem: the creation of a legal regime lacking the certainty desired by many business people.

The theory that these laws "encourage" the use of security procedures is questionable. If indeed certain technological security techniques are uniquely situated to the needs of secure electronic commerce, they may well be implemented without the adoption of specific rules. "One compelling example of the dramatic success of open PKI is the ubiquitous use of the SSL (Secure Sockets Layer) protocol over shared paths such as the Internet for e-commerce."[147] That proposition, while asserted as evidence of the need for PKI specific legislation, arguably proves the opposite: if there is a good, secure method of doing electronic commerce, that method will be implemented as a matter of sound business practices, not as the result of PKI specific legislation. In other words, the technology implementation itself provides the necessary security and certainty necessary for electronic commerce without the need for legislative intervention.[148]

---

145. The need to revise our domestic and international laws to accommodate electronic commerce has been a theme for well over a decade, yet we are still attempting to address that need through statutory enactment.

146. *Cf.* C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, 34 SAN DIEGO L. REV. 1225 (1997).

147. Baum, *supra* note 124, at 38. According to Baum, the total number of sites using SSL has risen from 486 in the third quarter of 1996, to 104,760 in the third quarter with a projected rise in the fourth quarter of 1999 to 307,206. The total number of sessions, as opposed to sites, has similarly increased during that period from 291,600 to 134,775,517, and is projected to rise to 636,335,396. *Id.*

148. An example lies within the development of the SET protocol, which involves the use of digital signatures in the credit card system. MasterCard and Visa, who under current arrangements potentially bear the risk of fraudulent transactions, charge their participating merchants a percentage based on the risk involved in particular transactions, e.g., the rate assessed for telephone order charges is much higher than the rate assessed in transactions evidenced by both the card imprint and card holder signature. They have announced, however, that when the SET protocol is implemented in the credit card system, and, presumably, the risks of fraud drop, they will lower their merchant discount rate by several percent. Thus, the benefits of security implementation are being realized not through the

The difficulty with much of this debate over whether or not to recognize specific means of technological security is that the discussion is misplaced. If the technology provides reasonable means of security, people will implement the technology for that reason, not because the law says so. A person who installs locks on his or her door does not do so because greater legal protection is afforded those who use the technology; a person installs locks because experience has shown that locks are one means of stopping intruders. A business that requires checks to be signed by more than one officer does so not because the law requires but because it is a good business practice that reduces risks of fraud, and a bank which institutes the practice of manually examining the signatures on checks over a given amount does so not because the law requires it but because it is a prudent banking practice to reduce risk of fraud. The economic and other benefits to be gained from implementation of secure systems is not disputed; what is disputed is the need for the law to enact legislation saying that these secure systems are secure and therefore are entitled to special treatment. Such legislation may be neither needed nor wise.

There is no doubt that "security" in electronic commerce is an important issue, but the debate over electronic signature legislation is misleading in that it fails to recognize that security is more than merely the legal effects to be given to certain technological security techniques. Once we recognize that fundamental point, we can place the discussions about what type of legislation is necessary and appropriate in perspective and evaluate the claims for what they are worth.

---

enactment of any legislation but through marketplace recognition of the risk reduction additional technological security brings.

Ira Glasser
Executive Director – American Civil Liberties Union

Mr. Glasser has served as Executive Director of the American Civil Liberties Union since 1978. Previously, he was executive director of the New York Civil Liberties Union.

Prior to his affiliation with the ACLU, Mr. Glasser was a mathematician and a member of the science and mathematics faculties of Queens College and Sarah Lawrence College. He was also editor of *Current Magazine*.

Mr. Glasser authored a book, *Visions of Liberties: The Bill of Rights for All Americans*, published in November 1991. An insightful analysis of how our rights developed, written to commemorate the 200th anniversary of the Bill of Rights, *Visions* was published by Arcade Publishing, Inc., in New York City.

In addition to *Visions*, Mr. Glasser is a widely published essayist on civil liberties principals and issues, whose writings have appeared in *The New York Times*, *The Village Voice*, *Harper's*, *The New Republic*, *The Nation*, and *Christianity and Crisis*, among other publications. He is also the co-author of *Doing Good: The Limits of Benevolence*, published by Pantheon in 1978.

Mr. Glasser received a B.S. degree in Mathematics and graduated with honors in Literature and the Arts from Queens College in 1959. He has a master's degree in mathematics from Ohio State University and also studied sociology and philosophy on the graduate level at the New School for Social Research.

Born and raised in New York, Mr. Glasser is married and the father of four children.