1998

Couriers Without Luggage: Negotiable Instruments and Digital Signatures

Jane Kaufman Winn
University of Washington School of Law

COURIERS WITHOUT LUGGAGE: NEGOTIABLE INSTRUMENTS AND DIGITAL SIGNATURES

JANE KAUFMAN WINN*

I. INTRODUCTION

Negotiable instruments have long played a venerable role in commercial transactions, and negotiable instruments law is an integral part of the Uniform Commercial Code (U.C.C.).[1] One of the identifying characteristics of a negotiable instrument is that it must strictly comply with the formal requirements of negotiable

* Associate Professor of Law, Southern Methodist University; http://www.smu.edu/~jwinn, jwinn@mail.smu.edu. The author would like to thank Dwight Arthur, Amy Boss, Julia Forrester, John Gregory, Paul Turner, and Benjamin Wright for their helpful comments on earlier drafts.

[1] In 1990, U.C.C. Article 3 underwent a significant revision. *See* Henry J. Bailey, *New 1990 Uniform Commercial Code: Article 3, Negotiable Instruments, and Article 4, Bank Deposits and Collections*, 29 WILLIAMETTE L. REV. 409, 409 (1993). By 1997, the 1990 revised official text had been adopted in forty-eight jurisdictions. Thomas C. Baxter, Jr. et al., *Revised Articles 3 and 4 of The UCC: Will New York Say Nix?*, 114 BANKING L.J. 219, 219 (1997).

instruments law to avoid being relegated to the status of an ordinary contract.[2] In 1846, Chief Justice Gibson of the Supreme Court of Pennsylvania wrote the following: "[A] negotiable bill or note is a courier without luggage. It is a requisite that it be framed in the fewest possible words, and those importing the most certain and precise contract . . . . To be within the statute, it must be free from contingencies or conditions that would embarrass it in its course. . . ."[3] During their heyday in the eighteenth and nineteenth centuries, negotiable instruments were used to mitigate a shortage of metallic currency and to support the expansion of commercial transactions stemming from the industrial revolution.[4]

Digital signatures may play a role in the information revolution similar to the role played by negotiable instruments in the industrial revolution. Digital signatures bear a certain resemblance to negotiable instruments, such as a complex, formalistic definition of the basic device, and, in some models, a similar approach to loss allocation. This Article will describe the basic characteristics of digital signatures, as well as the functions they serve, or may serve in the future, in facilitating electronic commerce conducted over open, insecure computer networks such as the Internet.[5] For the purposes of this Article, a digital signature will be defined as

> [a] transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine (1) whether the transformation was created using the private key that corresponds to the signer's public key, and (2) whether the initial message has been altered since the transformation was made.[6]

A digital signature is distinguished from the broader, more generic "electronic signature," which is generally used to describe any form of electronic authentication.[7] Electronic signatures may include a name in the "From" header in

[2] U.C.C. Article 3 provides the formal requirements for a negotiable instrument. U.C.C. § 3-104(a)(1) to (3) (1995). When these formal requirements have been met, the payment obligation of the party issuing the note or uncertified check merges with the negotiable instrument, suspending the obligation until the instrument is paid or dishonored. U.C.C. § 3-310(b) (1995). If the instrument is a certified check, cashier's check, or teller's check, the obligation is immediately discharged. U.C.C. § 3-310(a) (1995). Once the payment obligation has merged with the instrument, title to the instrument can be transferred by negotiating the instrument. U.C.C. § 3-201(a) (1995).

[3] Overton v. Tyler, 3 Pa. 346, 347 (1846).

[4] Grant Gilmore, *Formalism and the Law of Negotiable Instruments*, 13 CREIGHTON L. REV. 441, 447 (1979) [hereinafter Gilmore, *Formalism*].

[5] For a discussion of the different meanings of "open" in computing environments and the significance of computer security for electronic commerce, see Jane Winn, *Open Systems, Free Markets and the Regulation of Internet Commerce*, 72 TUL. L. REV. (forthcoming 1998), *available on the Internet*, (visited Mar. 10, 1998) <http://www.smu.edu~jwinn/esig.htm>.

[6] INFORMATION SECURITY COMMITTEE, AMERICAN BAR ASS'N, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE 42, 43 (1996) [hereinafter DIGITAL SIGNATURE GUIDELINES]. For a more complete explanation of digital signature technology, see *infra* Part III.

[7] DIGITAL SIGNATURE GUIDELINES, *supra* note 6, at 3.

an electronic mail message, a digitized handwritten signature such as are used by some retail electronic point of sale payment systems, or a typed electronic version of a paper-based holographic signature such as "/s/Jane Winn."[8] Just as a negotiable instrument is a type of contract that meets the formal requirements of negotiable instruments law, a digital signature is a type of electronic authentication method that meets the formal requirements of asymmetric cryptography deployed within a public key infrastructure.[9]

Although digital signature technology has not yet been widely adopted for business use, many proponents of this technology believe that it will soon become a standard business practice.[10] Until adequate experience with commercial applications of this technology develops the "best practices" or standards for its use, questions will abound as to what liability might arise from the use of digital signature technology. To resolve some of the legal uncertainty associated with its use, the American Bar Association published the Digital Signature Guidelines in 1996.[11] This path-breaking work is the product of a project undertaken from 1992 to 1996 by the members of the Information Security Committee of the ABA Science and Technology Section.[12] The Guidelines attempt to set out a coherent regulatory framework within which digital signature technology could be implemented on a large scale for the commercial environment. The approach taken by the Guidelines mimics in many respects the structure of classical negotiability doctrines.[13] This article will analyze the similarities and differences between classical doctrines of negotiable instruments law and the role negotiable instruments played in commercial transactions. Additionally, this article will examine the regulatory norms suggested in the Guidelines and the role they envisage for digital signature technology in the emerging world of global electronic commerce.

For an earlier generation of commercial lawyers, negotiability was virtually

[8] *Id.* at 43.

[9] WARWICK FORD & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE 107-09, 111-12 (1997).

[10] See, for example, the discussion of the Secure Electronic Transaction (SET) protocol being developed by Visa International and MasterCard. *Visa-Electronic Commerce*—SET (visited Feb. 19, 1998) <http://www.visa.com/cgi-bin/vec/nt/ecomm/set/main.html?2+0>. Its developers hope SET will become a standard for Internet and other new electronic commerce applications.

[11] DIGITAL SIGNATURE GUIDELINES, *supra* note 6, at 4.

[12] *Id.* at 1. The same effort also resulted in the Utah Digital Signature Act. UTAH CODE ANN. §§ 46-3-101 to -504 (Supp. 1997). Alan Asay, one of the reporters of the Guidelines, was also the principal architect of the Utah Digital Signature Act, and the two projects have many common features. The Utah legislation differs in certain aspects from the Guidelines, such as in the specific requirements set forth by Utah for the licensing of certification authorities. UTAH CODE ANN. §§ 46-3-201 to -204 (Supp. 1997). Thus, because the Guidelines are a more general, theoretical statement of the principles animating the two projects this article will not focus on the Utah statute. For a detailed discussion of the Utah legislation and the issues it raises, see C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L. REV. 1143 (1996) [hereinafter Biddle, *Misplaced Priorities*], and C. Bradford Biddle, *Public Key Infrastructure and "Digital Signature" Legislation: 10 Public Policy Questions*, (visited Mar. 3, 1998) <http://www.cooley.com/scripts/article.ixe?id=ar_1502> [hereinafter Biddle, *Policy Questions*].

[13] *See generally* James Stevens Rogers, *The Myth of Negotiability*, 31 B.C. L. REV. 265, 272-83 . (1990) (discussing bills and notes of the classical era).

synonymous with marketability; thus, the drafters of the Guidelines copied elements of negotiability in the hope of improving the marketability of digital signatures. Professor Gilmore observed that the drafters of the U.C.C. believed "that whenever any kind of property came into the market—that is, became the subject of a large volume of transactions either of outright sale or of transfer for security—then that kind of property sooner or later acquired some or all of the attributes of negotiability. . . ."[14] At a minimum, these attributes included free transferability, recognition of special rights for good faith purchasers for value, and certain procedural advantages in the enforcement of the obligation, such as a presumption of consideration.[15] The spread of the classical doctrines of negotiability from instruments to a wide range of commercial transactions in the nineteenth and early twentieth centuries reflected a conviction on the part of lawyers and merchants that negotiability facilitates commercial transactions by minimizing the administrative burdens of processing information about property rights.[16] Similarly, the Guidelines strive to facilitate twenty-first-century commercial transactions by minimizing the administrative burdens of processing communications and protecting rights in information in electronic commerce transactions.

Prior to the very recent explosion of interest in the Internet, for decades electronic commerce had been conducted on a large scale over closed networks. Since the late 1960s, billions of dollars in funds transfers have been executed over networked computer systems such as the Federal Reserve Wire Network (Fedwire), Clearing House Interbank Payment System (CHIPS), and the automated clearing house system (ACH); billions of dollars of goods have been sold over electronic data interchange networks. These closed, proprietary networks were built during the era of mainframe computer systems and are now being challenged by open networks of distributed client-server computer systems such as the Internet. Assimilating new technologies into existing commercial practices and business models is a daunting task. Probably for this reason, the early debate over the impact of the Internet on business practices seemingly has been dominated by those most familiar with Internet technology. Also, the early discussions of how digital signature technology may be used for business applications were apparently dominated by the technologically proficient, and surprisingly little reference was made to existing electronic commerce applications.[17] As a result, the model of

[14] Grant Gilmore, *The Good Faith Purchase Idea and the Uniform Commercial Code: Confessions of a Repentant Draftsman*, 15 GA. L. REV. 605, 611 (1981) [hereinafter Gilmore, *Confessions*].

[15] Grant Gilmore, *The Commercial Doctrine of Good Faith Purchase*, 63 YALE L. J. 1057, 1064-66 (1954) [hereinafter Gilmore, *Good Faith*].

[16] *Id.* at 1070-72.

[17] See, for example, the summaries of approaches to digital signature technology in FORD & BAUM, *supra* note 9, Chapter 3. These authors suggest that a sale of $2 million worth of steel to a questionable foreign manufacturer would require stronger security technology than less risky transactions, but they do not discuss the relationship of such an electronic commerce transaction to existing international business practices such as obtaining a letter of credit. FORD & BAUM, *supra* note 9, at 76.

electronic commerce contained within the Digital Signature Guidelines may be of less practical relevance than its drafters hoped.

This Article explores how, despite their similarity in aspiration, negotiable instruments law and the Guidelines nevertheless widely diverge in their applicability to actual business transactions. Negotiable instruments law originated in the medieval "law merchant," and is the product of a centuries-long colloquy between merchants, lawyers, and courts.[18] The doctrines of negotiability served an important role in enabling commercial transactions.[19] By contrast, digital signature technology is a great novelty in commercial transactions. The fundamental commercial law issue raised by the Guidelines is whether legal standards should build from either a given technology or from business practices associated with the use of that technology. Because there is not yet a body of commercial practices associated with digital signature technology, if the correct protocol is the latter, then no legislation is yet appropriate. However, without some form of standardization, the lack of coordination of Internet electronic commerce systems will present an obstacle to individual transactors, and this lack of guidance may stifle the rate of adoption of the technology.

While the focus of the Guidelines may seem artificially narrow when contrasted with existing bodies of commercial law, their focus is comprehensible within the larger context of the possible future of electronic commerce. Shared by many of the advocates of Internet electronic commerce is a vision of the costless and instantaneous global auction market that the Internet could support through the deployment of efficient security procedures.[20] This global auction market could consist of computer agents programmed to search the Internet and execute transactions once necessary variables had been reviewed and accepted by the computer agent on behalf of the real-world principal.

The asymmetric cryptography upon which the Guidelines are based is an essential element to the operation of such a global Internet market. The Guidelines were designed to be a first tentative step from existing commercial systems to this promised land of perfect technological efficiency. This Article suggests, however, that the Guidelines may not be well-rooted enough in contemporary electronic commercial practices to provide a practical bridge from the present to perfect technological efficiency.

[18] *See* JAMES STEVEN ROGERS, THE EARLY HISTORY OF THE LAW OF BILLS AND NOTES 12 (1995). The term "law merchant" refers to the body of law followed in the courts of fairs, markets, and major commercial cities and towns, which is distinct from the common law. *Id.* at 20.

[19] *See* Robert Charles Clark, *Abstract Rights Versus Paper Rights Under Article 9 of the Uniform Commercial Code*, 84 YALE L.J. 445, 476-77 (1975). Dean Clark points out that the "paperizing" of legal rights that were formerly recognized only in abstract form can greatly reduce the costs of administering legal rights; however, paperized rights can be supplanted by central recording systems which may further reduce costs. *Id.* at 477.

[20] *See, e.g.*, Robert Hettinga, *e$: The Wealth of Nation-states,* (last modified June 13, 1996) <http://www.shipwright.com/rants/rant_13.html> (predicting that strong cryptography will aid in the development of instantaneous settlement of trades for cash).

II. WHAT IS THE ORIGIN OF NEGOTIABLE INSTRUMENTS, AND WHAT BUSINESS OBJECTIVES DO THEY SERVE?

While it is now commonplace to question the .relevance of negotiable instruments law,[21] it is useful to discuss briefly the circumstances which gave rise to the doctrines of negotiability and the business functions that these doctrines served in their historical context.

A. Early Origins

Before considering the origins of negotiable instruments, pausing to define the term "negotiable" is worthwhile in the context of this discussion. Because one focus of this Article is the general concept of negotiability and the idea of negotiable instruments as they evolved over time, the definition of a negotiable instrument provided by the most recent version of U.C.C. Article 3[22] is not the most appropriate. Professor Gilmore suggests that the principal attributes of a negotiable instrument are as follows:

> (1) The paper must be freely assignable; no restraints on alienation will be tolerated.
> (2) The debt claim is "merged" into the paper evidencing the claim; thus the paper must be treated in many situations as if it were the claim itself:
>
> . . . .
>
> (3) In pursuing his claim against the obligor, the holder receives the benefit of a series of presumptions which cast on the defendant the greater part of the burden of proof normally

[21] The first academic to address this issue seems to have been Professor Rosenthal. Albert J. Rosenthal, *Negotiability—Who Needs It?*, 71 COLUM. L. REV. 375 (1971). Following his lead were Professors Gilmore, Rogers, and Mann. *See* Gilmore, *Formalism*, *supra* note 4; Gilmore, *Confessions*, *supra* note 14; James Steven Rogers, *The Irrelevance of Negotiable Instruments Concepts in the Law of the Check-Based Payment System*, 65 TEX. L. REV. 929 (1987); Ronald J. Mann, *Searching for Negotiability in Payment and Credit Systems*, 44 UCLA L. REV. 951 (1997).

[22] U.C.C. Article 3 defines negotiable instrument as

> an unconditional promise or order to pay a fixed amount of money, with or without interest or other charges described in the promise or order, if it:
> (1) is payable to bearer or to order at the time it is issued or first comes into possession of a holder;
> (2) is payable on demand or at a definite time; and
> (3) does not state any other undertaking or instruction by the person promising or ordering payment to do any act in addition to the payment of money, but the promise or order may contain (i) an undertaking or power to give, maintain, or protect collateral to secure payment, (ii) an authorization or power to the holder to confess judgment or realize on or dispose of collateral, or (iii) a waiver of the benefit of any law intended for the advantage or protection of an obligor.

U.C.C. § 3-104 (1995).

> carried by plaintiffs in contract actions.
>
> (4) On default by the obligor, the holder has an automatic right of recourse against prior indorsers.
>
> (5) [The purchase is a] "purchase in good faith, without notice and for value":
>
> . . . .
>
> (6) Any holder, even though he took the instrument in bad faith, with notice of defenses, after maturity and without giving value, has all the rights of any prior holder in due course from whom his title derives (provided only that he himself is not a party to any fraud or illegality affecting the instrument).
>
> (7) A holder in due course, or a holder whose title is derived from such a holder, holds the instrument free both of equities of prior owners of the instrument, and of defenses of the obligor except the so-called "real" defenses.[23]

While the doctrines of negotiability have evolved over time, many legal professionals often fail to recognize the degree to which these doctrines have changed and developed in responsè to changing commercial circumstances.[24] It is therefore necessary to review in summary fashion the historical origins of negotiability, its great significance in nineteenth- and early twentieth-century commercial practice, and its more recent decline in importance.

The traditional account of the development of negotiable instruments law begins in the Middle Ages with the development of the Lex Mercatoria, or law merchant.[25] The law merchant originated from the need to articulate customs and norms governing trading activities as merchants transacted in fairs located in many diverse regions of Europe in the Middle Ages.[26] The law merchant consisted of legal customs that developed through this trading activity. These customs were applied to resolve disputes that arose between merchants at trade fairs. Merchant customs were not considered part of the law of the territorial sovereign where the dispute arose or was adjudicated, but rather reflected the norms of the nomadic merchant community.[27] In England, the relationship between the law merchant and the common law was clarified in 1353 by the Statute of Staples.[28] This created separate courts for the adjudication of commercial disputes with a special focus on disputes arising out of the trade of staple commodities, which the king wished to promote.[29] Some of the earliest surviving records of negotiable instruments are

[23] Gilmore, *Good Faith*, *supra* note 15, at 1064-66 (citations omitted).

[24] *See* Rogers, *supra* note 13, at 267.

[25] *See generally* ROGERS, *supra* note 18, at 20; 8 WILLIAM S. HOLDSWORTH, A HISTORY OF ENGLISH LAW, 113-14 (1926).

[26] *Id.* at 21.

[27] *Id.* at 21-22.

[28] Statutes of Staples, 1353, 27 Edw. III.

[29] *Id.*

found in the records of the staple courts.[30]

Part of the conventional history of the development of negotiable instruments law has been the hostility of the common-law courts to the enforcement of merchant custom and to the legitimate business interests of merchants. Because of this conflict between merchant customs, such as negotiability and the general law governing obligations, that common-law courts applied through the writ system, the merchant community avoided using the courts of territorial sovereigns to resolve its disputes. This wholesale avoidance of the common-law courts by merchants was believed to have lasted until the incorporation of the law merchant into the common law through the work of eighteenth-century jurists such as Lord Mansfield.[31] The incorporation of the law merchant took place in large part through Lord Mansfield's practice of impaneling special juries composed of merchants to advise him on the nature of merchant custom, which then became part of the common law through the holdings of his reported decisions.[32]

This account of how the common law incorporated the law merchant highlights the novelty of commercial law doctrines and their marked departure from common-law norms. One classic example of this divergence is the difference between the general common-law principle of derivative title and the commercial doctrine of bona fide purchase.[33] Under derivative title, the transferee receives no greater rights than the transferor had to give. Under bona fide purchase, a transferee who takes in good faith and without notice of infirmities in the transferor's title may take free of those infirmities, effectively granting the transferee better title than that possessed by the transferor. This divergence between common-law and law merchant norms is thought to reflect the development of a clear body of legal rules within the law merchant.[34] The law merchant, prior to its incorporation, presumably included certain highly formalistic rules such as those governing negotiability or bona fide purchases because such formal rules were thought essential to support the rise of commerce.[35] In the case of negotiable instruments law, the development of bills and notes as a form of circulating currency in the era prior to regulated private banking institutions depended on the application of doctrines such as the holder in due course rule to certain contracts evidencing an obligation to pay money.[36]

However, recent scholarship has cast grave doubts on this conventional wisdom. It now seems unlikely that the origins of modern commercial law originate either in the hostility of the common law to the law merchant or in the incorporation

[30] *See* ROGERS, *supra* note 18, at 22.

[31] *Id.* at 24.

[32] Edward L. Rubin, *Learning from Lord Mansfield: Toward a Transferability Law for Modern Commercial Practice*, 31 IDAHO L. REV. 775, 780-82 (1995).

[33] The negotiable instruments doctrine of holder in due course is only one example of the bona fide purchase doctrine found throughout many areas of commercial law. *See* Gilmore, *Confessions*, *supra* note 14, at 607.

[34] Rogers, *supra* note 13, at 270 n.6 (citing J.M. OGDEN, THE LAW OF NEGOTIABLE INSTRUMENTS 9-10 (1909)).

[35] *See* Rogers, *supra* note 13, at 270.

[36] *Id.*

of the law merchant into the common law through the work of path-breaking jurists such as Lord Mansfield.[37] Commercial law cases were litigated in the king's courts throughout the period when merchants were thought to be unwilling to submit to the jurisdiction of territorial sovereigns.[38] The records of proceedings in the king's courts obscured the impression of infrequent commercial litigation by focusing almost exclusively on aspects of the writ system that are now thought of as procedural matters to the exclusion of the substantive elements of the cases.[39] As a result of this focus, it is often difficult to determine what was the substantive law at issue in all types of early cases, making commercial disputes indistinguishable from other disputes in the remaining written records. The written records that specified commercial cases which survive indicate the commercial matters were litigated as part of the general law governing obligations, without any indication that the parties sought the recognition of distinctive mercantile customs that diverged from the common law reflected in the writ system, and without any indication that similar cases brought in mercantile courts proceeded any differently.[40] The notion that commercial law developed apart from and in opposition to the common law seems to have originated much later, and to have been developed to legitimate innovations in commercial law and practice through the invocation of romantic, mythic notions of a formerly autonomous body of commercial custom.[41]

B. Classical Negotiability

The basic outlines of negotiable instruments law were clear in the common law by the eighteenth century.[42] The law of bills provided for transferability free from certain defenses that might be raised in common law actions, as well as certain procedural conventions that permitted their enforcement more rapidly than general contractual obligations.[43] In the prototypical transaction, a bill was created when a creditor instructed his or her debtor to pay over some part of the amount owed the creditor to a third party by issuing a draft.[44] Bills were issued for a variety of

[37] *See, e.g.*, ROBERT BRAUCHER & ROBERT A. RIEGERT, INTRODUCTION TO COMMERCIAL TRANSACTIONS 151 (1977) (noting that Mansfield handed down rules "that had been merchants' law for centuries").

[38] ROGERS, *supra* note 18, at 27.

[39] *See id.* at 19.

[40] *See id.* at 54.

[41] *Id.* at 150, 220. The process of inventing a mythic legal past in order to justify contemporary innovation without acknowledging it as such is described in J.G.A. POCOCK, THE ANCIENT CONSTITUTION AND THE FEUDAL LAW 261-64 (2d ed. 1987). Pocock discusses the role played in English political history by the anachronistic notion of an "ancient constitution," including the idea that the king as well as the people are subject to the law of the land, in the Glorious Revolution of 1688. *Id.* at 231-32.

[42] ROGERS, *supra* note 18, at 1-2.

[43] *Id.* at 125-27.

[44] *Id.* at 33-34.

purposes, including to settle debts and to evidence an extension of credit.[45]

In the early eighteenth century, merchants attempted to expand the application of negotiability doctrines from drafts to promissory notes. In two celebrated opinions, Chief Justice Holt declined to recognize this innovation.[46] These opinions were overruled by Parliament in the statute of 3 & 4 Anne, c. 9, which provided that promissory notes were negotiable in the same manner as bills.[47] Justice Holt's reasoning is a significant source of the myth of an autonomous law merchant and the hostility of common law institutions to him, although this is inaccurate as a reading of the case and as a surmise regarding the larger questions of legal history.[48]

The Statute of Anne was the law at issue in *Overton v. Tyler*.[49] In that case, two creditors were claiming priority in the distribution of the proceeds of a sheriff's sale of the debtor's goods, and the dispute was resolved by comparing the dates on which their respective judgments against the debtor were delivered to the sheriff. However, the second-in-time creditor objected that the first-in-time creditor's judgment was invalid because it was a judgment on a promissory note, and the debtor had not received the three-day grace period following presentment and dishonor as required under the Statute of Anne. Chief Justice Gibson ruled against the second-in-time creditor because the promissory note contained additional terms not authorized by the Statute of Anne; therefore, it was not a "courier without luggage." Thus, none of the provisions of the Statute of Anne, including the grace period, applied.[50]

Overton v. Tyler was handed down in 1846, toward the end of what Professor Rogers labels the "classical" era of negotiability, a period from the early eighteenth to the early nineteenth centuries.[51] During this era, negotiable bills and notes played a vital role in providing the necessary liquidity to finance the expansion of commerce and the inception of the industrial revolution. The amount of metallic currency in circulation was inadequate to meet the needs of transacting parties, and the pillar of the modern American payment system, the check, had not yet been developed.[52] The volume of negotiable bills and notes in circulation expanded to fill the vacuum, providing a sufficiently convenient and reliable alternative to specie to meet the demands of the rapidly expanding English and American economies.[53]

This expansion of the role of negotiable instruments was hardly uncontroversial. Professor Horwitz points out that the majority of American colonies did not recognize the negotiability of notes, the Statute of Anne

[45] *See id.* at 32-40.

[46] *Id.* at 177. The cases were *Clerke v. Martin*, 92 Eng. Rep. 6 (1702), and *Buller v. Crips*, 87 Eng. Rep. 793 (1703).

[47] ROGERS, *supra* note 18, at 184.

[48] *Id.* at 186.

[49] 3 Pa. 346 (1846).

[50] *Id.* at 348.

[51] Rogers, *supra* note 13, at 267.

[52] Gilmore, *Formalism*, *supra* note 4, at 447.

[53] *Id.* at 447-48.

notwithstanding.[54] In the colonies and in the early years of the republic, courts struggled to reconcile their concern with the plight of the maker of a note, who lost the right to raise legitimate defenses such as fraud if the note was negotiable and payment was sought by a holder in due course, with the economic need for a circulating currency composed of negotiable instruments.[55] The lack of uniformity in the enforcement of the doctrines of negotiability in state courts led holders of instruments to seek enforcement in federal courts. The Supreme Court endorsed this strategy in *Swift v. Tyson*,[56] when it found that federal courts could apply federal common law in commercial cases because commercial law doctrines were common to all jurisdictions and there was a need for uniformity in the application of the law.[57]

However, by the middle of the nineteenth century, demand for a circulating currency composed of bills and notes was already diminishing.[58] By the beginning of the twentieth century, currency reforms and modern uses of bank credit such as checking accounts had rendered the use of mercantile bills of exchange as currency obsolete.[59] Yet the doctrines of negotiability did not wither and die when the original business necessity that supported their development faded. Instead, the doctrines of negotiability redoubled in importance as they were applied to a wide range of new transactions. These transactions included conditional sales, or promissory notes issued by borrowers to banks that were not intended to circulate,[60] investment securities such as share certificates,[61] municipal bonds,[62] documents of

[54] MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW, 1780-1860, at 214 (1977).

[55] *Id.* at 218.

[56] 41 U.S. 1 (1842), *overruled by* Erie R.R. v. Tompkins, 304 U.S. 64, 79 (1938).

[57] In writing for the Court, Justice Story stated that Section 34 of the Judiciary Act of 1789,

> upon its true intendment and construction, is strictly limited to local statutes and local usages of the character before stated, and does not extend to contracts and other instruments of a commercial nature, the true interpretation and effect whereof are to be sought, not in the decisions of the local tribunals, but in the general principles and doctrines of commercial jurisprudence. Undoubtedly, the decisions of the local tribunals upon such subjects are entitled to, and will receive, the most deliberate attention and respect of this Court; but they cannot furnish positive rules, or conclusive authority, by which our own judgments are to be bound up and governed. The law respecting negotiable instruments may be truly declared in the languages of Cicero, adopted by Lord Mansfield in Luke v. Lyde, 2 Burr. R. 883, 887, to be in a great measure, not the law of a single country only, but of the commercial world.

41 U.S. at 19. Justice Story was the author of two leading commercial law treatises of the day. *See* JOSEPH STORY, COMMENTARIES ON THE LAW OF BILLS OF EXCHANGE, FOREIGN AND INLAND, AS ADMINISTERED IN ENGLAND AND AMERICA (1843); JOSEPH STORY, COMMENTARIES ON THE LAW OF PROMISSORY NOTES, AND GUARANTIES OF NOTES, AND CHECKS ON BANKS AND BANKERS (1845).

[58] Gilmore, *Formalism*, *supra* note 4, at 452.

[59] *Id.*

[60] *See* Gilmore, *Good Faith*, *supra* note 15, at 1093.

[61] *Id* at 1075.

[62] *Id.* at 1090-91.

title,[63] chattel paper,[64] and mortgage notes.[65] This rapid and multifaceted expansion of the doctrine of negotiability into various types of commercial transactions was accomplished because commercial lawyers believed that by doing so, the value of property exchanged in such transactions could be increased by removing obstacles to the free transferability of that property.[66]

This triumph of the doctrine of negotiability across so many categories of commercial transactions can be seen as part of a process described by Dean Clark as "paperizing" rights.[67] Dean Clark suggests that the progress of commercial law can be thought of as a movement away from primitive systems in which the entitlements of the parties are mere abstract ideas reflected only in the memories of the parties. In such a system, the costs of enforcing transfers of entitlements from one party to another are high, as is the risk of fraud and error.[68] A subsequent advance from a system of purely abstract entitlements is a system of possession in which entitlements are demonstrated through physical control of assets. While simpler to administer than the abstract entitlement system, a possessory system is severely limited in the types of entitlements it can administer.[69] When rights to tangible and intangible property are written down on paper, then many of the problems of the abstract and possessory models are eliminated. If a further step is taken, the paper that describes the entitlement can be treated as the embodiment of the abstract right it represents, and transfers of possession of the paper can be used to effect transfers of the underlying entitlement.[70] The rapid expansion of the doctrine of negotiability, which is a system for administering papers that embody abstract rights, seems to be driven by the desire of parties to commercial transactions to achieve the type of transactional efficiencies that Dean Clark suggests result from paperizing abstract rights.

C. *Modern Decline in Significance*

Simply paperizing rights does not represent the most efficient method of transferring entitlements to commercial property. Central recording or filing systems can be combined with paperized rights to permit the paper embodiment of the right. Also, notice of transfers of the paper embodiment can be kept in a central system to which potential transferees may refer.[71] Examples of registry systems combined with paperized rights include real property records offices and U.C.C. filing offices maintained by each state or local jurisdiction. Also, the centralized securities clearance system maintained by the Depository Trust Company and the

[63] *Id.* at 1077.
[64] *Id.* at 1081.
[65] *Id.* at 1082.
[66] *See* Gilmore, *Confessions*, *supra* note 14, at 611.
[67] Clark, *supra* note 19, at 476.
[68] *Id.* at 473-74.
[69] *Id.* at 475-76.
[70] *Id.* at 476-77.
[71] *Id.* at 478.

National Securities Clearing Corporation is a registry system combined with paperized rights because the basis for all registry entries reflecting transfers of rights are "jumbo" certificates representing millions of shares retained by the Depository Trust Company in its vaults.[72]

A further step beyond registries combined with paperized rights are modern systems designed to take full advantage of the efficiencies information technology can offer. Such systems include uncertificated securities such as mutual fund shares, U.S. Treasury obligations, and secondary mortgage obligations such as pass-through certificates offered by the Government National Mortgage Association and the Federal Home Loan Mortgage Corporation.[73] In addition, many modern electronic payment systems that support automated teller machines might be considered electronic registries that do not rely on paperized rights in their operation. The European Commission has provided support to BOLERO, a central electronic registry service for international trade documents that is expected to become operational in 1998.[74]

D. Negotiability as a Loss Allocation System

Under modern conditions of falling communications and information processing costs, registry systems can provide greater certainty to transferees of rights at a lower cost than systems based on paperized rights. However, the decline in significance of the doctrines of negotiability is not only a reflection of the emergence of new information technologies that reduce the costs of maintaining private centralized registry-like systems to administer transfers of entitlements. The attempt by unscrupulous merchants to cut off valid defenses against themselves or their associates through the application of doctrines of negotiability to consumers was resisted first by courts[75] and then by the Federal Trade Commission (FTC), which passed a blanket prohibition on the application of holder in due course doctrines in commercial transactions.[76] In transactions between two parties in business, it may be reasonable to expect that the transactors understand the fundamentals of negotiability and are prepared to accept the risks associated with it, such as the possibility of being haled into court by an adversary armed with extraordinary procedural advantages. It seemed obvious to most observers at the

[72] U.C.C. Revised Article 8, Prefatory Note I(D) (1995).

[73] *Id.* I(C).

[74] Andrew Reinbach, *Bringing Trade Documentation into the 20th Century*, BANK SYSTEMS +TECHNOLOGY, Feb. 1997, at 23, 23.

[75] Gilmore, *Good Faith*, *supra* note 15, at 1093-1102.

[76] Holder in Due Course Rule, 16 C.F.R. § 433.2 (1997). The FTC holder in due course regulations were first enacted in 1971. *See* JAMES J. WHITE & ROBERT S. SUMMERS, UNIFORM COMMERCIAL CODE 530 (4th ed. 1995). However, in certain consumer transactions abuses still exist where negotiable instruments are used to finance fraudulent home improvement schemes. *See* Julia Patterson Forrester, *Constructing a New Theoretical Framework for Home Improvement Financing*, 75 OR. L. REV. 1095, 1111 (1996).

time, however, that this was too high a standard to expect from consumers.[77]

The FTC rule was designed to transfer the costs of fraud and malfeasance on the part of merchants to creditors who are better equipped than consumers to absorb losses on individual transactions or to seek compensation from the corrupt merchant.[78] This recasts a problem in the development of legal doctrine as a problem in managing social costs or in allocating losses.[79] A system for managing the transaction costs associated with transfers of entitlements can include loss spreading, loss reduction and loss imposition principles.[80] Viewing the traditional doctrines of negotiability in this light, it becomes clear that negotiability offers the parties a decentralized, individualistic loss-reduction, and loss-imposition system. This is in marked contrast with some more modern commercial transaction systems, such as the credit card system, which primarily relies more on centralized loss reduction and loss spreading policies.[81]

Some of the risks associated with commercial transactions include the following: the vendor may not have good title to the asset being transferred; the purchaser may not be able to pay the agreed amount or the payment, once received, will later be revoked; and the vendor may falsely represent the subject matter of the transaction. A centralized system for pooling the risks of commercial transactions under negotiability doctrines is difficult to establish for several reasons. The traditional model of a commercial transaction tacitly assumed by negotiable instruments law involves isolated dealings between natural persons who may be strangers and for whom litigation is the ultimate enforcement mechanism for shifting losses once they occur. With regard to the classical era of negotiability in the eighteenth and nineteenth centuries, the idea of establishing a large, centrally administered risk pool for commercial transactions is anachronistic. Until very recently, the overhead of setting up a centralized risk spreading system was prohibitive if the normal transactions were isolated, discrete transactions between strangers.

Parties to negotiable instruments transactions are thus pushed to manage risks on an individual basis and to self-insure. Risk management is easier to accomplish for a party who engages in enough transactions to create its own risk pool whose net worth is large in relation to the amount at issue.[82] Likewise, risk management

[77] White and Summers, after voicing their objections to the procedure used by the FTC to effectively abolish the holder in due course doctrine in consumer transactions, state: "While we do not share the belief of FTC zealots that it was the most awful thing in Western jurisprudence, we believe that on balance the world is better off with abolition of the holder in due course doctrine in consumer transactions." WHITE & SUMMERS, *supra* note 76, at 531.

[78] Preservation of Consumers' Claims and Defenses, 40 Fed. Reg. 53,506, 53,523 (1975); Forrester, *supra* note 76, at 1107-08.

[79] The modern law and economics literature that recasts doctrinal issues as economic efficiency questions began with R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960), and Guido Calabresi, *Some Thoughts on Risk Distribution and the Law of Torts*, 70 YALE L.J. 499 (1961).

[80] Robert D. Cooter & Edward L. Rubin, *A Theory of Loss Allocation for Consumer Payments*, 66 TEX. L. REV. 63, 70 (1987).

[81] *See id.* at 97.

[82] *See id.* at 71.

is more difficult for those parties who engage in few transactions or whose net worth is small in relation to the amount at issue. A collective insurance system for risks associated with negotiable instrument transactions is not impossible. Many retail merchants who accept checks from the public now have alternatives to self-insurance. For a small charge on each transaction, they can purchase indemnity from a commercial check guaranty service that assumes the costs of collecting dishonored checks. However, these indemnity services are not available to consumers that accept negotiable instruments as payment.

Although loss spreading is generally incompatible with the structure of traditional negotiability doctrines, negotiability permits loss imposition and loss reduction to take place. Loss imposition is accomplished not only through the special procedural privileges enjoyed by a holder in due course. Specifically, transfer warranties protect the final purchaser of an instrument from losses that might arise from defects in title without regard to whether the purchaser qualifies as a holder in due course.[83]

Loss reduction strategies can be implemented by any party who, under the loss imposition provisions of negotiable instruments law, would be stuck with the cost of fraud, error, or failure of one of the parties to the transaction to fulfil its performance obligations. The maker or drawer of a negotiable instrument needs to recognize that in return for the lower cost of financing a transaction which results from the choice of documenting the obligation to pay as a negotiable instrument, the maker or drawer is assuming a greater risk of losing the right to assert otherwise valid contract defenses. The classic fact patterns used to teach negotiability doctrines involve disputes between two "innocents"—neither party is directly responsible for the fraud, error, or default giving rise to the loss—yet, the true malfeasor or incompetent is judgment proof or is beyond the court's jurisdiction. Negotiability provides a mechanism for assigning the loss to one of the two innocent parties.

The loss imposition rules of negotiable instruments law can produce outcomes that seem unduly harsh in some contexts such as when holder in due course doctrines are applied to consumers. The apparent harshness of these rules is comprehensible in light of the historical circumstances under which negotiability developed, before modern risk pooling schemes were commonplace. If these outcomes are in fact fair, it is because of the willingness of commercial parties to accept a system with clearly defined, well-known rules and to implement loss reduction strategies accordingly.[84]

[83] U.C.C. § 3-416 (1995). Transfer warranties in the current version of U.C.C. Article 3 apply to any "transferee" and include warranties that the transferor is "entitled to enforce the instrument," that all signatures on the instrument are genuine, that "the instrument has not been altered," that there are no defenses which can be asserted against the transferor, and that the transferor has no knowledge of the insolvency of the maker or drawer. *Id.* § 3-416(a)(1)-(5).

[84] In keeping with the tradition of clear rules, older restatements of negotiable instrument law allocated the entire loss for fraud and error to only one of the parties. One of the innovations in the 1990 revisions of Article 3 was a movement away from a contributory negligence standard in the provisions governing allocation of certain fraud and forgery losses toward a comparative fault

In the classical era of negotiability, familiarity with negotiability rules could be considered a form of human or social capital which transactors might try to use to their competitive advantage.[85] To the extent that the parties to a transaction know and understand negotiable instruments law, they can reduce the direct costs of executing the transaction by taking advantage of the formal standards of negotiability to structure and document the transaction. Negotiability was applied to a wide range of commercial transactions in the late nineteenth and early twentieth centuries in part to achieve the transactional efficiencies that result from the application of a well-defined, widely used set of rules.[86]

While it may be reasonable to apply doctrines of negotiability to commercial parties, it is less certain that the same conclusion should prevail in transactions in which one party is a consumer. Consumers are at a disadvantage in many commercial transactions because the costs of trying to negotiate a deal that varies from the standard form contract are disproportionately high for the consumer. In addition, the costs of achieving an equivalent mastery of the information needed to make a rational decision in each transaction disfavors the consumer.[87] As repeat players in many of their commercial transactions, commercial parties can afford to invest in structuring transaction forms and developing loss-reduction expertise for routine types of transactions. However, consumers are often infrequent participants in many markets; thus, an equivalent investment by a consumer would dwarf the value of any individual transaction and would be difficult to justify on efficiency grounds. Because consumers cannot be expected to develop an adequate familiarity with the doctrines of negotiability, they cannot appreciate the amount and nature of loss-avoiding procedures that should be adopted to lower the risk of being forced to accept a loss for fraud, error, or other problem such as insolvency by another transactor.

The significance of negotiability may be declining in many nonconsumer commercial transactions. Professor Mann has studied contemporary commercial practices and discovered that the focus of traditional negotiability on merging abstract rights with pieces of paper now imposes substantial costs on businesses.[88]

standard that permits a court to divide the loss between the parties based on their relative fault. *See* U.C.C. § 3-406 cmt. 4 (1995).

[85] Investments in human capital are "activities that influence future monetary and psychic income by increasing the resources in people . . . . The many forms of such investments include schooling, on-the-job training, medical care, migration, and searching for information about prices and incomes." GARY S. BECKER, HUMAN CAPITAL 11 (3d ed. 1993). Social capital has been defined as a resource that "facilitates production, but is not consumed or otherwise used up in production" . . . and is derived from "ordinarily informal relationships, established for noneconomic purposes, yet with economic consequences." James S. Coleman, *A Rational Choice Perspective on Economic Sociology, in* THE HANDBOOK OF ECONOMIC SOCIOLOGY 166, 175 (Niel J. Smelser & Richard Swedberg eds., 1994).

[86] *See, e.g.*, Gilmore, *Confessions, supra* note 14, at 611-12 (discussing the explosion of accounts-receivable financing and its incorporation into the first uniform receiveables financing statute).

[87] Cooter & Rubin, *supra* note 80, at 68-69.

[88] Mann, *supra* note 21, at 956.

Transactions that are structured to take advantage of modern information technologies and to avoid paperized rights systems like negotiability may be less costly for transactors.[89] Professor Mann's empirical studies mirror the work of earlier jurists who noted the same decline by analyzing the development of legal doctrine. Furthermore, the studies point toward the conclusion that the real economic significance of negotiability has probably been in decline for decades. For example, the check collection system processes papers that are negotiable instruments, yet such a system operates largely without reference to the doctrines of negotiability.[90]

This is not to say that significant exceptions to the general trend do not exist. Issuing commercial paper is a common method of raising working capital for businesses, and it "is generally issued in bearer form and is fully negotiable."[91] Mortgage notes that are eligible for sale to secondary market institutions such as the Federal Home Loan Mortgage Corporation must also be fully negotiable.[92] Under certain circumstances, the Federal Deposit Insurance Corporation enjoys a form of holder in due course status when it acts as receiver to collect on loans in the portfolio of failed financial institutions.[93]

In both commercial and consumer contexts, electronic commerce is supplanting paper-based commercial practices. Large proprietary networks have revolutionized many commercial practices. The rise in importance of wire transfer systems such as Fedwire, maintained by the Federal Reserve Banks, or CHIPS, the wire transfer system maintained by the New York Clearing House Interbank Payment System, led to the creation of U.C.C. Article 4A which governs wholesale funds transfers.[94] The rise of automated clearinghouse funds transfer systems and other electronic funds transfer (EFT) systems that support the retail consumer network of automated teller machines and point of sale payment systems is another other example of a closed, proprietary network that operates on a global scale. Visa, MasterCard, and other major card issuers operate equivalent systems. U.C.C. Article 8 was revised in 1994 in light of the electronic securities transfer system maintained by the Depository Trust Company and the National Securities Clearing Corporation which has dramatically reduced the reliance on paper certificates in national securities markets.[95]

Some of these new systems based on modern information technology incorporate risk spreading, while others retain the decentralized, individualistic loss allocation model that characterizes negotiability. Credit card and consumer EFT transactions are subject to limits on the liability that can be imposed on consumers,

[89] *Id.* at 961-62.

[90] *Id.* at 985.

[91] Rubin, *supra* note 32, at 791.

[92] *See* James A. Newell & Michael R. Gordon, *Electronic Commerce and Negotiable Instruments (Electronic Promissory Notes)*, 31 IDAHO L. REV. 819, 821 (1995).

[93] Marie T. Reilly, *The FDIC as Holder in Due Course: Some Law and Economics*, COLUM. BUS. L. REV. 165, 167-68 (1992).

[94] U.C.C. Article 4A, Prefatory Note, *Why is Article 4A Needed?* (1995).

[95] *See* U.C.C. Revised Article 8, Prefatory Note I(D) (1995).

and as a result, those losses that cannot be imposed on merchants are shifted to the financial institutions which are capable of spreading losses across their consumers' accounts. These losses are then recaptured as higher user fees, which effectively operate as a sort of insurance premium.[96] Within the securities trading system, small investors are protected by account insurance provided by the Securities Investor Protection Corporation, but large investors are at risk if the securities intermediary they have chosen becomes insolvent.[97]

The allocation of risks assumed by banks that make up the wholesale wire transfer system (system banks) when executing their clients' funds transfers is very similar to the loss allocation system of classical negotiability. For example, U.C.C. Article 4A provides that any bank which accepts an order from a client to wire funds to another party must assume the risk of failure of any intermediary bank if the funds transfer is not successful.[98] This rule encourages the implementation of loss reduction strategies by encouraging system banks to avoid intermediary banks whose solvency is at risk, but does not permit any risk-pooling between system participants. As a loss imposition rule, it places the losses such as those caused by the unexpected default of a customer or another bank on the bank that dealt most proximately with the defaulting party. Also, when combined with the requirement that the "money-back guarantee" may not be waived by agreement,[99] it prevents the bank bearing the loss from shifting the loss to a more remote party. A similar result is achieved in many negotiable instrument cases through the operation of indorsement and warranty liability rules.

There are still many commercial transactions in which negotiability (or something like it) plays an important role, although this method is clearly becoming obsolete. Perhaps one obvious successor to negotiability in modern commercial practice are the decentralized, individualistic loss allocation systems used in some modern commercial transaction systems. This type of loss allocation system is not often found in consumer transactions; however, regulatory and market pressures have supported the development of transaction systems for consumer use that

[96] Consumer credit card liability for unauthorized use is limited to $50. Regulation Z, 12 C.F.R. § 226.12(b)(1) (1997). Consumer liability for unauthorized electronic funds transfers may be capped at $50 or $500, depending on the promptness of the consumer in reporting the problem. If the consumer fails to report an unauthorized transfer within 60 days after the financial institution sends a statement, the consumers possible losses may not be capped. Regulation E, 12 C.F.R. § 205.6(b) (1997). If a consumer protests a credit card charge as fraudulent, the loss is shifted to the merchant who originated the charge; alternatively, if recovery from the merchant is not possible, then the acquiring bank who granted a provisional credit on the charge to the merchant is liable. EDWARD L. RUBIN & ROBERT COOTER, THE PAYMENT SYSTEM: CASES, MATERIALS AND ISSUES 781 (2d ed. 1994). The loss spreading within the credit card system takes place when the acquiring bank raises its customers' fees to cover its losses due to merchant fraud.

[97] *See* James Steven Rogers, *Policy Perspectives on Revised U.C.C. Article 8*, 43 UCLA L. REV. 1431, 1469 (1996).

[98] U.C.C. § 4A-402(e) (1995). This is the wholesale wire transfer system's "money back guarantee" to its customers. If the customer designates the intermediary bank, however, it does not apply. *Id.*

[99] U.C.C. § 4A-402(f) (1995).

negotiability, was historically tied with a loss allocation regime that did not support loss-spreading, the modern example of retail check guarantee services shows that negotiability is not incompatible with loss spreading. However, modern electronic transactions systems based on public or private registries have no close historical tie with any system of loss allocation. Some modern electronic systems incorporate a forced insurance system and risk-pooling, while others permit the parties to self-insure and take full responsibility for their own risk management solutions.

Today, the Internet is the frontier of electronic commerce. The Internet offers the promise of transaction costs far below those incurred by transaction systems that rely on mainframe computers and closed, proprietary networks. However, the Internet will not host a large volume of commercial transactions conducted over the Internet until transactors feel satisfied that Internet commerce security approaches that of closed-networks electronic commerce systems. In addition, business solutions must be standardized to permit intersystem compatibility within an open network. Digital signature technology represents the first attempt to resolve some of the security and standardization problems posed by the open, public nature of the Internet.

III. WHAT IS THE ORIGIN OF DIGITAL SIGNATURES, AND WHAT BUSINESS OBJECTIVES DO THEY SERVE?

A. *Military and Commercial Use of Symmetric Key Cryptography*

Digital signatures are a specific application of encryption technology, or cryptography. In turn, cryptography is one element of the larger field of information and computer system security. Computer security takes into account many factors, "including various technical safeguards, trustworthy and capable personnel, high degrees of physical security, competent administrative oversight, and good operational procedures."[100] Until very recently, cryptography has been one of the least used of the available technical safeguards.[101] When it has been used, the mechanics of its deployment have not been widely disseminated. Thus, the appropriate role of cryptographic tools in commercial transaction systems has not been as widely debated or analyzed as other issues at the intersection of information technology and commercial law.[102]

Various forms of encryption have been used to maintain the confidentiality of information for over four thousand years.[103] Encryption involves transforming the

[100] NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 51 (Kenneth W. Dam & Herbert S. Lin eds., 1996).

[101] *Id.* at 51-52.

[102] For example, the introduction of computerized check processing technology in the 1950s spurred debate over electronic payment system issues, and the commercial use of the telegraph in the nineteenth century originated electronic contract formation issues that have been widely debated since the 1980s. See generally RUBIN & COOTER, *supra* note 96, at 108-111 (discussing the development of the law of check collection systems).

[103] *See* DAVID KAHN, THE CODEBREAKERS 68 (1967).

information for over four thousand years.[103] Encryption involves transforming the text to be protected into a form that cannot be deciphered without having a copy of the key used to modify the original text. Simple cryptographic systems operate on the same principle as Captain Midnight decoder rings: a "cipher" is established to transform text into a secure form. The original text is called the "plaintext," and the transformed text is known as the "ciphertext."[104] For example, if the cipher is the alphabet in reverse order, then the plaintext "Captain Midnight" becomes the ciphertext "Xzkgzrm Nrwmrtsg." The process of converting plaintext to ciphertext is a function of the encryption algorithm.[105]

In 1949, Claude Shannon established the scientific basis for modern cryptography with the development of information theory which provided a mathematical basis for analyzing cryptographic systems.[106] Modern encryption technology is based on using a complex mathematical function in combination with a unique number which serves as the encryption key to transform plaintext into ciphertext. Once a message has been encrypted, it can be decrypted by running it through a second complex function together with an encryption key.[107] In private key, or symmetric cryptography, the same secret key is used both to encrypt and decrypt. In public key, or asymmetric cryptography, two different but mathematically related keys are used for encryption and decryption.[108] Some of the relevant differences between public key and symmetric key cryptosystems in electronic commerce are discussed below.

The quality of encryption technology security is measured by how resistant an encrypted message is to being decrypted by someone who does not have the secret key.[109] The simplest way to try to break an encoded message is a "brute force" attack, which consists of trying every possible key until the correct key is found.[110] "Because of the rapidly decreasing cost of computation, cryptographic systems that cost $1 billion to break in 1945 can be broken for approximately $10 today."[111] Because this trend is expected to continue into the future, cryptographic systems being designed to support electronic commerce applications today should have large safety margins to protect against the effects of future advances in technology.

Although the functions used to encrypt and decrypt messages are available on many computers, controlling access to the encryption key ensures the confidentiality of the encrypted message.[112]

The longer the encryption key, the harder it is for someone without access to

[103] *See* DAVID KAHN, THE CODEBREAKERS 68 (1967).

[104] *See* NATIONAL RESEARCH COUNCIL, *supra* note 100, at 374.

[105] *Id.*

[106] *Id.* at 364. Shannon's seminal work is CLAUDE E. SHANNON & WARREN WEAVER, THE MATHEMATICAL THEORY OF COMMUNICATION (1963).

[107] NATIONAL RESEARCH COUNCIL, *supra* note 100, at 374.

[108] *Id.* at 375.

[109] *See id.* at 378.

[110] *Id.* at 379-81.

[111] *Id.* at 384.

[112] *Id.* at 377.

the key to decrypt the ciphertext. The length of the number used for the secret key is expressed in bits, such as a 56-bit key. Each bit in a key can be 1 or 0, so for a 56-bit key there are 2^{56}, or 72,057,594,037,900,000, possible different keys.[113] The Data Encryption Standard (DES), adopted as a U.S. government standard in 1977 and as an American National Standards Institute Standard in 1981, uses a 56-bit key.[114] If the attacker had the capability to test a billion keys a second, it would take 834 days to test all possible keys.[115] In other words, by using technology available in 1998, it is possible for someone with enough time and money to break a message encrypted with a 56-bit key. In 1996, a computer equipped with an application specific chip could test 30 million DES keys per second.[116] It is estimated that a government agency willing to invest $300 million in an array of such chips could break a DES key in 12 seconds.[117] While it is unlikely that any government in the world currently possesses such equipment, rapidly falling prices for information processing power make it difficult to predict when a government's security or military agencies will possess such capabilities.[118]

A longer key makes the encryption more difficult to crack by several orders of magnitude. According to another estimate, it would take 70,000 years to decrypt a file protected by an 80-bit key using technology available in 1998.[119] To decrypt a message encrypted with a 128-bit key with technology available in 1998, it would take longer than current estimates for the life of the universe.[120] Thus, while cracking any message encrypted with modern encryption technology is not easy, encryption with longer secret keys is significantly more secure.

The first applications of computer-based encryption technology in the United States were in the military and financial institutions.[121] In response to military needs, the U.S. Department of Defense (DoD) developed early computer security standards. By the 1980s, the DoD issued Trusted Computer System Evaluation Criteria (TCSEC) as standards for information system security, including the management of cryptosystems. Although systems developed according to TCSEC are considered trustworthy systems, the standards in TCSEC reflect conditions that characterize military rather than private commercial security applications.[122] For example, TCSEC places more emphasis on confidentiality and less emphasis on integrity and availability of resources, issues of greater concern in private

[113] SIMSON GARFINKEL, WEB SECURITY AND COMMERCE 190 (1997).

[114] *Id.* at 193. Garfinkel notes that the DES command only gives access to keys expressed as hexidecimal numbers, which reduces the number of keys actually available in DES by 90% to 7,213,895,789,838,340 (96^8). *Id.* at 190.

[115] *Id.*

[116] DONAL O'MAHONY ET AL., ELECTRONIC PAYMENT SYSTEMS 24 (1997).

[117] *Id.*

[118] BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 300 (2d ed. 1996).

[119] William Wong, *How Safe is Internet Traffic?*, PC WEEK, Oct. 27, 1997, at 116, 118. In 1993, a computer capable of breaking DES keys in 3.5 hours was estimated to cost $1 million. SCHNEIER, *supra* note 118, at 300.

[120] *Id.*

[121] RITA C. SUMMERS, SECURE COMPUTING: THREATS AND SAFEGUARDS 41 (1997).

[122] *Id.*

information systems.[123] TCSEC also reflects the security concerns of an earlier generation of computer technology, which becomes more apparent as multiuser mainframe computers are displaced by distributed computer networks. Furthermore, compatibility of security standards between users is a crucial issue for electronic commerce that was not addressed in TCSEC.[124] Similarly, secure military messaging systems developed for DoD are poorly suited for commercial applications because they rely on a rigid hierarchy and facilitate top-down communications only.[125]

United States banking and financial institutions have created a vast and highly reliable network of computers that provide electronic funds transfers throughout the world. The movement toward automated financial services began in the 1950s with the expansion of retail banking services and the development of "full service" banking.[126] The automation of the check collection process and the movement of banks into the credit card business reflect this trend. In the 1960s, banks began to develop EFT systems using computer technology that had been acquired to support check processing. A nationwide EFT network was established, including a chain of ACHs and networks of automated teller machines (ATM).[127] The 1970s brought predictions that the checkless society was imminent, based on the assumption that the electronic funds transfer system would expand to include point-of-sale (POS) payment functions. However, the public proved more resistant to the replacement of paper checks with electronic funds transfers than anticipated, and it was not until the 1990s that retail POS EFT services began to achieve significant market share.[128]

During the 1960s and 1970s, the wholesale wire transfer system was developed for the commercial banking services market. In the early 1970s, Fedwire was created to automate funds transfers through the Federal Reserve System. At the same time, the New York Clearinghouse Association established CHIPS. The Society for Worldwide Interbank Fund Transfers (SWIFT) began operations in 1977 as a secure communications network that, unlike the Fedwire or CHIPS, does not provide settlement functions.[129]

Through the development of these and other proprietary systems such as the communications networks that provide for central-switch transmission of messages between participants in the credit card system, financial service providers in the United States have built one of the largest electronic commerce networks in the world. In developing these networks and the services they support, financial

[123] By contrast, digital signature technology does not provide confidentiality of the message text, but guarantees the integrity of the message and protection against its later repudiation by the apparent sender. *See infra* text accompanying notes 149-51.

[124] SUMMERS, *supra* note 121.

[125] *See* FORD & BAUM, *supra* note 9, at 271.

[126] *See* DONALD I. BAKER & ROLAND E. BRANDEL, THE LAW OF ELECTRONIC FUNDS TRANSFERS ¶1.01 (3d ed. 1996).

[127] *Id.*

[128] *Id.*

[129] *Id.* ¶1.03[9].

institutions have developed comprehensive approaches to security.[130] This includes policies to safeguard the financial institution's central processing facilities from physical damage, breaches in employee security procedures, and software failures.[131] In addition, encryption may be used for communications between remote locations and the central processing facilities.[132] To secure customer access at remote locations, financial institutions will generally issue cards and personal identification numbers to customers which control access to customer funds. In addition, financial remote access providers may take steps in designing the ATM facility, such as installing a surveillance camera, to minimize the risk that customers will be attacked or observed while accessing funds.[133]

With the exception of possessing a magnetic strip card or remembering the personal identification number (PIN) for consumer EFT access devices, security systems are transparent to the retail consumer of electronic financial services. Because of consumer protection regulations, financial service providers absorb the costs of most security failures of retail financial electronic service networks, even if caused by the consumer.[134] This allocation of liability in favor of the institutional transactor has prompted institutional participants in these systems to invest heavily in security technology. Security procedures now used by credit card issuers to combat fraud include mailing inactive cards that require cardholders to make contact with the issuer by telephone to activate the card, placing holograms on the card to make reproduction of the card more difficult, placing a photograph of the cardholder on the card to improve the accuracy of identification checks, and encoding the magnetic strip with algorithms that aid in matching the card with the proper cardholder.[135] In addition, neural network technology can be used to compare cardholder usage with known patterns of fraud, and expert or rules-based systems can be programmed to react when established parameters of activities are exceeded.[136]

In commercial wire transfer services, the customer and the bank must agree to commercially reasonable security procedures for the bank to avoid liability for unauthorized transfers from the customer's account.[137] If a bank has executed an unauthorized funds transfer instruction after the bank has established an economically reasonable security procedure, the bank's customer can avoid liability for the amount of the funds transfer by showing that the bank did not follow the security procedure, or the instruction did not originate with personnel or facilities

[130] *See* Susan Hubbell Nycum, *Security for Electronic Funds Transfer System*, 37 U. PITT. L. REV. 709, 710 (1976).

[131] BAKER & BRANDEL, *supra* note 126, ¶19.05[1].

[132] *Id.* ¶19.05[2].

[133] *Id.* ¶19.05[3].

[134] *See* Regulation Z, 12 C.F.R. § 226.12 (1997); Regulation E, 12 C.F.R. § 205.6 (1997).

[135] *Technology Stems Credit Card Fraud,* 13:24 Financial Services Report, Nov. 20, 1996, *available in* LEXIS, Bankng Library, Philps File.

[136] *Id.*

[137] *See* U.C.C. § 4A-202(a), (b) (1995); U.C.C. § 4A-201 (1995) (defintion of "security procedure").

under the customer's control.[138] The loss allocation rules place the risk of unauthorized payment orders initially on the bank, but permit the bank to shift liability to the customer by insuring that the customer implements a commercially reasonable security procedure. However, if the customer can meet the substantial burden of proving that a loss was not his or her fault, then the bank is forced to absorb the loss.

Symmetric cryptography is commonly employed within well-established electronic financial services networks. The Data Encryption Standard (DES) is the most widely used form of encryption technology in financial services networks.[139] In the early 1970s, when the military accounted for most cryptography research, IBM developed and marketed the DES algorithm. At the same time IBM was independently developing DES, the National Bureau of Standards (NBS), later renamed the National Institute of Standards and Technology (NIST), issued a call for proposals of a standard encryption algorithm.[140] After testing the algorithm to determine its security and suitability for a national standard, the NBS entered into a nonexclusive, royalty-free license that permitted the use of DES as a standard form of encryption. After a period of public comment, DES was adopted as a federal standard in 1976.[141] In 1981, the American National Standards Institute (ANSI) approved DES as a private sector standard. The ANSI Financial Institution Retail Security Working Group developed a DES-based standard for authentication of retail financial messages. The American Bankers Association also adopted a standard recommending DES for encryption.[142] Because the DES algorithm has been widely known and used for decades, financial institutions may use Triple-DES as an alternative to DES to decrease the possibility that a DES could be decrypted by a simple brute-force attack.[143] Triple-DES uses the DES algorithm three times, incorporating two different keys to achieve greater security, and is an appealing choice for financial institutions which have already installed DES equipment.[144]

DES is a symmetric key cryptography system, which means the same key is used to encrypt and decrypt the plaintext. The administration of symmetric key systems within closed systems is a serious but not unmanageable problem. The primary key management problem within symmetric key systems is finding a way to distribute the keys to those who need them without compromising the security of the keys in transit.[145] One solution is to take a page from the old James Bond novels, give the key to a courier in a sealed briefcase, and handcuff the briefcase to the courier. If the courier fails to arrive or the seal is broken, then the key is

[138] *See* U.C.C. § 4A-202(b), 4A-203(a)(2) (1995). The customer might also be able to avoid liability by showing the bank acted in bad faith. U.C.C. § 4A-202(b)(ii) (1995).

[139] SCHNEIER, *supra* note 118, at 265-268.

[140] *Id.*

[141] *Id.*

[142] *Id.*

[143] O'MAHONY ET AL., *supra* note 116 at 25.

[144] *Id.*

[145] SIMSON GARFINKEL, PGP: PRETTY GOOD PRIVACY 45 (1995).

presumed compromised and not used.[146] The overhead associated with such a distribution system may not be significant in the context of national security during the Cold War, but is obviously too great for mainstream electronic commerce applications today. Another shortcoming of symmetric key cryptography is that it cannot be used between parties with no prior contact because they must first find a way to share copies of the key. One solution is to create a central key distribution system. However, a key distribution system may create more problems than it solves because the individuals who run the key distribution system may not be as trustworthy as they should be.[147] The key management problems of symmetric key cryptography can be avoided by using asymmetric or public key encryption, which is the heart of digital signatures.

B. Public Key Cryptography and Its Promise for Open Network Commerce

The first public key system was described in 1976 by Whitfield Diffie and Martin Hellman.[148] A short time later, Ronald Rivest, Adi Shamir, and Len Adelman developed another public key system.[149] The great advantage of a public key system is that it permits individuals to use two different but related keys to maintain the confidentiality of their communications. One key, the private key, is kept secret by the owner, while the other key, the public key, can be widely distributed. The two keys are mathematically related, but one of the features of public key cryptography is that it is computationally infeasible to derive one key from knowledge of the other.

It is a convention among those who try to explain public key cryptography to the uninitiated to use hypotheticals populated with Alice, Bob, and Carol.[150] In a public key cryptography system, Alice and Bob exchange public keys. When Bob wants to communicate securely with Alice, he uses her public key to encrypt a message, confident that no one other than Alice may decrypt the message. If Alice wants to send Bob a message and provide Bob with confidence that it must have come from Alice, Alice may encrypt her message with her private key. After Bob receives the message, he decrypts it with his copy of Alice's public key, certain that the message originated with Alice.

The most secure system for exchanging keys in a public key cryptography system is like the most secure system for distributing private keys: a face-to-face transaction between parties with a prior acquaintance. If Alice and Bob feel confident of the security of their e-mail communications, they can exchange public

[146] *Id.* at 42.

[147] *Id.* at 46.

[148] *Id.* at 49.

[149] *Id.*

[150] I have been unable to track down the origin of this convention. The first initials of the names are not an adequate explanation because there are many common given names in English that begin with A, B, and C. It helps the clarity of the explanation, however, to have different genders because then the referents of personal pronouns remain clear. *See* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 51-56 (1996).

keys via e-mail. If Alice and Bob have no prior dealings, however, they may be reluctant to trust simple e-mail.

The usefulness of public key cryptography is not limited to guaranteeing the confidentiality of messages. The digital signature function of public key cryptography can also be used to identify the party sending a message without encrypting the text. A digital signature is produced by first running the message to be signed through a hash function program that produces a digest of the entire message.[151] One characteristic of this message digest is that if any change is made to the message, when the message is run through the hash function again, it will produce a totally different digest. Once this digest has been computed, the digest is encrypted with the private key of the sender, Alice. This encrypted digest is the digital signature. The plaintext of the message is sent to the recipient, Bob, together with the digital signature. Bob, who must already be in possession of Alice's public key, runs the message through the same hash function and produces a message digest independently. Bob then uses Alice's public key (the public key of the signer) to decrypt the digest that was appended by Alice to the message. If the two digests are identical, then Bob can reasonably have a high degree of confidence that only Alice (or someone who obtained control of Alice's key) sent the message, and that the text of the message has not been tampered with in transit.

However, even public key cryptography does not eliminate the problem of how to administer the distribution of keys. Someone might establish a "Get to Know Bill Gates" web site, generate a matched key pair and post the public key to the web site for anyone in the world to download and use in their correspondence with "Bill Gates." Yet no sensible person would believe that the person with whom they were communicating by using this key and the e-mail address on the web site was actually the chief executive officer of Microsoft.

There are various solutions to the problem of distributing public keys in a manner that gives the recipient confidence that the public key belongs to the person to whom it appears to belong. One solution was advanced by Phil Zimmerman, who wrote a public key cryptography program, called Pretty Good Privacy (PGP), for use by private citizens.[152] The "web of trust"[153] allows each person using PGP to have the option of certifiying that other keys do indeed belong to the individuals who purport to use them.[154] Whenever a PGP user receives a key, the user is given the opportunity to review the other PGP users' certification of the key, and is asked to make a notation in the program regarding the degree to which the user trusts the authenticity of the identity of the purported user. To return to Alice and Bob, Bob may be a complete stranger to Alice, but Bob had his key certified by Carol, who is a good friend of Alice's. When PGP tells Alice that Carol has certified Bob's key, Alice may be willing to trust that the person sending her what purports to be Bob's

[151] FORD & BAUM, *supra* note 9, at 113.

[152] *See* GARFINKEL, *supra* note 145, at 85-103.

[153] *Id.*

[154] *Id.*

public key is in fact Bob.[155]

The Digital Signature Guidelines focus on the possibility of using a trusted third party, known as a "certification authority" (CA), to bind the identity of a person in the material world with the use of a specific key pair in an online environment.[156] The Digital Signature Guidelines define a certification authority as "[a] person who issues a certificate."[157] The procedure used by a CA to review an application from a prospective subscriber may be one of the CA practices described in a "certification practice statement" (CPS).[158] In order to issue certificates for subscribers' public keys, the CA must have a "trustworthy system."[159] If the CA operates a trustworthy system, the CA will be able to provide reliable "time-stamps" for issuance of certificates, thus allowing relying parties to know with certainty the time when the certificate will expire and reliance on it would no longer be reasonable.[160] What level of system security is appropriate to achieve a trustworthy system is a question that can only be resolved in light of the all circumstances under which the system will be used.[161]

To return to the story of Alice and Bob, we can now introduce Carol, the CA. Assuming that Alice and Bob do not have any prior acquaintance, then Carol can perform an invaluable service of permitting Alice and Bob to make each other's acquaintance in an online environment and to have confidence that they know with whom they are dealing. Bob sends his public key to Alice included in Carol's certificate, which includes, among other things, a copy of Bob's public key signed by Carol's private key.[162] If Alice has a copy of Carol's public key that she believes

[155] *Id.* at 235.

[156] DIGITAL SIGNATURE GUIDELINES, *supra* note 6, at 80. *See also* Froomkin, *supra* note 150, at 49-50. ("This article aims to describe what CAs do, explain why they are important to electronic commerce, and suggest that they are likely to provoke some interesting legal problems.").

[157] DIGITAL SIGNATURE GUIDELINES, *supra* note 6, at 37. Section 1.23 defines "person" as "[a] human being or an organization (or a device under the control thereof which is capable of signing a message or verifying a digital signature)." *Id.* at 58. Section 1.16 defines "issue a certificate" as "[t]he acts of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate." *Id.* at 50. Section 1.5 defines "certificate" as "[a] message which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it." *Id.* at 35.

[158] *Id.* at 39-40. A CPS is "[a] statement of the practices which a certification authority employs in issuing certificates." *Id.*

[159] Section 1.35 defines trustworthy system as "[c]omputer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonably reliable level of availability, reliability and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security principles." *Id.* at 69.

[160] *Id.* at 66.

[161] *Id.* cmt. 1.35.3, at 71.

[162] It is possible to view actual digital signature certificates in most recent releases of popular web browser programs. For example, in Netscape Communicator 4.0, certificates stored in the browser program can be viewed by choosing the "Communicator" menu, and then selecting "Security Info" from the list of options on the Communicator menu. A dialog box appears that provides information on many aspects of Communicator's security functions, including certificates. Certificates are organized into groups of "Yours," "People," "Web sites," and "Signers." The category of signers is

to be trustworthy, then she can use that public key to verify Carol's signature on the certificate. Once she has successfully verified Carol's public key, Alice can have have confidence that Bob's key is what it purports to be. Using Carol's CA services, however, solves one problem—whether to trust that Bob's public key actually has some connection to the human being Bob with whom Alice believes she is dealing—only if two new problems can also be solved. These problems are: (1) whether Alice understands the degree of scrutiny applied by Carol before issuing Bob a certificate and has thought about whether that degree of scrutiny is appropriate for the use Alice has in mind for Bob's key; and (2) whether there is a system for distributing Carol's keys that inspires the confidence of people like Alice and Bob that they do actually have a copy of Carol's key.

C. Risk Allocation Systems for Emerging Electronic Commerce Systems

The manner in which public key cryptography is used to create a digital signature is quite clear and unproblematic; however, the larger institutional framework within which public key cryptography will be administered is still quite controversial. At one extreme of the spectrum of possible public key infrastructures (PKI) is the PGP web of trust model, and at the other extreme are the closed and highly regulated models developed for military use of public key cryptography. The web of trust is a wholly decentralized, user-controlled system of evaluating the trustworthiness of key as compared to the U.S. Department of Defense's rigidly hierarchical, top-down PKI.[163] Most proposed or existing PKIs, including the CA model proposed in the Digital Signature Guidelines, are somewhere in between the military model and the web of trust.[164] The members of the Information Security Committee of the ABA Science and Technology division are working to develop standards in many areas surrounding the administration of PKIs,[165] as is the Internet Council of the National Automated Clearing House Association.[166] These groups directed their work toward finding a viable solution to the problems facing Alice

reserved for certificate authorities, who are "certificate signers." The certificates of many commercial CAs are installed in the browser program automatically. This enables the browser to verify automatically a digital signature certificate offered by an Internet commerce web site without requiring the individual using the browser program to take the necessary steps to obtain the CA's certificate.

[163] FORD & BAUM, *supra* note 9, at 270.

[164] *See id.* at 263-314 (describing several different model PKIs in chapter 7).

[165] For information about the work of the Information Security Committee, see ABA Section of Science & Tech., Elec. Commerce Div., *Information Security Committee Home Page* (visited May 5, 1998) <http://www.abanet.org/scitech/ec/isc/home.html>. In early 1998, the Accreditation Workgroup was drafting Guidelines for Certificate Policies and Accreditation Criteria that it hopes to finalize later this year. *Id.* The ABA Committee on Cyberspace Law has also undertaken major projects addressing issues raised by the impact of the Internet on commercial law, which are described at ABA Section of Business Law, *Committee on Cyberspace Law* (visited May 5, 1998) <http://www.abanet.org/buslaw/cyber/>.

[166] Information about the Internet Council is available at *The Internet Council* (last modified Mar. 9, 1998) <http://www.nacha.org/tic/default.htm>.

when she decides whether to rely on Carol's certificate.

While digital signature technology was not developed with the Internet in mind, it offers tremendous promise as a solution to several problems associated with using the Internet for business transactions. The Internet began in 1969 as a federally subsidized network among universities and government research laboratories with possible military applications.[167] The Department of Defense Advanced Research Projects Agency funded the development of the Internet during the 1970s.[168] The Internet developed as a distributed, packet switching network that could continue functioning even if parts of the network were disabled.[169] The technical standards that define the Internet are all public, permitting the computer hardware of any manufacture and many different types of software and operating systems to integrate into the network.[170] Among the most important Internet applications are e-mail, electronic bulletin boards, file transfer protocols that permit downloading files from remote locations, protocols that support remote access to different computers on the network, and information browsing via hyperlinks or searching, either with or without a graphical user interface.[171]

While the Internet may be uniquely suited for disseminating information,[172] its openness and flexibility render it highly insecure, especially in comparison with existing large scale computer networks supporting electronic financial services. The technology which facilitates the free flow of information over the Internet also leaves gaping holes where computer vandals and criminals can break into systems connected to the Internet. Once malfeasors have gained unauthorized access to an unprotected or poorly secured site, that site may become the launching point for further attacks, exposing the owner of the hacked site to not only the cost of repairing damage to his or her own site, but possible liability to third parties. Many technical flaws have emerged in software designed to support electronic commerce over the Internet, and while publicized bugs have been corrected, the number of bugs not yet detected is unclear. Information system security problems are complex, designing trustworthy systems is very difficult, and the amount of reliable information about Internet security available to many users is inadequate even for a diligent or careful person to learn to take adequate precautions.

While the Internet has made the topic of electronic commerce more visible than ever, many of the issues debated in the Internet electronic commerce context actually have much broader relevance. The manner in which computer and communications technology is used by businesses is rapidly transforming, and the integration of Internet functions and resources is only one piece of the puzzle.[173]

[167] FORD & BAUM, *supra* note 9, at 17.

[168] *Id.*

[169] *Id.*

[170] *Id.*

[171] *Id.* at 18.

[172] U.S. District Court Judge Stewart Dalzell labeled the Internet "the most participatory form of mass speech yet developed. . . ." ACLU v. Reno, 929 F. Supp. 824, 883 (E.D. Pa. 1996).

[173] Jon William Toigo, *Enterprise Computing Platform Evolution: Technology Trends Change as Fast as Fashion Styles*, 11 ENTERPRISE SYS. J. 54 (1996) (WOT).

Many types of business information processing are migrating from mainframe computers toward networked computer systems, which entails a move away from offline, batch processing of data to online, real time processing of data. Enterprise resource management software can replace older, hierarchical, compartmentalized legacy computing systems and can offer competitive advantages to companies that effectively use distributed computing services. As enterprises provide customers and employees with greater access to information technology, the physical and technological security of older systems will no longer adequately secure commercial operations. Presently no equivalent to generally accepted accounting principles exists for the analysis of information system security issues within emerging models of business information technology.[174] Until a consensus emerges on precisely what security is necessary to conduct commerce over open networks such as the Internet, the representatives of various industries that are already established players in the electronic commerce arena and the representatives of new players working to bring new technologies to market will likely vigorously debate what constitutes reasonable commercial practices with regard to information security.

The Digital Signature Guidelines represent one of the first attempts to develop a comprehensive business model, including a risk allocation system, for the deployment of digital signature technology in electronic commerce.[175] The primary focus of the Guidelines is on a specific technology, public key cryptography, and developing a legal framework which might encourage transactors to deploy that technology. The business application the drafters apparently used as the test case in drawing up the recommendations in the Guidelines was quite different from the type of business applications commonly found in electronic commerce today. This test case was a business transaction between two parties who have no prior contact in either the online environment or the physical world and who want to enter into a contract to be performed entirely online.[176] The drafters apparently assumed that they could eliminate the most significant obstacles to the deployment of digital signature technology in electronic commerce by drafting a solution that worked for

[174] For example, in 1991, the U.S. National Research Council called for the development of such a system in its report, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, 1991. In 1992, OECD issued its Guidelines for the Security of Information Systems which contained general principles that might serve as a foundation for a statement of detailed generally accepted system security principles. Winn, *supra* note 5. In 1998, it was not yet apparent what concrete steps have been taken toward the development of such a set of principles. *See* Winn, *supra* note 5 (discussing the guideline proposals).

[175] DIGITAL SIGNATURE GUIDELINES, *supra* note 6. I was not aware of the drafting process of the Guidelines, let alone part of it, so I cannot comment on the drafting process from the perspective of a participant. However, I have talked at length with quite a few of the participants, and the following discussion is based on certain points about which there seems to be a consensus.

[176] This fact pattern is sometimes referred to as an "open system" but there are apparently as many different interpretations of open system as there are individuals using the term. The ABA Science and Technology Section Information Security Committee has a working group trying to develop a comprehensive taxonomy of situations in which public key cryptography might be deployed and to define standard terms to refer to those situations.

this most extreme case. They thought that less radical applications of this technology, such as in dealings between two parties who have had sustained prior contact in either the online environment or the physical world, were inherently less intractable, and therefore less urgently needed a framework such as that proposed in the Guidelines.[177]

The Guidelines do not contain a detailed discussion of how strangers with no prior relationship might conduct electronic commerce in the future; however, the roles assigned to the CA, the subscriber, and the relying party to a digital signature transaction make sense under the assumption that many such transactions will take place in the future. The model CA reflected in the Digital Signature Guidelines is based on the assumption that a contractual relationship will exist between the CA and the subscriber but not between the CA and the relying party. One can obviously imagine a system in which a CA enters into contractual relationships with prospective relying parties, researching and certifying the digital signatures of prospective transactors for the express benefit of the relying party. Instead, the maintenance of a "certificate revocation list" (CRL) by the CA protects the interests of the relying party in the Digital Signature Guidelines. Before relying on a certificate, relying parties should check the CRL to determine if it has been revoked by the CA or canceled at the request of the subscriber.

In the event either the subscriber or the relying party suffers a loss in a transaction in which one of the CA's certificates was used to authenticate a digital signature, the Guidelines may abrogate the right of either party to proceed against the CA.[178] This safe harbor provides that a CA is not liable to either a subscriber or a relying party if it has complied with the terms of its own CPS and complied with the provisions of the Guidelines.[179] The Comments to this section explain that this protection for the CA against liability arising outside the terms of its CPS or a statute based on the Guidelines was felt to be necessary to induce responsible parties to play the essential role of CA in this uncharted area of commercial transactions.[180] This has proved to be a controversial provision of the Guidelines that few legislatures have chosen to adopt.[181] The Utah and Washington digital

[177] Fact patterns in which the parties using public key cryptography already stand in some defined relationship to each other are sometimes referred to as "closed systems," but this term is as ambiguous as its logical inverse, open system.

[178] DIGITAL SIGNATURE GUIDELINES, *supra* note 6, § 3.14, at 99-100.

[179] *Id.*

[180] *Id.* cmt. 3.14.1, at 100.

[181] Many states have considered, but few have adopted, digital signature legislation which follows the proposals of the Digital Signature Guidelines. For an analysis of electronic commerce and digital signature initiatives taken through fall 1997, see Internet Law & Policy Forum, *Survey of State Electronic & Digital Signature Legislative Initiatives* (visited May 5, 1998) <http://www.ilpf.org/digsig/digrep.htm>. For a current survey of various legislative initiatives regarding electronic commerce and digital signatures, see McBride, Baker & Coles, *Summary of Electronic Commerce and Digital Signature Legislation* (last modified Mar. 10, 1998) <http://mbc.com/ds_sum.html>. For some criticisms of the approach taken in the Guidelines, see Biddle, *Misplaced Priorities*, *supra* note 12, at 1166-67; Biddle, *Policy Questions*, *supra* note 12; and Winn, *supra* note 5. Another controversial safe harbor provision in the Guidelines, the presumption

signature statutes, enacted originally in 1995 and 1996 respectively, adopted comprehensive licensing regimes to provide public oversight of CAs before a CA could qualify for a safe harbor from liability outside the terms of the CA's CPS or the relevant statutory regime.[182]

This drafting strategy is fundamentally at odds with the strategy of the drafters of the Uniform Commercial Code.[183] The U.C.C. was designed to restate and modernize the existing law governing certain categories of commercial transactions, and as a result was essentially more conservative and historical in orientation than the Digital Signature Guidelines. The U.C.C. aims to create certainty for transactors by building on existing trade usages and commercial practices while retaining enough flexibility to cope with inevitable innovations. The Guidelines, by contrast, were inspired by the desire to bring public key cryptography to a new audience; thus, by definition there could not yet be any existing trade usages or commercial practices to draw upon. Therefore, the Guidelines try to anticipate the future commercial applications. For example, the Guidelines draw on engineering standards such as the ITU/ISO x.500 directory standard which provides a system for controlling and accessing information about names and identities.[184]

The focus of the Guidelines on a transaction between two strangers, who might be located in different countries but who are brought together for the first time online, has certain structural similarities with the "courier without luggage" concept emphasized in Chief Justice Gibson's opinion in *Overton v. Tyler*.[185] In order for a contract representing a right to payment to circulate as the equivalent of currency, it had to comply with strict formal standards limiting the terms the parties could use in drawing up the instrument.[186] The commercial benefit conferred by the rigid formalism of negotiable instruments law was the creation of the financial liquidity necessary to grease the wheels of early nineteenth century commerce. Public key cryptography offers the promise of providing a secure framework in which transactors will have enough confidence to participate in the global Internet market, thus greasing the wheels of twenty-first century commerce. In order for digital signatures to operate as the twenty-first century equivalent of Gibson's nineteenth-century "courier without luggage," universally recognized formal standards will have to be established to permit the interoperability of separately administered

that a digital signature is the signature of the party identified in the certificate, is discussed below. *See infra* text accompanying notes 227-30.

[182] For the licensing provisions of the relevant statutes, see UTAH CODE ANN. § 46-3-201 to -204 (Supp. 1997), and WASH. REV. CODE ANN. §§ 19.34.100-.101 (West Supp. 1998).

[183] *See, e.g.*, Karl Llewellyn, *Why a Commercial Code?*, 22 TENN. L. REV. 779, 779 (1953) (describing the purpose of the UCC); Grant Gilmore, *On Statutory Obsolesence*, 39 U. COLO. L. REV. 461, 461 (1967) (discussing the reasons for and history of the codifications of commercial law).

[184] The x.500 directory standard was developed by the International Consultative Committee on Telegraphy and Telephony (ICCTT), later renamed the International Telecommunication Union-Telecommunication Standardization Bureau (ITU-T), in collaboration with the International Organization for Standards (ISO). DIGITAL SIGNATURE GUIDELINES, *supra* note 6, at 21.

[185] 3 Pa. 346, 347 (1846). For a discussion of the facts and holding of the case, see *supra* text accompanying notes 3, 42.

[186] *Id.*

PKIs. Harmonious national and transnational standards governing the technological and legal framework for the commercial use of public key cryptography will have to be set before the transaction between strangers in the global electronic marketplace can become a commercial reality.[187]

The difficulty of expanding the application of public key cryptography outside of communities with a defined class of members is finding a way to permit one party to evaluate and accept certificates issued by CAs with whom that party had no prior dealings, just as existing national and transnational technology standards permit telephone calls to connect any two places in the world. Scalability and interoperabilty of PKIs may be a more difficult problem to solve than the problem of telecommunications standards.[188] In order to be successful, PKIs must resolve both technical and legal issues, and the very considerable problems of designing software and hardware to support transnational interoperability of digital signature technology will be hampered until there is some consensus on the legal framework within which it will be deployed. While the drafters of the Digital Signature Guidelines hoped that the Guidelines would offer a framework around which a such consensus could be crafted, in the months and years following the publication of the Guidelines, that consensus appears to be growing ever more elusive.[189]

The narrow focus of the Guidelines on an implementation of a radically new technology seems to reflect a decision by the drafters that existing large-scale electronic commerce applications have limited or no precedential value for their enterprise. One further assumption implicit in the Digital Signature Guidelines distinguishes the hypothetical fact pattern from virtually all electronic commerce as it is conducted today: it would be uneconomical for the CA to establish contractual privity with the relying party. The advantage to a CA of entering into a contract with the relying party is that the CA can use the contract to limit his or her exposure to the relying party for losses arising in a transaction in which the CA's certificate had been used.[190] In existing electronic commerce systems, risks

[187] For a more detailed discussion of some of the thorny problems that must be resolved, see FORD & BAUM, *supra* note 9, at 265-281 (discussing Certification Authority Interrelationship Structures).

[188] International telecommunications are possible because of international engineering standards established by the International Telecommunications Union (ITU). For a discussion of the history and operation of the ITU, see CARL CARGILL, OPEN SYSTEMS STANDARDIZATION 211-214 (1996).

[189] One observer has noted that the varying degrees of success enjoyed by those lobbying for a comprehensive approach to digital signature legislation have produced such a bewildering array of different laws that digital signature technology is in danger of being "loved to death" by its staunchest proponents. Stewart A. Baker, *International Developments Affecting Digital Signatures* (last modified Oct. 1997) <http://www.steptoe.com/digsig2.htm>.

[190] *Cf.* Kline v. First W. Gov't Sec., Inc., 24 F.3d 480 (3d Cir. 1994) (refusing to grant summary judgment to a law firm that denied its liability to investors based on opinion letters the law firm issued to an investment firm marketing tax shelters on the effectiveness of those investments as tax shelters after the IRS disallowed the investments as tax shelters). The court noted that notwithstanding the attempt of the law firm to limit its potential liability to investors by stating in the opinion letters that they were for the exclusive use of the investment firm, the law firm knew that the investment firm was distributing copies of the opinion letters to prospective investors to encourage them to invest. *Id.* at

are managed through a combination of contracts, government regulation, and rules for private membership organizations such as the clearinghouses that process funds transfers. The drafters of the Digital Signature Guidelines seemed to assume that the deployment of public key cryptography in those environments would not require legislation along the lines suggested in the Guidelines because those parties had already created a functional legal framework for their transactions that could be adapted to incorporate new technologies.[191] The development of the Secure Electronic Transaction (SET) protocol by Visa International and MasterCard is an example of the development of a public key infrastructure that will be integrated into existing global networks.[192] The legal framework that supports Visa and MasterCard, with the exception of certain key consumer protection regulations, is provided by contracts between the parties. By 1998, however, the vigorous debate taking place within trade associations such as the National Automated Clearing House Association,[193] Commerce Net,[194] and the Financial Services Technology Consortium (FSTC)[195] regarding the development of public key infrastructures for existing electronic commerce systems indicates that the process of incorporating public key cryptography and Internet communications into existing electronic commerce systems may raise problems just as difficult as the fact pattern addressed by the drafters of the Guidelines.

The whole concept of a digital signature certificate as a universal form of identification in cyberspace seems more closely related to certain ministerial functions performed by government officials in the conduct of official business than it does to the type of services commercial parties require when entering into contractual relationships with strangers, especially strangers in foreign jurisdictions. Commercial parties commonly rely on services such as letters of credit offered by banks in order to manage the risk in transnational trade, in which the contracting parties expect the banks to confirm not only the identity of the other party to the transaction, but.creditworthiness as well. Even the concept of a universal ID is foreign to parties in the United States. While national ID cards are common outside the United States, the closest thing Americans have to a national ID card is a driver's license or a passport.

A second analogy can be drawn between the CA function in the Digital

487. Cases such as *Kline* indicate that a CA might reasonably be concerned about its ability to limit its liability to the terms set out in its certification practice statement.

[191] It must be noted that the Digital Signature Guidelines includes a formal disclaimer of any intent by its drafters that the Guidelines be used as model legislation. DIGITAL SIGNATURE GUIDELINES, *supra* note 6, at 23.

[192] Information about SET can be accessed at the Visa web site at *SET Secure Electronic Transaction at Visa* (visited May 5, 1998) <http://www.visa.com/cgi-bin/vee/nt/ecomm/set/main.html?2+0>.

[193] Information about the National Automated Clearing House Association is available at *Electronic Payments* (last modified Mar. 3, 1998) <http://www.nacha.org>.

[194] Information about Commerce Net is available at *Commerce Net* (visited May 5, 1998) <http://www.commerce.net/research/presentations/eco/index.html>.

[195] *See* Financial Services Technology Consortium, *The Bank Internet Payment System* (visited May 5, 1998) <http://www.fstc.org/projects/bips/index.html>.

Signature Guidelines and the function of a notary, who in the United States is an independent party who generally lacks the professional qualifications of the *notaire* in civil law jurisdictions.[196] The CyberNotary Committee of the ABA Science and Technology Committee has worked to develop the concept of a "CyberNotary," but it remains unclear if this concept will develop into a viable commercial service.[197] The physical world of business transactions has no commercial equivalent of this service that the CA provides in the Guidelines. Thus, while the drafters of the Guidelines seemed confident that the enhanced level of security that public key cryptography provides would trigger a demand for CA services among businesses migrating to Internet commerce, no real precedent in the United States supports operating an identification service for profit. It remains unclear what kind of business model will ultimately allow for-profit enterprises to offer digital signature certification services for Internet transactions.

The business entity offering a service that most closely resembles the description of a certification authority given in the Digital Signature Guidelines is a privately held company called VeriSign, Inc.[198] VeriSign provides digital signature certificates, which it calls "Digital IDs,"[199] and also provides certification authority technology to third parties, which it refers to as "private label certificate services."[200] According to an undated white paper entitled *Digital IDs for Servers: High-level Security at a Low Cost*, "over 1,500,000 VeriSign Client Digital IDs have been issued to users of Netscape and Microsoft browsers."[201] In addition, the white paper states that "[o]ver 45,000 commercial sites are using VeriSign Server Digital IDs to create secure channels with customers."[202] The white paper explains how electronic commerce servers can be equipped with Digital IDs and then can use the public key associated with the Digital ID to set up a secure channel of communication between the remote computer running an Internet browser application and the server using the Secure Sockets Layer (SSL) communication protocol.[203] The white paper adds that the next step in implementing client authentication will be for electronic commerce servers to require their customers to

[196] For a general discussion of the difference between the functions of notaries in the United States and in civil law jurisdictions, see RUDOLF B. SCHLESINGER ET AL., COMPARATIVE LAW: CASES, TEXT, MATERIALS 18-23 (5th ed. 1988).

[197] *See* ABA Section of Science and Technology Electronic Commerce Division, *CyberNotary Committee Home Page* (visited May 5, 1998) <http://www.abanet.org/scitech/ec/cn/home.html>.

[198] *See VeriSign Electronic Credentials for the Internet* (visited May 5, 1998) <http://www.verisign.com>.

[199] *See Digital ID's: The New Advantage* (visited May 5, 1998) <http://www.verisign.com/clientauth/whitepaper.html> (explaining Digital IDS).

[200] VeriSign's private label services include support for the SET protocol being developed by Visa International and MasterCard.

[201] *Digital IDs for Servers: High Level Security at a Low Cost* (visited May 5, 1998) <http://www.verisign.com/products/sites/serverauth.html>. While many certificates have been issued, it remains unclear how many have been used in commercial transactions.

[202] *Id.*

[203] *Id.*

identify themselves with Digital IDs.[204]

While VeriSign anticipates the use of Digital IDs to support the use of digital signatures as described in the Digital Signature Guidelines in the near future, that is not yet the primary application of the public key technology products it has developed. Public key cryptography is being used instead to support the use of symmetric or secret key cryptography to transport credit card information between the Internet browser program on the consumer's computer and the retail merchant's electronic commerce server.[205] While the ability of the consumer to enter into a secure communication channel with the Internet merchant increases the level of confidence enjoyed by consumers that they are dealing with a legitimate web site, the use of a Digital ID by the electronic commerce server does not amount to a binding signature by the merchant on a contract with the consumer. Rather, the entire transaction is a variant of telephone catalog sales. As with credit card sales completed over the telephone, the merchant assumes the risk that the credit card use is unauthorized. As such, the merchant is subject both to federal consumer protection legislation and to the terms of its contract with the bank that acquires its credit card charge authorizations regarding the consumer's right to demand a refund of charges to his or her credit card account.[206]

If the VeriSign white paper is correct that the next phase in Internet electronic commerce will include the requirement that consumers use digital signatures and that those digital signatures be certified by CAs such as VeriSign, the amount of risk that the consumer is expected to bear in Internet transactions may dramatically increase. If consumers are able to enter into binding contracts without the use of credit cards and the consumer protections credit cards import, many of their rights and obligations will be defined by the terms of their VeriSign Subscriber Agreement,[207] which incorporates by reference the terms of the VeriSign Certification Practice Statement (CPS).[208] However, consumers may have additional

[204] *Id.*

[205] *See Digital Ids: The New Advantage* (visited May 5, 1998) <http://www.verisign.com/clientauth/whitepaper.html> (illustrating the public key cryptography). Symmetric key cryptography generates the session key that is used to encrypt all communication between the consumer client computer and the merchant server computer. Symmetric key cryptography is used because it is less computationally intensive than public key cryptography and therefore less likely to slow down the response time of the consumer's computer in executing the consumer's purchase instructions. Public key cryptography is used to solve the symmetric key distribution problem. *See* FORD & BAUM, *supra* note 9, at 101-10 (comparing symmetric cryptosystems and public key cryptosystems).

[206] The official commentary to Regulation Z, 12 C.F.R. § 226.12, makes it clear that the practice of accepting credit card information over the telephone is done entirely at the merchant's risk in the event a cardholder later claims that a payment was unauthorized. 12 C.F.R. § 226.12(b)(2)(iii) cmt. 1, at 351 (1997). Because the bank that issued the credit card has not provided the merchant a means to identify the user under these circumstances, the issuer has not fulfilled one of the conditions (that the card issuer has provided a means to identify the cardholder on the account or the authorized user of the card), for imposing liability on the cardholder. *Id.* § 226.12(b)(2)(iii) cmt. 3, at 351 (1997).

[207] *VeriSign Public Certification Services: Subscriber Agreement* (visited May 5, 1998) <http://www.verisign.com/repository/SUBAGR.html>.

[208] *VeriSign Certification Practice Statement* (version 1.2, May 30, 1997)

rights under the Netsure Protection Plan.[209] The rights of merchants who verify consumer digital signatures by using the VeriSign Certificate Revocation List will be governed by the VerSign Relying Party Agreement.[210]

The VeriSign CPS defines the procedures Versign will follow before issuing a Digital ID. Individual Digital IDs are currently offered in three classes.[211] Class 1 Digital IDs "are issued to individuals only," and are issued after VeriSign determines that there are no existing entries in VeriSign's database of subscribers with the same name and e-mail address.[212] The CPS notes that these certificates are not suitable for commercial use where proof of identity is required.[213] Class 2 Digital IDs are "currently issued to individuals only" after VeriSign checks not only its own database of subscribers, but also performs an automated check of the applicant's information against "well-recognized consumer databases."[214] The CPS emphasizes that Class 2 certificates, "[A]lthough . . . an advanced automated method of authenticating a certificate applicant's signature," are issued without requiring the applicant's personal appearance before a trusted party such as a notary; therefore, relying parties should take this into account before accepting a Class 2 certificate as identification of the subscriber.[215] While VeriSign Digital IDs issued under these circumstances may become popular when used in connection with other existing consumer transaction systems such as credit cards, it is unclear whether there will ever be a market where transactions are executed in reliance on such a Digital ID alone.[216]

<http://www.verisign.com/repository/CPS> [hereinafter *CPS*].

[209] *NetSure Protection Plan* (version 1.0, June 20, 1997) <http://www.verisign.com/repository/netsure/index.html>. According to the Netsure Frequently Asked Questions page,

> NetSure is an extended warranty Internet program which provides Digital ID^{SM} holders with protection against accidental occurrences such as loss of the subscriber's private key (corresponding to the public key in the Digital ID) and theft, corruption, impersonation, certain loss of use and unintentional disclosure of a subscriber's private key to others, provided that you, a subscriber, have fulfilled your obligations. Your obligations as stated in the CPS include *taking reasonable precautions to prevent loss or unauthorized use of your private key and to use computer systems which are reasonably secure from intrusion or misuse.*

NetSure^{SM} Protection Plan: Frequently Asked Questions (visited May 5, 1998) <http://www.verisign.com/repository/netsure-faq/> (emphasis added). Given the lack of objective standards as to what constitutes reasonable security for home personal computer use, it may be very difficult for most consumers ever to establish a valid claim under this contract language. See *supra*, text at notes 173-74, for a discussion of the divergence between the assumptions about consumer computer security among the developer community and the reality of consumer computer security.

[210] *VeriSign Public Certification Services: Relying Party Agreement* (visited Feb. 27, 1998) <http://www.verisign.com/repository/rpa.html>.

[211] *CPS, supra* note 208, § 2.2, at 7.

[212] *Id.* § 2.2.1, at 7-8.

[213] *Id.* § 2.2.1, at 8.

[214] *Id.* § 2.2.2, at 8.

[215] *Id.* at 9 (emphasis in the original).

[216] For this reason, Stewart Baker has labeled them "cheap certificates." *See* Baker, *supra* note

Class 3 certificates may be issued to individuals or organizations.[217] Class 3 certificates issued to individuals "provide important assurances of the identity of individual subscribers by requiring their personal (physical) appearance before class 3 LRA or its delegate (such as a notary)."[218] For an organization, such as a corporation or government agency, to receive a Class 3 certificate, VeriSign's CPS specifies that the organization's application process must "include[] review by the applicable Class 3 IA of authorization records provided by the applicant or third-party business databases, and independent call-backs ("out-of-band" communications)."[219] Because Class 3 certificates require a personal appearance by an individual applicant before a trusted third party, they are a much more reliable means of identification than are either the Class 1 or Class 2 certificates.

While VeriSign Digital IDs are of limited use to merchants doing business over the Internet in managing transaction risks, they represent a potential nightmare of unlimited personal liability for consumers. Under the VeriSign CPS, a subscriber who accepts a VeriSign Digital ID must represent, among other things, that "no unauthorized person has ever had access to the subscriber's private key" at the time of acceptance of the certificate and throughout the operational period of the certificate.[220] In addition, "[b]y accepting a certificate, the subscriber assumes a duty to retain control of the subscriber's private key, to use a trustworthy system, and to take reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use."[221] According to some consumer advocates, this trustworthy system standard is a totally inappropriate method of evaluating security on home personal computers used by consumers.[222]

Downloading and installing the most recent release of Pretty Good Privacy (PGP) results in the storage of the consumer's public and private keys on the hard drive of the computer. That private key can be accessed by typing in a pass phrase. Unauthorized third parties may gain access to this private key merely by accessing the computer and guessing the pass phrase.[223] Guessing the pass phrase can be attempted most easily by copying relevant files from the consumer's hard drive to another computer, and then taking as much time as is needed to determine the pass

189, at 2.

[217] *CPS, supra* note 208, § 2.2.3, at 9.

[218] *Id.*

[219] *Id.*

[220] *CPS, supra* note 208, § 7.2, at 53.

[221] *Id.* § 7.3, at 54. The CPS "trustworthy system" is defined as "Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonably reliable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a 'trusted system' as recognized in classified government nomenclature." *Id.* § 13.1, at 98.

[222] Cem Kaner, *Speed Bump on the Fraud Superhighway: The Insecurity of the Digital Signature*, UCC BULLETIN (West Group), Jan. 1998, at 2 [hereinafter Kaner, *Speed Bump*]; Cem Kaner et al., *SPLAT! Requirements Bugs on the Information Superhighway*, SOFTWARE QA MAG. (forthcoming 1998) [hereinafter Kaner, *SPLAT!*].

[223] Kaner, *Speed Bump, supra* note 222, at 4.

phrase by guesswork.[224] Individuals untrained in computer security are notoriously bad at devising secure passwords, so in many cases the perpetrator easily discovers the pass phrase.

Unauthorized third parties use several techniques to gain access to consumers' home personal computers for long enough to copy the relevant files to another computer. These techniques include copying the files while the computer is in the shop for repairs, or while a repair technician works on the consumer's computer on site. In addition, some software support programs copy large amounts of information from the customer's system in order to analyze the problems the customer is experiencing. The same software can be used to make unauthorized copies of specific applications and data files without the consumer's knowledge or consent. Therefore, the consumer may be in the awkward position of having no idea how a copy of his or her private key was obtained and, as a result, no way to prove that he or she maintained a trustworthy system as required by the CPS.

As a risk allocation system, the VeriSign CPS is moving in the opposite direction of most other electronic commerce systems, and resembles the system established by credit card issuers prior to federal consumer regulations protection.[225] No significant pooling of risks exists for consumer subscribers because, although insurance is now offered, the insurance mimics the standard of care the subscriber is required to maintain by the CPS and, thus, is unlikely to offer any relief to a consumer who cannot prove how a copy of his or her private key was obtained. The CPS allocates fraud or error losses to the consumer who is likely to be much less sophisticated than VeriSign, and is completely incapable of deploying the kind of technology used by credit card companies to reduce fraud.[226] The problem of information asymmetry is acute in consumer dealings with VeriSign because no plain language disclosure of the risk allocation system exists outside the CPS, which is over 100 pages of single spaced text written in dense legal prose.

The inappropriate allocation of risk implemented by the VeriSign CPS would only be exacerbated in a jurisdiction with legislation modeled on the Digital Signature Guidelines. Section 5.6(2) of the Guidelines provides that in disputes involving digital signatures, there is a rebuttable presumption that the signature belongs to the party identified in the certificate as the subscriber.[227] The comments to section 5.6[228] explain that this provision is modeled after the presumption that the issuer's signature is genuine under negotiable instruments law.[229] Given the focus

[224] *Id.*

[225] *See* CLARK BARKLEY, THE LAW OF BANK DEPOSITS, COLLECTIONS AND CREDIT CARDS ¶ 15.03 (rev. ed. 1995).

[226] *See supra* notes 134-36 (discussing the use of holograms and neural networks as security procedures). VeriSign would have difficulty taking advantage of the technology employed by credit card companies today because VeriSign has not designed its system to permit the CA to monitor individual transactions. Rather, the CA certifies the online identity of a party for a defined period of time.

[227] DIGITAL SIGNATURE GUIDELINES, *supra* note 6, § 5.6(2), at 117.

[228] *Id.* § 5.65 cmt.

[229] *See* U.C.C. § 3-308 (1991 & Supp. 1997) (governing proof of signatures and providing that

of the Guidelines'drafters on the technology of public key cryptography, it is not surprising that a presumption of validity seemed appropriate. With regard to the operation of public key cryptography, when one key of a key pair is used to decrypt a message, it is virtually irrebutable that the other key in the pair was used to encrypt the message.

The problem with creating presumptions regarding the legal significance of the use of public key cryptography is that no appreciable experience exists regarding its use outside of military environments. It is not yet clear what type of security procedures consumers can reasonably be expected to follow, but there seems to be little congruence between what information security experts and developers of digital signature applications seem to expect and the reality of personal computer use by consumers.[230] Without consumer protection legislation such as that used to force credit card issuers to bear the majority of fraud costs, there will be little pressure on developers to accept the additional costs of designing applications that incorporate realistic accommodations for consumers.

In what is colloquially know as the "Grandma picks a bad password and loses her house" scenario,[231] a consumer who is not particularly sophisticated will install an encryption program on her personal computer, choose a pass phrase that is easy to guess, subscribe to a service such as the VeriSign Digital ID service, and lose control of her key through some process she does not recognize or understand. The party making unauthorized use of her key will purchase $1 million in software over the Internet in a very short period of time in transactions that do not exceed the reliance limit in the certificate. When Grandma tries to defend herself against the claims of the merchants who have delivered software to someone claiming to be Grandma, not only must Grandma establish that she maintained a trustworthy system (if she is subject to the terms of the VeriSign CPS) in order to avoid liability, she will have to rebut a presumption that the digital signature used in all the unauthorized transactions is not, in fact, her signature.

Presumptions can simplify litigation by eliminating the requirement that a party prove each element of his or her case in detail in situations where, as a matter of fact or public policy, a connection between certain facts can be presumed to exist without proof. In the context of negotiable instruments law, the presumptions associated with the signatures of the parties began to take shape in the nineteenth

any party wishing to deny the validity of a signature must do so in his or her pleadings or will be deemed to have admitted the validity of the signature, and that a signature will be presumed authentic and authorized unless the purported signer is dead or incompetent at the time of the litigation).

[230] Kaner, *SPLAT!*, *supra* note 222.

[231] The "Grandma picks a bad password" scenario has apparently passed into Internet technology folklore. *See* Kaner, *SPLAT!*, *supra* note 222; Baker, *supra* note 189, at 2. The impact of a "Grandma picks a bad password" case could be very substantial if Grandma tells her story on *The Oprah Winfrey Show* and *20/20*, thereby driving consumers away from Internet commerce in droves and prompting state attorneys general to consider commencing class action law suits against CAs issuing what Stewart Baker has labeled "cheap certificates." *See supra* note 216 and accompanying text.

century when the modern pleading rules replaced the writ system of pleading.[232] It was not until UCC Article 3 was completed in 1957 that a formal system of presumptions was established. Comment 1 to the 1957 version of section 3-307 explained that a presumption expressly provided by statute was new, although similar provisions could be found in a number of states.[233] The Comment goes on to explain that "[t]he presumption rests upon the fact that in ordinary experience forged or unauthorized signatures are very uncommon, and normally any evidence is within the control of the defendant or more accessible to him."[234] The problem with creating a similar presumption regarding the legal significance of an act that is not yet taken in commercial settings is that there is not yet any "ordinary experience" regarding how common unauthorized uses of digital signatures will, in fact, be. Given that the VeriSign CPS holds consumers to a standard that seems unrealistically high, it is plausible that the unauthorized use of digital signatures may occur with some frequency.

While the VeriSign Digital ID is not yet in wide use in Internet consumer transactions, a large volume of Internet consumer transactions take place through the use of credit cards. The most successful consumer-oriented Internet commerce site is run by Dell Computers and is reported to sell $3 million in personal computer orders per day.[235] The Dell web site includes an explanation of the security used to protect the confidentiality of the consumer's credit card number and gives the consumer the option of telephoning in the order if the consumer feels uncomfortable with the security procedures even after the explanation.[236] The Land's End web site explains to consumers in plain language how the consumer's liability is limited, how encryption is used within the Secure Sockets Layer (SSL) protocol to protect such information during its transmission over the Internet, as well as telephone and fax numbers for consumers who feel uncomfortable with Internet ordering.[237] In addition, the Lands' End site also explains Lands' End privacy policies and how those policies can be evaluated in light of emerging industry standards regarding consumer privacy rights.[238]

These successful sites have incorporated the credit card risk allocation model into their business model for Internet commerce and are working to develop their image as responsible purveyors of Internet commerce. Because the credit card system operates as a complex system of trade association rules and bilateral contracts, its use in Internet retail applications simplifies many of the problems associated with designing a PKI capable of handling anonymous global Internet

[232] Rogers, *supra* note 13, at 316-17.

[233] U.C.C. § 3-307 cmt. 1 (1957).

[234] *Id.*

[235] *See E-Commerce is Biggest Between Business Sites*, N.Y. POST, Dec. 26, 1997, at 33 (noting business-to-business sales records). The Dell web site is located at <http://www.dell.com>.

[236] *Store Security* (visited Mar. 1, 1998) <http:www.dell.com/store/into/safe.htm>.

[237] *Security on the Land's End Web Site* (visited May 5, 1998) <http://www.landsend.com/spawn.cgi?NODESECURITY0897&GRAPHIC&ZEROPAGE&08878 25296159>.

[238] *Id.*

commerce. The CA supporting the use of SSL to communicate credit card information securely over the Internet is merely verifying the identity of the server so that a secure communication channel can be set up; it is not verifying the identity of the parties to the transaction in order to permit the parties to rely on digitally signed messages as binding contracts. Many advocates of public key cryptography assume that the primary application of this technology will be to bind the real world identity of an individual to an online identity. The success of retail Internet commerce web sites may question that assumption.

The volume of business-to-business Internet electronic commerce may soon dwarf the volume of Internet retail transactions. The most successful business-to-business electronic commerce site is that of Cisco Systems, which one source has reported as selling $3 billion a year of routers and other networking equipment over its web site by late 1997.[239] The Cisco model of business-to-business Internet electronic commerce is a variation of the trading partner agreement model developed for electronic data interchange business-to-business electronic commerce that gained popularity in the 1980s.[240] The contract between Cisco and the party wishing to purchase Cisco products over the Internet is the Networked Commerce Enrollment Agreement, which requires the customer to agree that he or she will be bound by the actions of anyone gaining access to the Cisco web site and ordering equipment through the use of the passwords issued the customer by Cisco.[241] The agreement also includes a list of authorized users and their passwords, which the customer may revise at any time, and a list of the terms and conditions governing the sale of goods and services.[242] Cisco does not accept enrollment agreements online. Instead, it requires customers seeking authorization to fax in a signed agreement which it will review and return by fax before the customer may begin placing orders online.

Cisco allocates the risk of loss of unauthorized use of passwords to the customer after requiring the customer to sign a contract making the allocation of risk explicit and requiring the customer to identify individuals authorized to trade with Cisco and to assign those individuals passwords.[243] This risk allocation is similar to that established in the Uniform Commercial Code in which the more technologically sophisticated party, the bank, must agree to commercially reasonable security procedure with its customer before the risk of loss due to unauthorized funds transfers can be shifted to the customer.[244] Cisco's procedures easily can be integrated into its existing purchasing procedures and are substantially

[239] *See E-Commerce is Biggest Between Business Sites*, *supra* note 235, at 33.

[240] For a discussion of EDI technology and the use of trading partner agreements, see Electronic Messaging Services Task Force, *The Commercial Use of Electronic Data Interchange—A Report and Model Trading Partner Agreement*, 45 BUS. LAW. 1645 (1990).

[241] *Cisco Systems, Inc. Networked Commerce Enrollment Agreement* (last modified Sept. 12, 1997) <http://www.cisco.com/warp/public/437/eca.html>.

[242] *See id.*

[243] *Id.*

[244] *See* U.C.C. §§ 4A-202(b), 203 cmt. 4 (1995).

similar to procedures used to conduct more traditional EDI electronic contracting.[245] Because the Cisco System operates as a series of bilateral contracts and the security it incorporates involves the use of passwords instead of public key cryptography, it would not be accurate to describe Cisco as a CA or the system it has built for its customers as a PKI. However, the success of the Cisco Internet electronic commerce system testifies to the resilience and continued relevance of existing models of electronic commerce in Internet environments.

Another business-to-business Internet commerce application that includes an operational PKI using public key cryptography is that part of the Open Access Same-time Information System (OASIS) which contracted with the Joint Transmission Services Information Network (JTSIN) Consortium for administrative and security services.[246] The OASIS program was created in response to a mandate from the Federal Energy Regulatory Commission (FERC) in 1996 to the electric energy industry to make information about the availability of transmission capacity accessible to customers over the Internet.[247] A coalition of eight (out of twenty) regional power pools formed the JTSIN Consortium to promote the use of interoperable technology and standards while complying with the FERC mandate.[248] The consortium contracted with several technology companies to design and operate its member web sites.[249] TradeWave, Inc. was selected to act as CA for the pools participating in the consortium.[250] The relationship between TradeWave as CA and the consortium members is similar to that of Cisco and its customers. TradeWave executed contracts with each participating electric utility in which TradeWave undertook to maintain a CRL. The actual issuance of certificates, however, is delegated to "local registration agents" (LRAs) who are designated by the electric utilities.[251] TradeWave does not accept responsibility for the issuance of unauthorized certificates because it requires the consortium participants to designate LRAs.[252]

The risk allocation model implemented by OASIS is similar to the risk allocation model in Article 4A of the U.C.C. The decision to delegate the oversight of the certificate issuance process to the electric utilities was made by the JTSIN consortium in light of which party was best able to prevent fraud or error. Before any electric utility assumed its responsibility as a LRA, their obligations were made clear in face-to-face negotiations with the representatives of TradeWave.[253] The

[245] *See generally* Electronic Messaging Services Task Force, *supra* note 240, at 1717 (model providing guidelines for establishing commercial trading practices which implement electronic data exchange).

[246] For a more detailed explanation of the operation of the OASIS PKI, see Alexander J. Cavalli & Jane K. Winn, *Internet Security in the Electric Utility Industry*, 39 Jurimetrics J. (forthcoming 1998) (manuscript on file with author).

[247] *Id.*

[248] *Id.*

[249] *Id.*

[250] *Id.*

[251] *Id.*

[252] Cavalli & Winn, *supra* note 246.

[253] *Id.*

OASIS PKI is now operational and has been successful in meeting the objectives of the JTSIN consortium members.[254] The cost of providing CA services is kept low because the most onerous responsibilities a CA might undertake have been devolved to the LRAs. Moreover, the LRAs were able to make informed decisions before accepting those responsibilities.

IV. IN WHAT WAYS ARE NEGOTIABLE INSTRUMENTS AND DIGITAL SIGNATURES SIMILAR? IN WHAT WAYS ARE THEY DIFFERENT?

At the most general level, negotiable instruments and digital signatures are similar in that they are both mechanisms for regulating the rights and obligations of parties to commercial transactions that can only be given effect if the parties comply with certain rigid formalities in their execution. Both mechanisms are regulated by a decentralized risk allocation system that forces parties to take responsibility for loss avoidance. This risk allocation is achieved both through a combination of substantive and pleading rules that attempt to streamline the enforcement of the rights of third parties against those releasing these devices into the stream of commerce. Neither classical negotiable instruments law nor the ABA Digital Signature Guidelines is sensitive to the inappropriateness of holding consumers to the same standards as commercial entities.

Beyond these general observations, any appearance of similarity rapidly begins to erode. At the most fundamental level, the classical doctrines of negotiable instruments law reflects centuries of development of commercial practice and the incremental development of commercial law through a colloquy between merchants, courts, and legislatures. By contrast, public key cryptography is not yet widely deployed in any business context. The debate over the proper regulation of this technology is only beginning, and no consensus has yet emerged. However, a group of advocates has been lobbying for certain statutory safe harbors to promote the use of this technology. Such legislation is clearly premature, however, in light of the uncertainty surrounding various competing models for implementing public key cryptography.

Apparently, consumers were not well represented in the drafting of the Digital Signature Guidelines. As a result, the Guidelines adopt a risk allocation model that is directly contrary to those used in established electronic commerce systems.[255] In modern risk allocation systems, losses due to error or fraud associated with the use of digital signature technology can be reduced by imposing losses on parties to the extent that such loss imposition provides incentives to modify behavior. Losses that cannot be avoided through the manipulation of loss imposition rules can be distributed among system participants through risk pooling and insurance systems. The Guidelines disregard these principles and allocate losses to subscribers and relying parties, which may include consumers or other technologically

[254] *Id.*

[255] *See generally* Winn, *supra* note 5, at 33 (discussing the approaches of VeriSign and the U.C.C.).

unsophisticated parties. The Guidelines shield CAs, who have the best opportunity to reduce losses through research and development and to pool risks through the collection of insurance premiums in the form of user fees. The drafters of the Guidelines focused a great deal of attention on what potential CAs might want in the way of limitations of liability, but neglected to discuss what constitutes appropriate levels of risk associated with consumer use of new technologies. Rather, the complex issue of precisely what type of precautions consumers can be expected to implement is subsumed by rules that require subscribers to maintain trustworthy systems and to prevent the compromise of their private key.[256]

The Digital Signature Guidelines were the product of thoughtful debates over a period of several years by a group of technologists and attorneys committed to encouraging the commercial exploitation of a specific technology. This is a very different process than that which produced the modern law regulating widely used negotiable instruments such as checks.[257] Negotiable instruments law developed through precedent until its restatement in the British Bills of Exchange Act, drafted in 1882.[258] In the United States, the first uniform law issued by the National Conference of Commissioners on Uniform State Law (NCCUSL) was the Negotiable Instruments Law in 1896, which was based in part on the British Act and which was then soon adopted in all states except Louisiana.[259] U.C.C. Article 4 now governs checks as they are handled within the check collection system and is based on the American Bankers Association Check Collection Code.[260] The ABA Check Collection Code was completed in 1929 and adopted in 18 states by 1932,[261] twenty-five years before its redaction into Article 4. The Check Collection Code was based on the American Bankers Association standard form contract, which had been in use since 1924.[262] In 1989, Article 4A, governing the law of funds transfers, was promulgated by NCCUSL. It applied to a funds transfer system that had been operation since the 1970s.[263] The much longer time periods over which these bodies of law evolved reflect not only an accumulated understanding among the participants of their legal rights and obligations, they also reflect the long experience of the participants with the underlying commercial transactions. Because commercial law is designed to enable private transactions rather than to impose regulatory mandates, there must first be a commercial practice for these new laws to be effective. No such commercial practice yet exists in the case of digital

[256] DIGITAL SIGNATURE GUIDELINES, *supra* note 6, §§ 4.1, 4.3, at 101, 103. The concept of a trustworthy system was developed by the U.S. Department of Defense in its Trusted Computer System Evaluation Criteria (TCSEC). *See supra* text accompanying notes 119-25.

[257] The accusation that Articles 3 and 4 of the U.C.C. represent a sell out to special interests is something that the Guidelines and the U.C.C. articles share. *See* Gilmore, *Formalism*, *supra* note 4, at 457 (commenting on the influences of the Negotiable Instruments Law of 1896 and the U.C.C.).

[258] *Id.*

[259] BRAUCHER & RIEGERT, *supra* note 37, at 21.

[260] *See* Hal S. Scott, *The Risk Fixers*, 91 HARV. L. REV. 737, 761-2 & n.80 (1978).

[261] *Id.* at 762.

[262] *Id.*

[263] BAKER & BRANDEL, *supra* note 126, ¶1.03[9].

signatures.

The Digital Signature Guidelines resemble one of the less successful amendments to the Uniform Commercial Code, the 1978 revision of Article 8 governing investment securities.[264] Article 8 was revised in the 1970s to take account of the movement in the securities industry away from paper-based processing toward computer processing for settlement and clearance of securities trades.[265] The 1978 amendments promoted the use of a specific technology—the certificate-less securities system being devised by the U.S. Treasury for U.S. government obligations.[266] The drafters of the 1978 revisions, like the drafters of the Guidelines, assumed that some encouragement was necessary to prod the private sector into following the lead of government in embracing a new technology. However, what the drafters failed to observe was that the securities industry was devising its own solution to the "back-office crunch" problem that was different from the solution devised by the Treasury.[267] As a result, by the late 1980s, leaders of the securities industry and their lenders asked the American Bar Association and NCCUSL to revise Article 8 to bring it into line with existing commercial practice. The language of the 1978 revisions bore no relationship to existing practices, and the lack of certainty surrounding the legal effect of common industry practices was feared likely to reduce the volume of credit lenders were willing to advance securities firms. The 1994 revisions to Article 8 were based on a careful analysis of current industry practices and include a novel approach to loss allocation that is based on an analysis of those practices.

Most provisions of the U.C.C. can be thought of as reflecting the incremental accumulation of business practice distilled into standard contract terms and further defined through case law. While it was not true historically, there is no longer any impediment to the use of general contract law by business parties to achieve the functional equivalent of negotiability.[268] Likewise, there is no legal impediment to a party wishing to offer commercial CA services within an Internet PKI to bind both the subscriber and the relying party by contract to the limitations it wishes to impose on its liability arising from transactions entered into in reliance on its certificate. The impediment at this point is cost, and certain business models of how to develop a market for CA services in the Internet marketplace will not be able absorb the high cost of contracting with all the parties to transactions using digital signature certificates. There is plenty of evidence that some parties are finding viable business models for deploying public key cryptography in commercial

[264] *See* U.C.C. Article 8, Prefatory Note (1995) (discussing the 1978 amendments); James Steven Rogers, *Policy Perspectives on Revised U.C.C. Article 8*, 43 UCLA L. REV. 1431, 1441-49 (1996) (explaining the requirements of the new system).

[265] *Id.*

[266] *See* Charles W. Mooney, Jr., *Beyond Negotiability: A New Model for Transfer and Pledge of Interests in Securities Controlled by Intermediaries*, 12 CARDOZO L. REV. 305, 311-12 (1990).

[267] *Id.* at 311 n.6.

[268] *See generally* David Frisch & Henry D. Gabriel, *Much Ado About Nothing: Achieving Essential Negotiability in an Electronic Environment*, 31 IDAHO L. REV. 747, 760-72 (1995) (disussing the need for alternatives to traditional paper-based rules in electronic commerce).

environments, and until there is more evidence about which models will succeed and which will fail, legislatures should not intervene to favor one commercial venture over another.

Commercial law is best positioned to enable transactors to conduct their business efficiently when the doctrines of commercial law resonate with the common understanding of the parties. The common understanding of parties conducting electronic commerce in large volumes today is not reflected in the ABA Digital Signature Guidelines. The meteoric rise of the Internet from an obscure network used by academics and technologists to a popular culture phenomenon in only a matter of months indicates the fact that it is far from certain that Internet electronic commerce will indeed build on existing models of commercial practice. However, with each passing month there is more evidence that many of the first commercial applications are simply not viable business models, and that applications of Internet technology that build incrementally on existing experience with electronic commerce may very well succeed.

V. CONCLUSION

The idea that certain doctrines of the law merchant, such as negotiability, developed outside the common law and in sharp opposition to it was once a widely accepted notion among academics and practicing attorneys interested in the development of commercial law. This idea has been shown by recent scholarship to be inaccurate. It seems based on little more than some spectacularly bad readings of a few reported judicial opinions studied in isolation from their larger historical context. Negotiable instruments law developed incrementally, through a dialogue between courts, legislators, and the business community. The development of the Digital Signature Guidelines resembles the mythic account of the development of the doctrines of negotiability, however, more than it does the more accurate revisionist account.

The Guidelines attempt to import wholesale into commercial law a normative framework based on technical standards developed by engineers without reference to most major existing electronic commerce applications. The assumption of the Guidelines' drafters seems to have been that the future of open network electronic commerce will be so different from existing closed network electronic commerce that existing models would not be helpful for their project. Given the absence of any established commercial practices corresponding to their model transaction, the Guidelines adopt a regulatory rather than enabling posture. However, it remains to be seen whether open network electronic commerce will in fact be so radically different from closed network electronic commerce, and whether the Guidelines will have the anticipated channeling effect on the development of electronic commerce.

The risk allocation model suggested in the Digital Signature Guidelines draws on the risk allocation model contained in classical negotiable instruments law. The use of rules that resemble negotiability to make a new product more marketable in commerce mirrors in many respects the spread of the doctrines of negotiability to encompass many new types of commercial transactions that were documented by Professor Gilmore in 1954.[269] The analogy quickly breaks down, however, because the spread of negotiability noted by Professor Gilmore reflected commercial practices and was not imposed on the parties by regulators outside the business community.

If parties to a commercial transaction are able to adopt risk avoidance or risk pooling strategies, then the parties may find that loss allocation rules such as negotiability suit their needs well. However, under modern conditions of communication and information processing efficiency, the parties have alternatives to predictable but harsh systems of loss allocation like negotiability. In any modern system of commercial transactions, risk management systems involving centralized risk pooling and insurance should be considered before a system that imposes losses on consumers who will not be able to predict or control the risk.

Dwight Arthur, a professional technologist who has closely followed the debates about how best to develop PKIs that can support the commercial exploitation of the Internet, suggested an analogy for understanding why it might be premature to develop detailed regulations governing the commercial use of public key cryptography. He suggested that the commercial use of the global information infrastructure is now at an equivalent level of development to that of the national transportation infrastructure of the United States in the late nineteenth century. The internal combustion engine had been invented, and the use of asphalt for paving roads had been developed. The current effort to regulate how PKIs will ultimately be used on the Internet makes as much sense as trying to draw up regulations governing the interstate expressway system in light of the knowledge of the properties of internal combustion engines and tarmac.[270] The impulse behind the Digital Signature Guidelines is laudable, but the analogy to well established commercial practices and commercial law doctrines that regulate them is poorly taken. Before a commercial law of Internet commerce can develop, a record of successful commercial practices must first be established.

[269] Gilmore, *Good Faith*, *supra* note 15.

[270] This analogy was created by Dwight Arthur, Managing Director of Technology, National Securities Clearing Corporation. E-mail correspondence with Dwight Arthur (Aug. 15, 1997) (on file with author).