RECENT DEVELOPMENTS IN DIGITAL SIGNATURE LEGISLATION AND ELECTRONIC COMMERCE

By Kalama M. Lui-Kwan

While many of the new information policies regulate the activity growing out of the new information economy—such as decency,[1] class action lawsuits,[2] and taxes[3]—only a few deal with the underlying electronic commerce infrastructure. One such bill considered by Congress this year deals with the enforceability of digital signatures, an authentication method which will prove to be one of the necessary components in the next stage of electronic commerce development.[4] Digital signature technology will probably influence the evolution of online businesses and electronic commerce.

Electronic commerce has provided thousands of companies and millions of consumers with the opportunity to generate and spend revenue at an incredible pace. How many people are shopping online? According to eMarketer, the number of online buyers will double in the year from December 1998 to December 1999 to 36.1 million, or 16.6% of the American population fourteen years or older.[5] How many users are actually purchasing goods or services? Jupiter Communications estimates that 35% of the online population purchased a service or product between 1997 and 1998, and that 95% of those buyers planned on shopping again in coming months.[6] IntelliQuest's data reflects a similar trend.[7] That organization's study found that 81% of those surveyed intended to shop or buy online in the next 12 months.[8] How much revenue will online stores generate in

1. *See* S. 1619, 105th Cong. (1998); S. 1482, 105th Cong. (1998).
2. *See* S. 1260, 105th Cong. (1998).
3. The Internet Tax Freedom Act was signed into law on October 21, 1998. *See* H.R. 4105, 105th Cong. (1998). *See generally* Christopher Cox, *Internet Tax Freedom Act Home Page* (visited Dec. 5, 1998) <http://www.house.gov/chriscox/nettax/>.
4. *See* H.R. 3472, 105th Cong. (1998); S. 1594, 105th Cong. (1998).
5. *See* eMarketer, *eCommerce Retail Shopping Report Sneak Preview #2: Number of Online Buyers will Double in 1999* (visited Dec. 5, 1998) <http://www.emarketer.com/ estats/ecsr_sneak2.html>.
6. *See* CyberAtlas, *Online Buyers Double by End of 1999* (visited Dec. 5, 1998) <http://cyberatlas.internet.com/market/retailing/emark.html>.
7. *See* eMarketer, *E-Commerce: It Just Keeps Growing* (visited Dec. 5, 1998) <http://www.emarketer.com/estats/113098_ecom.html>.
8. *See id.*

coming years? eMarketer claims that consumer online shopping revenues in the United States will rise from $4.5 billion in 1998 to approximately $15 billion in 2000 and to $35.3 billion by 2002.[9] Forrester Research estimates that global electronic commerce sales will be as high as $3.2 trillion by 2003.[10] Where are users spending their money? Jupiter Communications found that 48.7% of online consumers have purchased cars, 36.2% have purchased housewares, 35.9% have bought clothing, and 35.8% have purchased consumer electronics.[11] Investment bank Piper Jaffray found in a recent study that 22% of all retail securities trades in the first half of 1998 were conducted online. In fact, Piper Jaffray estimates that that percentage will increase to 27% of all retail trades in 1998.[12] These numbers reflect the incredible speed at which electronic commerce has grown over the past year, as well as the potential it holds for coming years. More important for the purposes of this paper, and for policymakers, is how these numbers demonstrate the importance of global electronic commerce to consumers and the need for laws that regulate, or refrain from regulating, their behavior.

How will digital signatures impact the online environment? Digital signatures essentially allow parties to authenticate their documents when communicating online.[13] This is particularly useful for parties who want to know that their contract is enforceable, or for companies that want to be assured that customers with whom they are dealing online are truthfully representing themselves.[14] Therefore, digital signatures are likely to have a

---

9. *See* eMarketer, *eCommerce Retail Shopping Report Sneak Preview #1: The Size and Growth of the Consumer eCommerce Market* (visited Dec. 5, 1998) <http://www.emarketer.com/estats/ecsr_sneak1.html>.

10. *See* Forrester Research, Inc., *Forrester Estimates Worldwide Internet Commerce Will Reach As High As $3.2 Trillion In 2003* (visited Dec. 5, 1998) <http://www.forrester.com/Press/Releases/Standard/0,1184,114,00.html>.

11. *See* CyberAtlas, *Price Holds Back Non-Shoppers* (visited Dec. 5, 1998) <http://www.cyberatlas.internet.com/market/retailing/price.html>.

12. *See* Piper Jaffray, Inc., *On-Line Trading Volumes Equal 22 Percent of All Retail Trading, According to Fifth Quarterly Piper Jaffray Report* (visited Dec. 5, 1998) <http://www.pjc.com/re/re_ne2.asp?id=108 >.

13. *See generally* VeriSign, Inc., *VeriSign Digital ID Center* (visited Jan. 29, 1999) <http://digitalid.verisign.com/id_intro.htm#whatis_signature>.

14. A vice-president at Visa USA, for example, explained during Senate testimony that the "authentication of the various parties participating in the Visa payment system, including cardholders, merchants, and Member financial institutions, is essential to the operation and integrity of this enormous payment network." *The Digital Signature and Electronic Authentication Law of 1998: Hearings on S. 1594 Before the Subcomm. on Financial Services and Technology*, 105th Cong. 1 (1998) (statement of Mr. Ken Liberman, Senior Vice President for Corporate Risk Management at Visa USA). A representative from The Bankers Roundtable echoed Lieberman's remarks, stating that, "[e]ven in

number of beneficial commercial applications. For example, companies that receive credit card numbers online will be able to use digital signature technology to verify the true identity of senders.[15] Digital signatures present extremely valuable opportunities for parties to enter into agreements outside of the client-merchant relationship. For example, if digital signatures were recognized under the law as an enforceable signature, an e-mailed offer of employment would be legally binding, just as if it were sent in writing and signed by the employer. Parties to a business agreement could negotiate deals more quickly with digital signatures because they would be able to tell whether their transmissions to each other were tampered with in transit and whether the information they received was truly sent by the other named party and not by an imposter.

Digital signatures should play an especially critical role as electronic commerce stands because authentication is growing more and more important. According to a study conducted by the Graphic, Visualization & Usability Center at the Georgia Institute of Technology, 48.6% of the more than 10,000 respondents indicated that they never provide false information.[16] This means that more than half of the respondents do actually report false information. If we rely on eMarketer's estimates regarding the size of the online consumer population,[17] more than 18 million American consumers will falsify their identities or personal information online by late 1999. This has become an important issue for companies as well as federal and state policymakers. As the Department of Commerce General Counsel indicated at a forum on authentication technologies, digital signatures are a "critical ingredient" in the development of private sector and public sector confidence in electronic commerce.[18]

---

this more complex world, businesses still need to assure that the person entering into a contract may be identified and consumers want to know that they are not liable for agreements that they did [not] enter." *Id.* (statement of Mr. Alfred Pollard, Senior Director for Legislative Affairs, The Bankers Roundtable).

15. Under the American Bar Association Digital Signature Guidelines, enforceable digital signatures should at least be able to "indicate who signed a document, message or record, and should be difficult for another person to produce without authorization." Information Security Committee, Electronic Commerce Division, Section of Science and Technology, American Bar Association, *Digital Signature Guidelines, Tutorial*, Aug. 1996, 3-7 *available at* <http://www.abanet.org/scitech/ec/isc/dsgfree.html>.

16. *See* Georgia Tech, *GVU's 9th WWW User Survey* (visited Dec. 5, 1998) <http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-04/>.

17. *See* CyberAtlas, *Online Buyers Double by End of 1999*, *supra* note 6.

18. *See Hearing on Electronic Authentication and Digital Signature: Hearings on S. 1594 Before the Subcomm. on Financial Services and Technology*, 105th Cong. 1 (1997) (statement of Mr. Alfred Pollard, Senior Director of Legislative Affairs, The Bankers

This paper will focus on the role of digital signatures in the growth of electronic commerce and on the recent legislative response to digital signatures by both federal and state policymakers. Because a full discussion of digital signature technology is beyond the scope of this Note, Part I provides only a brief overview of the digital signature technology. Part II discusses why digital signatures are useful, and what problems are created by their use. Part III reviews selected state and federal bills that have been enacted or proposed over the past year. Part IV proposes a number of issues that federal policymakers should consider as they vote on pending legislation and draft future bills. The paper concludes that, just as companies have developed technologies to address the problem of authentication, proactive policymakers can and should provide an appropriate legal infrastructure for digital signatures that balances the needs of both companies and consumers.

I. DIGITAL SIGNATURES DEFINED

Digital signatures authenticate electronic documents in much the same way that handwritten signatures authenticate printed documents.[19] Recipients of electronic documents accompanied by digital signatures may verify that senders are who they claim to be and that the documents have not been altered from the time of transmission.[20] In other words, senders may not disown digital signatures by claiming that they have been forged, and recipients can verify the identity of senders as well as the integrity of the documents

Digital signatures typically require the use of two keys, which are paid for by the sender and issued by a Certification Authority ("CA").[21] CAs are trusted third parties, such as banks or companies that specialize in digital signature technology, from which individuals and corporations can

---

Roundtable, quoting remarks by Department of Commerce General Counsel Andrew Pincus).

19. However, digital signatures do not guarantee privacy to users. Digital signatures are designed strictly for authentication purposes, and do not provide any privacy protections. *See* Graham Greenleaf & Roger Clarke, *Privacy Implications of Digital Signatures* (last modified Mar. 10, 1997) <http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html> (concluding that, as a result of the information that digital signatures reveal about individuals and the access given to organizations that have usually not been trusted by the public, consumers will "demand explicit privacy protections, far more substantial than the weak and patchy regime that is presently in place.").

20. *See* VeriSign, Inc., *VeriSign Digital ID Center*, *supra* note 13.

21. *See* A. Michael Froomkin, *Article 2B as Legal Software for Electronic Contracting—Operating System or Trojan Horse?*, 13 BERKELEY TECH. L.J. 1023, 1029 (1998).

purchase two keys, one "private" and one "public."[22] The private key is known only to the sending party, whereas the public key is publicly available. The keys are mathematically related, such that a message decrypted with the public key could have been encrypted only with the private key. Therefore, if a sender signs a document with his private key, the recipient can use the sender's public key and signature to confirm the authenticity of the document.

The technology works as follows. After writing his message, the sender performs a mathematical computation on his document, known as a "hash function," to generate a string of code called a "message digest."[23] Because the message digest is based on the specific content of this original document, any changes to the document would yield a different message digest.[24] The sender then encrypts this message digest with his private key, attaches this "signature"[25] to the end of the document, and sends the "signed" document to the recipient.[26]

The recipient, who has access to the sender's public key, may now verify both the sender's identity and the integrity of the document.[27] She does this by decrypting the "signature" with the sender's public key, which reveals the original message digest.[28] She then performs the hash function on her copy of the document, generating a fresh copy of the message digest.[29] Finally, she compares the two copies of the message digest, and, if they are identical, the recipient knows two things. First, she knows the information was not altered from the time it was sent until the time it was received,[30] and, therefore, was not altered in transit by hackers or technical malfunctions.[31] Second, because she successfully decrypted the message digest with the sender's public key, she knows it could only have been encrypted with the sender's private key.[32] Because only the sender

22. *See* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 51-53 (1996).

23. *See* VeriSign, Inc., *VeriSign Digital ID Center* (visited Feb. 20, 1999) <http://digitalid.verisign.com/id_intro.htm#signature_use>.

24. *See* Utah Department of Commerce, *Digital Signature Tutorial* (visited Nov. 16, 1998) <http://www.commerce.state.ut.us/web/commerce/digsig/tutorl.htm>.

25. *See* VeriSign, Inc., *VeriSign Digital ID Center*, *supra* note 23.

26. *See* Utah Department of Commerce, *Digital Signature Tutorial*, *supra* note 24.

27. *See id.*

28. *See id.*

29. *See id.*

30. *See id.*

31. *See id.*

32. *See* VeriSign, Inc., *VeriSign Digital ID Center*, *supra* note 13.

has access to his private key, the document could only have been sent by the sender.[33]

As an illustration, suppose Larry wants to send a digitally signed contract to Jen. He can create a message digest by applying a hash function to the contract. The message digest is a kind of encoded fingerprint; if any aspect of the message changes between the time Larry sends the message and the moment Jen decrypts the message, the fingerprint will change and Jen will be able to tell that the message has been altered. Larry encrypts the message digest with his private key, which he purchased from a popular and reliable Certificate Authority called, say, the Bank of Truth, Law and Justice ("BTLJ"). BTLJ is a trusted third party, and, like other banks, regularly performs other daily functions, such as providing loans to and holding deposits for its customers.[34] Larry sends the encrypted message digest and the contract to Jen. When Jen receives Larry's message, she has before her both the contract document and the encrypted message digest, which is Larry's digital signature. Using Larry's public key, which she also acquired from BTLJ, Jen decrypts the encrypted message digest. She then performs a hash function on the document to produce a new message digest. If the message digests match, Jen knows that the document was indeed sent from Larry and was not altered during transmission. She can be sure of these things because, first, Larry's public key can decrypt only those digital signatures encrypted by Larry's private key, and, second, the new message digest is identical to the message digest unlocked by the public key. This digital signature method is commonly known as Public Key Infrastructure ("PKI").[35]

II. DIGITAL SIGNATURES AND ELECTRONIC COMMERCE

A. Why Digital Signatures are Useful

Digital signature technology's greatest strength lies in its ability to authenticate and legally bind parties to online contracts and agreements,

---

33. *See id.*

34. *See id.*

35. *See generally* Thomas Smedinghoff, Government Information Technology Services Federal PKI Task Force Business and Legal Work Group, *Model Certificate Policy: Issues Regarding Certificate Policies* (last modified Mar. 25, 1998) <http://www.mbc.com/modelcp.html>. *See also* Santosh Chokhani & Warwick Ford, *Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*, Apr. 25, 1998, *available at* <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt> (discussing the popular X.509 international standard for authentication); American Bar Association, *Digital Signature Guidelines, Tutorial, supra* note 15.

just as handwritten signatures authenticate and bind parties in the paper-based world. Signatures typically serve four functions. First, signatures authenticate signers by providing evidence of their relationship to an agreement.[36] The traditional reliance on signatures is based, in part, on the difficulty of replicating the signatures of other people. Second, a document containing a handwritten signature is valuable because it is presumably original and authentic.[37] Third, signatures represent the affirmative act of signers who, with their signatures, establish the sense of having legally bound themselves to an agreement.[38] Finally, signatures provide a certain level of efficiency, especially when signatures are used to indicate authorization of a transaction.[39]

Under existing law, the Statute of Frauds requires signatures, but does not invalidate agreements made without signatures.[40] It does, however, render such transactions unenforceable in court.[41] If digital signatures were given the legal force of handwritten signatures, they would put to rest many questions that consumers and sellers alike have with conducting business online.[42] The introduction of digital signatures would make more companies feel comfortable with doing business online because they would be less concerned that people were using, for example, false credit card and checking account numbers or mailing addresses.[43] Similarly,

---

36. *See* American Bar Association, *Digital Signature Guidelines, Tutorial, supra* note 15; Lon L. Fuller, *Consideration and Form*, 41 COLUM. L. REV. 799, 800 (1941).

37. *See* American Bar Association, *Digital Signature Guidelines, Tutorial, supra* note 15.

38. *See id.*

39. *See id*; *see also* Fuller, *supra* note 36, at 801-02.

40. *See* American Bar Association, *Digital Signature Guidelines, Tutorial, supra* note 15; *see also* ARTHUR L. CORBIN, CORBIN ON CONTRACTS § 279, at 20-23 (1950). Digital signature technology is far from the first innovation to challenge traditional paper-based contract law. The telegraph, for example, provided a new format for negotiating and accepting contracts. Although more efficient, the telegraph created new "implications of erroneous messages" that led to questions regarding whether telegraphed contracts were enforceable. Marc Szafran, Note, *A Neo-Institutional Paradigm for Contracts Formed in Cyberspace: Judgment Day for the Statute of Frauds*, 14 CARDOZO ARTS & ENT. L.J. 491, 502-03 (1996). Digital signatures now have to overcome the same legal barrier once faced by the telegraph. The benefit of conducting transactions online outweigh the costs, but the Statute of Frauds still presents a question as to whether agreements that are electronically made will be legally enforceable. *See* R.J. Robertson, *Electronic Commerce on the Internet and the Statute of Frauds*, 49 S.C. L. REV. 787, 797 (1998).

41. *See* American Bar Association, *Digital Signature Guidelines, Tutorial, supra* note 15.

42. *See id.*

43. *See id.*

consumers may feel more comfortable doing business online because, in addition to the relative ease with which they may conduct transactions, they would be able to rest assured that the company they are dealing with is, in fact, the company it represents itself to be. For both parties, enforcing contracts using digital signatures would be simpler in the digital environment, provided that state and federal law recognizes digital signatures as representations that are as enforceable as handwritten signatures.[44]

The ease with which companies could adopt digital signature technology should create a number of opportunities for both consumers and corporations to engage in electronic commerce transactions. Using digital signature technology, for example, clients of an online stock trading service could acquire information about companies and purchase stock in those companies without defrauding the stock trading company by disclaiming the purchase of a stock that happens to suddenly plummet in value. Similarly, online stock trading services would be unable to disclaim quoted stock prices should there be any disagreement over whether the client purchased shares in a company based on information provided by the trading service at a given time.[45] The digital signature technology involved with the actual trade would not only have the capacity to stamp a date and time to the transaction, but also would allow both the and the service to verify that the other party was in fact engaged in the transaction. This is but one example of the almost innumerable commercial uses for digital signatures.

---

44. Digital signature technology, of course, is not going to solve all of the problems of contracting online. While digital signatures confer upon companies the benefit of authenticating their clients' information, they fail to resolve the problem of privity in the digital environment. *See* Robert Merges, *The End of Friction? Property Rights and Contract in the "Newtonian" World of On-Line Commerce*, 12 BERKELEY TECH. L.J. 115, 119 (1997). In addition to consent, enforceability of agreements made both online and in traditional business transactions requires privity between the original parties to the contract, as well as each party in the chain of possession. Suppose, for example, Diana licenses a software application to Ethan for use on one computer, and Ethan purchases the source code for the application to develop and sell his own competing version from Heather, who was party to a non-disclosure agreement with Diana. Further suppose that Ethan develops a competing version and posts the source code on a web site, from which Kenton downloads the information and develops his own version. Diana may have a cause of action against Heather, but not against Ethan, except through Heather, and probably not against Kenton at all. The transaction cost of enforcing agreements in this example are potentially high for Diana.

45. *See* VeriSign, Inc., *VeriSign Press Release: Barclays Selects VeriSign OnSite to Secure the First Online, Real-Time Share Trading System in the UK* (visited Feb. 13, 1999) <http://www.verisign.com/press/customer/barclays.html>.

B. Problems Raised by the Use of Digital Signatures

There are two obvious barriers confronting users of digital signature technology. First, as with almost all forms of technology, digital signature capabilities are not free. The institutional cost to the public may be significant, depending on the ability of decision-makers to plan effectively. Creating CAs, or at least designating pre-existing, trusted third parties, may be costly. At a minimum, existing institutions will need to spend money training their representatives to explain and sell the keys and software. At the opposite extreme, it will be expensive to create new institutions, establish accreditation procedures, and determine how to license and audit CAs.[46] There are also individual costs that a single user or a corporation must incur to purchase the actual software and keys from a CA.[47] The calculation of whether these costs exceed the benefits of creating a more predictable commercial and legal environment depends on whether policymakers can appropriately design and enact legislation that addresses the benefits and costs of digital signatures.

Second, while digital signatures may allow parties to enter into enforceable contracts, the multiplicity and differences among different state bills and laws relating to the use of digital signatures poses a problem for the widespread use and acceptance of the technology. This is a problem virtually as old as the Internet itself: what laws govern in cyberspace? If, for example, a consumer in California enters into an agreement with an online company based in Virginia with the assistance of digital signature technology, it is unclear which state law would govern the use of the technology and whether the digital signature would make the agreement as enforceable as if it were signed by a handwritten signature.

III. STATE AND FEDERAL DIGITAL SIGNATURE LEGISLATION

The fundamental question of how companies can safely identify users with whom they enter into agreements online was answered by the private

---

46. According to the American Bar Association's Science and Technology Section, the two general costs involved with using digital signatures are the costs of institutional overhead ("The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring quality in the performance of their functions.") and the costs to subscribers and relying parties, such as software and a payment to the CA for issuing the keys. *See supra* American Bar Association, *Digital Signature Guidelines, Tutorial,* note 15, at 16-17.

47. *See id.*

sector, which developed the technology behind digital signatures.[48] The remaining issue was whether companies would be allowed to use this technology under existing law and, if so, whether the technology would be recognized to the same extent as a handwritten signature. It seems that state legislatures, and their consumer constituents, were the logical bodies to address the legal issue.[49] The problem was that many states developed different and, in many cases, incompatible approaches.[50] As it became clearer to U.S. Senators and Representatives that these jurisdictional conflicts of law were inhibiting the development of electronic commerce across state borders, federal legislation became increasingly important.[51]

The widespread use of authentication technologies, including digital signatures, has been limited by the differences between different pieces of state legislation. While most states have passed or at least considered legislation relating to digital signatures, there is no national standard. More than forty states have enacted legislation authorizing the use of digital signatures, but many limit the types of functions for which digital signatures may be employed.[52] For example, although Utah[53] and the State of Washington permit the use of digital signatures for almost all public and private forms of communication,[54] Alabama's state government only recognizes digital signatures when filing tax returns and other documents with the

---

48. One of the first commercially successful companies to develop the digital signature technology is VeriSign. *See, e.g.*, VeriSign, Inc., *VeriSign Digital ID Center* (visited Jan. 29, 1999) <http://digitalid.verisign.com>.

49. Indeed, as indicated by Thomas Smedinghoff of McBride Baker & Coles, most states that have sought to address the issues raised by digital signatures have "concluded that it is necessary for a state agency ... to issue regulations governing the implementation and use of a digital signature infrastructure[.]" Thomas Smedinghoff, *Analyzing State Digital Signature Legislation* (last modified Aug. 1997) <http://www.mbc.com/ds_rev.html>. *See generally* Thomas Smedignhoff, *Summary of Electronic Commerce And Digital Signature Legislation* (last modified Dec. 1, 1998) <http://www.mbc.com/ds_sum.html>.

50. *See infra* note 75 and accompanying text.

51. Senator Bob Bennett, for example, issued a press release in 1998 stating that he would be introducing "the Digital SEAL (Signature and Electronic Authentication Law)" because he recognized the "immediate need for discussion of technology's impact on modern financial transactions. *See* Sen. Bob Bennett, *Sen. Bennett—Press Release* (visited Aug. 29, 1998) <http://www.senate.gov/~bennett/pr020298.html>.

52. Thomas Smedinghoff of the Chicago firm McBride, Baker & Coles maintains an updated list of state, federal and international statutes related to digital signatures. *See* Smedinghoff, *Summary of Electronic Commerce And Digital Signature Legislation*, *supra* note 49.

53. *See* S. 107, 52nd Leg., 1st Reg. Sess. (Utah 1998).

54. *See* WASH. REV. CODE § 19.34 (1998).

Department of Revenue.[55] Colorado allows the use of PKI-based digital signatures only for the electronic filing of UCC financing statements.[56] Maine limits the use of PKI-based digital signatures to applications under the Motor Vehicle Code.[57] The Hawaii State Legislature has passed legislation authorizing the use of digital signatures, but only to file electronically court documents.[58] New Jersey's state legislature does not recognize the legal authority of digital signatures at all. California allows residents to use digital signatures to communicate with public agencies and file community college admissions applications, certain securities-related documents, certificates of death, and various reports required under the Political Reform Act of 1974.[59] The Nevada State government limits the use of digital signatures to financial transactions with the state and to filings with state courts and public agencies.[60] Missouri limits the use of digital signatures to filings by business organizations of documents with the Secretary of State and to electronically filed reports by candidates for public office.[61]

While some states have been reluctant to authorize the widespread use of digital signatures, a select number of states have decided to embrace the authentication method. Among the states with far-reaching digital signature legislation include Georgia,[62] West Virginia,[63] Iowa,[64] New Hampshire,[65] Wisconsin,[66] Kansas,[67] Alaska,[68] South Dakota,[69] Minnesota,[70] Nebraska,[71] Kentucky,[72] Oregon,[73] and Illinois.[74]

---

55. *See* ALA. CODE § 40.30 (1997).
56. *See* S. 97-155, 61st G.A., 1st Reg. Sess. (Colo. 1997).
57. *See* S. 473, 118th Leg., 1st Reg. Sess. (Me. 1997).
58. *See* HAW. REV. STAT. § 601 (1995).
59. *See* CA GOV'T CODE § 16.5; Ass. 521, 1997-1998 Leg., 1st Reg. Sess. (Cal. 1997); Ass. 521, 1997-1998 Leg., 1st Reg. Sess. (Cal. 1997); Ass. 2755, 1995-1995 Leg., 1st Reg. Sess. (Cal. 1995); S. 49, 1997-1998 Leg., 1st Reg. Sess. (Cal. 1997).
60. *See* S. 42, 69th Leg., 1st Reg. Sess. (Nev. 1997); Ass. 386, 69th Leg., 1st Reg. Sess. (Nev. 1997).
61. *See* S. 844, 89th G.A., 2nd Reg. Sess. (Mo. 1998); S. 680, 89th G.A., 2nd Reg. Sess. (Mo. 1998).
62. *See* S. 103, 144th G.A., 1st Reg. Sess. (Ga. 1997).
63. *See* H.R. 4293, 73rd Leg., 2nd Reg. Sess. (W. Va. 1998).
64. *See* H.F. 2474, 77th G.A., 1st Reg. Sess. (Iowa 1997).
65. *See* H.R. 290, 155th G.C., 1st Reg. Sess. (N.H. 1997).
66. *See* Ass. 811, 93rd Leg., 1st Reg. Sess. (Wis. 1997).
67. *See* H.R. 2059, 77th Leg., 1st Reg. Sess. (Kan. 1997).
68. *See* S. 232, 20th Leg., 2nd Reg. Sess. (Alaska 1997).
69. *See* S.B. 63., 74th Leg., 1st Reg. Sess. (S.D. 1999).
70. *See* S. 2068, 80th Leg., 1st Reg. Sess. (Minn. 1997).
71. *See* Leg. 924, 95th Leg., 2nd Reg. Sess. (Neb. 1997).
72. *See* H.R. 708, 1998 Leg., 1st Reg. Sess. (Ky. 1998).
73. *See* H.R. 3046, 69th Leg., 1st Reg. Sess. (Or. 1997).

In addition to their disagreement over when digital signatures should be enforceable, states also make widespread use difficult by authorizing incompatible technologies. Citibank's General Counsel, for example, has explained that

> [s]ome states provide that electronic authentication must be accomplished through public key cryptography. Still others maintain that mere "electronic signatures"—which use any electronic or digital method employed by the parties—are adequate to establish message and identity authentication. However, these methods will lead to incompatible and non-interoperable authentication systems, as well as less secure, less trustworthy and possibly rogue authentication systems that could undermine the safety and soundness of electronic banking and commerce.[75]

As a result of the differences among state laws, legal and some technical incompatibility issues prevent an end user in Connecticut – which limits the use of digital signatures to updating medical records maintained in hospitals[76] – from using a digital signature to authenticate a message sent to a server based in, say, Wyoming, which limits the use of digital signatures to filings with the Secretary of State.[77] It is technically possible for the user in Connecticut to purchase books online from a store in Wyoming, but the user would probably be unable under state law to send an enforceable digital signature to the store's server. This is one of a multitude of possible scenarios where state laws inhibit the authentication capability offered by digital signatures. While it is commendable that state legislatures have attempted to authorize the use of digital signatures, state regulations have unquestionably hampered interstate electronic commerce.

The U.S. Congress has responded with hearings on digital signatures and legislation in both the House[78] and the Senate.[79] On February 2, 1998, Senator Robert Bennett introduced legislation that would enable financial institutions to use digital signatures to authenticate transactions with their

74. *See* H.R. 3180, 1997-1998 Leg., 1st Reg. Sess. (Ill. 1997).

75. *See Hearing on Electronic Authentication and Digital, supra* note 18 (statement of Mr. P. Michael Nugent, General Counsel for Technology and Intellectual Property, Citibank).

76. *See* CONN. GEN. STAT. § 19a-25a (1997).

77. *See* WYO. STAT. ANN. § 9-1-306 (1996).

78. *See* H.R. 3472, 105th Cong. (1998).

79. *See* S. 1594, 105th Cong. (1998).

customers.[80] He called hearings to discuss the limitations and possibilities of digital signatures in October 1997 and again in March 1998.[81] In their prepared testimony, participants frequently repeated a number of issues any piece of federal legislation should consider when addressing digital signature use and standards.[82]

First, federal legislation should be offered for the sake of providing a uniform legal framework.[83] This is particularly important because the discrepancies among state laws stunt interstate electronic commerce. Furthermore, the failure to develop a national standard could inhibit the development of national Certification Authorities or even "severely limit the ability of CAs to operate across state or national borders."[84] Second, legislation should allow non-financial institutions to participate in the use of electronic authentication services.[85] Recent advances in electronic authentication and security have focused on the requirements of financial transactions. For example, Secure Electronic Transaction and Open Trading

---

80. *See The Digital Signature and Electronic Authentication Law of 1998: Hearings, supra* note 14 (statement of Robert F. Bennett, Chairman, Subcomm. on Financial Services and Technology).

81. For a full list of witnesses and testimony at both hearings, see Senate Banking Committee, *Witness List and Prepared Testimony, Hearing on Electronic Authentication and Digital Signature* (visited Aug. 29, 1998) <http://www.senate.gov/~banking/97_10hrg/102897/witness/witness.htm>; Senate Banking Committee, *Witness Panel, Hearing on S.1594, The Digital Signature and Electronic Authentication Law of 1998* (visited Aug. 29, 1998) <http://www.senate.gov/~banking/98_03hrg/031198/witness/witness.htm>.

82. *See* Senate Banking Committee, *Witness List and Prepared Testimony, supra* note 81; Senate Banking Committee, *Witness Panel, supra* note 81.

83. The senior vice president for Visa explained during testimony that "the benefits of digital signature technology can be maximized for the Visa system only if this technology can be used in the same way throughout the United States." *The Digital Signature and Electronic Authentication Law of 1998: Hearings, supra* note 14. Alfred Pollard, of The Bankers Roundtable, similarly argued that, "electronic commerce would operate under extreme disadvantage and development would be hindered if state laws subjected a device intended to provide customer security and system integrity to uneven and conflicting enforcement." *Id.*

84. *Hearing on Electronic Authentication and Digital Signature, supra*, note 18 (statement of Mr. Robert Kramer, Vice President for Policy Analysis and Development, Bank of America).

85. Harris Miller, of the Information Technology Association of America, stated that the scope of the bill should be extended beyond financial institutions to include "insurance companies, brokerage houses, mutual funds, and new Internet businesses [that] provide various types of financial services to American consumers and are involved in business to business transactions." *The Digital Signature and Electronic Authentication Law of 1998: Hearings, supra* note 14 (statement of Mr. Harris N. Miller, President, Information Technology Association of America).

Protocols are two methods that have been adopted to provide some security standards on the web. Partly because of the broad acceptance of these methods, some industry advocates have pushed for federal legislation that would allow depository institutions insured by the FDIC to use electronic authentication technologies.[86] One consequence of such legislation would be that banks and other financial institutions would be exempt from state law registration or licensing requirements.[87] This protected status would provide banks and similar institutions with "a national monopoly for electronic authentication."[88] Legislation, then, should not favor one industry over others as the national electronic authenticator because the different applications of digital signature technology may later require other appropriate institutions to serve as CAs. Third, and perhaps most importantly, legislation should explicitly authorize institutions to use digital signatures to conduct transactions or business online.[89] In the traditional business environment, handwritten signatures typically suffice for the purposes of demonstrating that a particular person has agreed to a particular set of contractual agreements. While this requirement has served businesses well in the paper-based world, it has made companies wary of engaging in business transactions online, thereby restraining the development of electronic commerce.[90]

Bennett's legislation, The Digital Signature and Electronic Authentication Law of 1998 ("SEAL"),[91] purports to fulfill most if not all of the requirements issued by hearing panelists. It is an attempt at providing a governing legal framework, which leaves room for non-financial institutions to participate in the use of digital signatures while allowing banks and other related organizations to move forward in the development and

86. *See Hearing on Electronic Authentication and Digital Signature, supra* note 18 (statement of Mr. Richard Mossburg, Associate Counsel for Government Affairs, Ford Motor Credit Company—Legal Office).

87. *See id.*

88. *Id.*

89. *See, e.g., Hearing on Electronic Authentication and Digital Signature, supra* note 75. Nugent explained during testimony that legislation should "allow financial institutions to employ electronic authentication in the conduct of their business." *Id.*

90. A number of scholars have addressed the problems posed by the Statute of Frauds in the development of digital signatures and electronic commerce generally. *See generally* Richard L. Field, *The Electronic Future of Cash: 1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 AM. U. L. REV. 967, 982 (1997); Robertson, *supra* note 40, at 797 (explaining that, despite the advantages of doing business online, "many business persons remain unwilling to conduct business electronically so long as there is substantial doubt concerning the legal validity of agreements entered into electronically.").

91. S. 1594, 105th Cong. (1998).

use of authentication technologies.[92] The bill is also technologically neutral, allowing room for the introduction of new technologies, and sensitive to the need to preserve consumers' rights under the Truth in Lending Act and the Electronic Fund Transfer Act.[93] These are substantial benefits, but it is not clear whether the bill addresses all of the major issues raised by the digital signature technology.

IV. IDEAL FEDERAL LEGISLATION

Ideal digital signature legislation would accomplish two broad and sometimes competing goals. It would encourage the development of electronic commerce by addressing the needs of companies affected by digital signatures while also protecting the privacy of consumers who engage in online transactions. SEAL meets some of these goals, but not all. If the current Congress does not pass SEAL in its current form, future digital signature legislation should consider the following issues. If Congress does pass SEAL, the remaining issues should be addressed by further legislation.

SEAL, as it is drafted, addresses several major concerns raised by industry executives.[94] First, companies would no longer need to worry about complying with conflicting state laws because the bill would create a unified federal framework for authentication methods. Second, corporate executives would have fewer concerns about credit card fraud because the bill would allow them to rely on the identity of users as provided by their digital signatures. Companies already rely on the identity of users by matching the signature on the back of a credit card to the signature consumers must write onto a credit receipt, so federal law would simply extend a commonly accepted practice to the digital environment. Third, companies would also be able to create new authentication technologies, without the fear of producing a new innovation that has no market. In other words, the bill's reach does not seem to extend only to existing technologies; new authentication methods would be as enforceable as today's methods. Technological neutrality is especially important because the government should not be in the business of influencing the market by mandating what technologies should be used. Furthermore, legislation should not mandate the use of a technology that may quickly become antiquated.

---

92. *See id.*
93. *See id.*
94. *See* S. 1594, 105th Cong. (1998).

However, SEAL does not include the consumer privacy protections that any ideal digital signature legislation should contain. Ideal legislation should protect private keys from unauthorized access by third parties, including both private citizens and law enforcement officials. Further, ideal legislation should encourage CAs to issue different digital signatures for different purposes.[95] There are at least three specific issues that ideal legislation should address.

First, ideal digital signature legislation should specify that CAs shall not release private keys to third parties except in narrow, specified circumstances. This provision should apply to both private parties and law enforcement, and would help prevent third parties from impersonating the owner of the private key. Therefore, the PKI for digital signatures should not be tied to key escrow.[96] In 1994, the Clinton Administration unveiled the Clipper Chip, a device that would encrypt data with keys the government could access from software key escrow for law enforcement purposes.[97] After that initiative failed, the Administration proposed in its 1996 White Paper that a public key infrastructure include an escrowing of private encryption keys.[98] It is foreseeable that, if the Clipper Chip effort and the White Paper are viewed as proposals to provide government with access to encrypted information, the government may similarly attempt to acquire access to keys used in digital signatures for law enforcement purposes by requiring that private keys be placed in escrow.[99] It is not clear,

---

95. For example, one digital signature could be used to make purchases with a particular credit card, another could be used to purchase or sell securities, and a third could be used to file tax documents with appropriate government agencies.

96. *See* James X. Dempsey & Alan Davidson, Center for Democracy & Technology, *Digital Signatures | Comments of the Center for Democracy and Technology to NIST* (visited Feb. 13, 1999) <http://www.cdt.org/digsig/nistcom.html>.

97. *See* A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow,"* 1996 U. CHI. LEGAL F. 15, 19 (1996).

98. *See* INFORMATION INFRASTRUCTURE TASK FORCE, THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE, 196-97 (1995) ("[T]he Working Group supports efforts to work with industry on key-escrow encryption technologies and other encryption products which could be exported without compromising U.S. intelligence gathering and law enforcement.").

99. This attempt has already been made. Indeed, Senator McCain introduced in 1997 S. 909, the Secure Public Networks Act, which would create a system of regulated Certificate Authorities and key recovery agents. This system would require a "key recovery agent, whether or not registered by the Secretary under this Act, [to] disclose recovery information to a Federal or State government entity, to permit it to achieve the lawful purposes specified in subsection (2) of this section upon the receipt of a subpoena described in subsection (4)...." S. 909, 105th Cong. § 106(3) (1997). The subsection (2) referred to in the citation describes a broad list of purposes that appears to favor govern-

though, that there is a legitimate reason why law enforcement officials should need digital signatures. Even if there were a legitimate reason, it would have to be substantial to outweigh the cost involved with the potential abuse of such keys. If a third party, even the government, had access to the keys, the possibilities for impersonation would be significant. In sum, while the encryption of data is different from the authentication of users, SEAL, or its successor, should discourage the government from acquiring access to private keys—as it has attempted to acquire access to keys for encrypted data—and, even if third parties do access the private keys, should limit the circumstances under which the keys would be made available.

Second, in addition to shielding private keys from third parties, ideal digital signature legislation should encourage, or perhaps require, CAs to issue different keys for different functions.[100] This would further protect consumer privacy by ensuring that, if a third party got unauthorized access to someone's private key, that key would be of only limited use. Such legislation probably should be aimed at CAs, not consumers, because consumers are unlikely to take the trouble to set up separate digital signature accounts on their own to avoid the accumulation of a single personal information record. If this second concern were somehow incorporated into new legislation, the new bill would also have to, as SEAL seems to do now, apply the enforceability of digital signatures to both financial as well as non-financial transactions.[101]

---

ment access to information over personal protection of privacy. As of this writing, no decision has been made about the passage of S. 909.

100. Perhaps, for example, a state agency could be allowed under federal law to serve as a CA that issued public and private keys for the sole purpose of dealing with other state agencies for tasks such as motor vehicle registration or state tax filings. A financial institution could be allowed under federal law to serve as a CA that issued keys only for commercial transactions on the Internet. A CA in the state judiciary system could be established and federally designated to issue keys for the use of state court filings. This would reduce the possibility that, for example, a commercial entity could attempt to use the digital signature to acquire more information than is necessary to complete a transaction. The concern here is that an organization would consider, in a decision, otherwise irrelevant information garnered from the digital signature or would sell the information to a third party. As a rule, digital signatures should not, for example, reveal to curious and technologically savvy employers the health records of potential employees with whom employment agreements are exchanged online.

101. Applying the enforceability to both financial and non-financial transactions is important because, if digital signature owners actually do use the technology, they should be able to do more than simply purchase goods. Users could, for example, file state documents, accept or make offers of employment, or consult with a physician over a telemedicine network.

Third, in addition to adhering to strict privacy guidelines, CAs should be required to be licensed by an appropriate government agency so that consumers will rely only on trusted third parties. The justification for this requirement is to protect consumers from entrepreneurs who decide to start a business as a CA for the sake of selling information about clients. If SEAL—or future legislation, if Congress rejects SEAL—was amended to prohibit non-licensed CAs from formation or operation, it would successfully preclude the problem of allowing entrepreneurs from accumulating private information from others.

V. CONCLUSION

Digital signature technology was developed in part to address the authentication needs of companies and consumers as they engage in transactions online. As electronic commerce develops and authentication becomes more important, consumers and companies will probably rely on digital signatures more often than they do now. While much of the present discussion about digital signatures focuses on its financial applications, the technology will likely be used eventually for both financial and non-financial transactions.

Private sector decision-makers and entrepreneurs have been quick to adapt to change in the digital environment, despite the reluctance of their public sector counterparts. Part of the reason why many Representatives and Senators have hesitated to address digital signatures, and other technology-related issues, is that technology companies have not composed a significant part of their states' economies until recently. It is also possible to argue that many policymakers are not as literate or comfortable with technology issues, and, therefore, have been reluctant to address the necessary changes until private sector lobbyists from the technology industry established a stronger presence in Washington.

Despite their late start, however, policymakers in state legislatures and the U.S. Congress have been busy in the past year drafting legislation that has had both positive and negative effects. While the recent activity of state legislatures has allowed consumers to use digital signatures for some purposes, and in that sense had a positive effect, the multiplicity of state laws has revealed a nationwide disagreement over when digital signatures should be enforceable. Congress reacted with federal legislation that would provide, among other things, a uniform framework for the use of digital signatures. While the legislation has had the positive impact of encouraging the commercial use of digital signatures, it fails to address certain issues related to consumer privacy. If SEAL is passed in its current

form, future legislation should be proposed to protect the privacy of consumers without inhibiting the development or use of digital signature technology. If SEAL fails to pass, the issue should be revisited soon after with a successor bill that more equitably addresses the needs of both companies and consumers.