ARTICLES

BROWSE-WRAPS, CLICK-WRAPS AND CYBERLAW: OUR SHRINKING (WRAP) WORLD

Michael Dessent[1]

I. INTRODUCTION

"Dear Prof. Abby:

Last week I was called by my telephone carrier who wanted to know if I would agree to contract with them for high speed internet service. After listening to their sales pitch, I said that I would. Following a series of questions about compatibility with my computer, she then asked me if she could record my voice as the "signature" of my assent. I said it was okay. Then she asked me whether I agreed to the terms, telling me that I must speak the words, "I agree." She then recorded my verbal assent! Now, I'm not sure if I want the service after all. Am I stuck?

Searchingly yours,

BROWSER-MOUSE"

"DEAR BROWSER-MOUSE: Welcome to the digital age! Not to sound cheesy, but if you aren't current with the internet, you might become road-kill on the information superhighway - so congratulations! Yes, you're contractually bound - even without signing any writing!

Professor Abby"

II. OVERVIEW OF THE PROBLEMS

Whether by a click of a button, email or thumbprint, businesses are offering unique ways to bind consumers in the world of e-commerce. Professors Arthur Corbin and Samuel Williston must be rolling over in that big law school in the sky.

Within the last year, online purchases were close to one half a billion dollars. It is estimated that by the year 2004, such sales

1. Professor of Law and Dean Emeritus, California Western School of Law; B.S. Northwestern University, 1964; J.D., cum laude, Northwestern University School of Law, 1967.

will reach $3.2 trillion.[2] The popularity of internet sales and contracts is largely due to the cost effectiveness and speed of transacting online.[3] This profound rise in electronic transactions has, predictably, called for legislation that would protect consumers against fraud, respect conflicting state and federal laws and permit a high level of security online. Possible? Let's see:

This area of the law recently was referred to as a potential "litigation nightmare."[4] Others call the new statutes lawyers' "retirement acts" for the several reasons addressed below. This paper will describe the different laws governing digital transactions, the issue of federal or state law preemption, conflicts of laws, dilemmas regarding fraud and security and where public policy burdens should fall in electronic transactions.

III. A BRIEF HISTORY OF THE RELEVANT LAWS

A. THE STATUTE OF FRAUDS

Remember one of your favorite topics in law school, the Statute of Frauds?[5] Prior to the recent adoption of the federal E-Sign Act,[6] courts could not readily accept electronic signatures or computer transactions as binding contractual events in large part because of the limitations of the Statute.[7]

For example, if there is a sale of goods, Article 2 of the Uniform Commercial Code requires "some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought for

2. Jonathan E. Stern, Note, *Federal Legislation: The Electronic Signatures in Global and National Commerce Act,* 16 BERKELEY TECH. L.J. 391 (2001).

3. Mike Watson, Note, *E-Commerce and E-Law, Is Everything E-Okay? Analysis of the Electronic Signatures in Global and National Commerce Act,* 53 BAYLOR L. REV. 803, 806 (2001).

4. P. Reed, *Consumers at Risk: A Litigation Nightmare with Electronic Signature Laws,* (October 24, 2000) *available at* http://law.about.com/library/weekly/aa102400a.htm. (Author maintains article on file.)

5. *See e.g.* U. C. C. § 2-201 (2002).

6. The Electronic Signatures in Global and Natural Commerce Act, 15 U.S.C. §§ 7001-7006 (2002).

7. *See, e.g.,* Roos v. Aloi, 487 N.Y.S.2d 637, 642-43 (Sup. Ct. 1985) (holding that an oral agreement by stockholders in a close corporation to be executed over ten years violated the one year limit in the Statute of Frauds); *see also* PMC v. Saban Entm't, 45 Cal.App.4th 579 (1996) (explaining that in a breach of contract claim, the agreement is unenforceable if it does not satisfy the requirement of a signed writing), and Phillippe v. Shappel Indus., 43 Cal.3d 1247, (Super. Ct. 1987) (holding that an oral commission agreement is invalid).

the sale of goods for $500 or more."[8] (Recent attempts to increase this minimum to $10,000 have failed.) The Statute of Frauds also would have barred electronic transactions (if it could have anticipated them) if performance of the contract would have exceeded one year from the date of making.[9]

As the popularity of online transactions grew,[10] states began to recognize the need for comprehensive and uniform laws governing electronic transmissions.[11] Additionally, the Statute of Frauds needed to be amended to allow for electronic signatures.[12]

In 1995, Utah was the first state to enact a law that regulated digital transactions.[13] This early statute was based on a technology-specific approach which gave only "digital signatures" legal enforceability.[14] By comparison, California's early law adopted a technology-neutral stance on signatures.[15]

In an effort to provide consistency among the state laws, in 1999 the National Conference of Commissioners on Uniform State Laws (NCCUSL) adopted the Uniform Electronic Transactions Act (UETA).[16] UETA basically states that an electronic signature is valid when coupled with the signer's intent to authenticate the "record."[17]

UETA deals with the validity of electronic transactions, attributes an electronic record to a person, resulting in changes and errors in transactions and requires electronic transactions to be retained in hard copy for reference.[18] UETA is technology neutral; that is, it does not specify which type of security feature or encryption will be legally binding.[19] Given the rapidly changing

8. U. C. C. § 2-201.

9. *Id.* at subsection (1).

10. Stern, *supra* note 2, at 391.

11. Adam R. Smart, Note, *E-Sign Versus State Electronic Signature Law: The Electronic Statutory Battleground,* 5 N.C. BANKING INST. 485 (2001).

12. *Id.* at 489.

13. *Id.* at 491.

14. Utah Code Ann. §§ 46-3-101 to 46-3-602 (1996).

15. Smart, *supra* note 11, at 491. *See e.g.* CAL. CIV. CODE §§ 1633.1-1633.17 (West 2000).

16. Uniform Electronic Transactions Act (UETA) (1999) *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited January 12, 2003).

17. Stern, *supra* note 2, at 394.

18. Watson, *supra* note 3, at 807.

19. *Id.*

nature of technology today, quick obsolescence is a given.[20] States sought to avoid the need for specific laws to be amended every time new technology enters the market.

Although the NCCUSL's intent in enacting the UETA was to foster uniformity in state technology laws,[21] its proposal may have had the contrary effect.[22] Many states focused their approach on consumer protection, specifically, certain minimum levels of security within electronic transactions, thus setting up barriers to businesses trying to use this new technology to increase sales.[23]

One effect of the states adopting differing versions of the UETA has created a tangled web of electronic signature laws with which both businesses and consumers have to deal.[24] Since the versatile nature of e-commerce lends itself to conducting interstate business, consumers and sellers are faced with distinguishing and complying with the various state laws.[25] Some jurisdictions favor consumer protection.[26] Others are more probusiness,[27] thus leading to forum selection clauses and the classic problems of the battle of the forms, adhesion and unconscionability issues and rolling contracts.[28]

B. E-SIGN

To eliminate some of the confusion among states, Congress passed the Electronic Signatures in Global and National Com-

20. Stern, *supra* note 2, at 406 (stating that the technology neutral approach of the UETA is justified by the fact that technology tends to be obsolete) (Critics say that the approach fosters the use of insecure procedures that make it easy for hackers to commit fraud online.)

21. Watson, *supra* note 3, at 806.

22. P. Reed, *supra* note 4.

23. Almost 40 states have adopted their form of UETA to date.

24. *Id. See also* Robert MacMillan, *Patchy State Laws Hamper E.Sign Rollout-Witnesses*, June 28, 2001, NEWSBYTES.COM. (Author maintains article on file.)

25. *Id.*

26. Va. Code Ann. § 59.1-491(b) (2000). Virginia's Code includes five extra factors to determine the evidentiary weight of an electronic signature. The factors are whether the signature is unique to the signer, capable of verification, under the signer's sole control, linked to the record in such a manner that it can be determined if any data contained in the record was changed subsequent to the electronic signature being affixed to the record, and created by a method appropriately reliable for the purpose for which the electronic signature was used.

27. CAL. CIV. CODE § 1633 (West 2002).

28. See U. C. C. § 2-207 (2000), and Hill v. Gateway 2000, Inc., 105 F.3rd 1147 (7th Cir. (Ill.), 1997).

merce Act ("E-Sign" or "The Act").[29] The policy objectives of E-Sign are to provide a nationally uniform framework in which to protect consumers and to foster the growth of e-commerce.[30] E-Sign provides that an electronic signature is not invalid simply because it is an electronic signature.[31] The Act is largely based on NCCUSL's proposal in that it does not "limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons . . . other than a requirement that contracts or other records be written, signed, or in nonelectronic form."[32]

To further this policy objective, the Act requires the retention of "accurate" records (presumably achieved through printing a hard copy).[33] If information relating to the transaction is to be provided to the consumer in writing, an electronic record will suffice as long as the consumer has "consented" to the electronic transaction.[34] For the consent to be valid, "a consumer must have read a clear and conspicuous statement relating to the consumer's choice and a confirmation of the consumer's ability to receive information electronically."[35] Clearly, the drafters of E-Sign were concerned with protecting a consumer's rights in an environment that is so susceptible to fraud.[36]

Moreover, E-Sign provides that certain topics are outside the scope of valid electronic document transactions.[37] Common sense dictates that instruments such as wills, codicils and testamentary trusts are not valid under E-Sign. Family law documents dealing with adoption and divorce also are not covered.[38] Other

29. 15 U.S.C.A. § 7001 et seq. (2002).
30. Watson, *supra* note 3, at 821.
31. 15 U.S.C.A. § 7001(a) (1).
32. *Id.* at.§ 7001(b)(1).
33. Watson, *supra* note 3, at 814.
34. 15 U.S.C.A. § 7001(c)(1)(a).
35. Recent cases have drawn a careful distinction between different types of electronic clauses. Clickwrap acceptances are being upheld where the buyer can read clear terms and affirmatively click "I accept" or "I agree." Compuserve, Inc. v. Patterson, 86 F.3rd 1447 (7th Cir. 1996), America Online, Inc. v. Booker, 781 So.2d 423 (Fla. App. 2001). However, where terms and conditions are merely posted on a website, and consent is "implied" (browsewraps), courts have refused enforcement. America Online, Inc. v. Super. Ct., 90 Cal.App.4th 1 (2001) and Groff v. A.O.L., File # P.C. 97-0331 (Rhode Island). The difference lies in the reasonableness of the negotiations, it appears.
36. Watson, *supra* note 3, at 815.
37. 15 U.S.C.A. § 7003.
38. *Id.* at § 7003(a).

exceptions include court orders, official government documents, (e.g., filing Articles of Organization for a new Limited Liability Company in California), notices of cancellation of utilities, evictions, termination of health insurance and product recalls. Likewise, security agreements and financing statements under the new Article 9 of the UCC must still be signed writings.[39]

The federal E-Sign officially allows states the option to avoid preemption by either adopting their own UETA[40] or implementing an alternative law as long as it is consistent with the provisions of E-Sign and does not require specific technology.[41] Since most electronic transactions involve interstate telecommunications, federal jurisdiction most often governs, but some contracts could be made through privately operated intrastate networks, thus necessitating a UETA. If a state chooses not to require specific technology, it must still make a specific reference to E-Sign.[42] Essentially, to be certain that no preemption will take place, a state must enact a law that is identical to UETA.[43] To date, no court has decided whether all of these modified state laws are preempted by E-Sign. As a result, companies take a risk when engaging in e-commerce in a state where the law does not comport with E-Sign.[44]

C. SECURITY UNDER E-SIGN

As defined by the E-Sign Act, an electronic signature is: "an electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[45] Further, an electronic record is "a contract or other record created, generated, sent, communicated, received, or stored by electronic means."[46]

There are several types and levels of security when signing a contract online. The National Consumer Law Center has admonished lawmakers that: "Given the current state of authenti-

39. *Id.* at § 7003(b).
40. *Id.* at § 7002(a).
41. *Id.*
42. Watson, *supra* note 3, at 819.
43. Sarah L. Roberts-Witt, *Sign of the Times,* PC MAGAZINE, April 23, 2002, at 69.
44. 15 U.S.C.A. § 7006.
45. *Id.*
46. Reed, *supra* note 4.

cation technology, it's much easier to forge or steal an e-signature than a written one."[47] But proponents of E-Sign state that "digital signatures, by their very nature, are more secure and provide a higher level of authenticity than a handwritten signature on a piece of paper ever could."[48] Since there is a difference of opinion on the relative security of digital signatures, it may be useful to discern what each level of security entails and how to attain the most secure signatures.

The simplest way to bind a consumer to a contract is by providing the terms, and then accepting the contract by clicking an "I Agree" button.[49] The next level in security is the "shared secrets"[50] method, which involves the use of passwords or credit cards to establish the consumer's intent to be bound to the contract.[51] For example, if a consumer were to buy a pair of rollerblades online, she would have to give her credit card number, thus showing that she intends to be bound to the transaction.

The third level of security is through "biometric authentication."[52] This technique recognizes a fingerprint, an iris or a voice to create a binding form of signature.[53] It requires a sample to be taken from a physiological characteristic of the consumer and stored for comparison to access that user's profile.[54] To authenticate the user, the previous profile is compared to the current user and presumably a match occurs where the identity of the consumer is verified.[55] Several corporations now deal in the biometric authentication of a consumer's signature.[56] They analyze the "shape, speed, stroke order, off-tablet motion, pen pressure and timing information" during signing.[57] Such characteristics are basically impossible to duplicate.

---

47. About.com, *Sign Here Please* (June 22,1998), *available at* http://net-security.about.com/library/weekly/aa062298.htm (last visited January 12, 2003).

48. Stern, *supra* note 2, at 395.

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.* at 396.

53. *Id.*

54. *Id.* at 395.

55. Cyber-SIGN, *The Legality of Electronic Signatures Using Cyber-Sign is Well Established*, *available at* http://www.cybersign.com/news news.htm. (Author maintains article on file.)

56. *Id.*

57. *Id.*

The most complicated security procedure is the digital signature. Before the enactment of E-Sign, some states required this high level of technology for a contract to be legally binding.[58] A digital signature consists of a private key and a public key infrastructure (PKI) which is distributed by a neutral third party, called a Certification Authority (CA).[59] When a consumer reads a contract and signs it using either a PIN, a smart card, a fingerprint reader, or a digitized signature, the consumer is issued a private key from the CA.[60] The private key is used to turn the contract, by way of a hashing algorithm, into a numerical code called a digest.[61] With that key, the digest is encrypted, and binds the consumer's digital signature.[62]

The sender's public key travels with the document. When the company receives the consumer's contract, it can be decrypted using the consumer's public key.[63] The hashing algorithm produces another digest, which is compared to the original digest. If the two digests match, then the signature has been authenticated.[64] A mismatch indicates that the document was tampered with after it was signed .[65] VeriSign,[66] Entrust Authority,[67] MobileTrust,[68] and VaCert,[69] are all companies that use PKI's and are independent CA's to vouch for an individual's identity.[70]

This technology is quite sensitive and has been verified under close scrutiny.[71] In one case, a user signed a document with a digital signature and then erased one single period from

58. Roberts-Witt, *supra* note 43, at 68.

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

64. About.com, *Sign Here Please*, *supra* note 47.

65. VeriSign Authentication and PKI Solutions, *available at* http://www.verisign.com (last visited January 12, 2003).

66. Entrust Authority, *available at* http://www.entrust.com (last visited January 12, 2003).

67. MobileTrust, *available at* http://www.certicom.com (last visited January 12, 2003).

68. ValiCert Trust Services, *available at* http://www.valicert.com (last visited January 12, 2003).

69. Roberts-Witt, *supra* note 43, at 71.

70. About.Com, *Sign Here Please*, *supra* note 47.

71. *Id.*

the document.[72] When the tester opened the document a "bad signature" message popped up.[73] The PKI can sense even the slightest change in a document that does not match up between the previous document and the current document.

Although the process does appear to be at a very high level of security, there are always computer hackers looking to breach security procedures.[74] For example, computer hackers, many of which are children (teenagers), have broken into high security systems such as Microsoft, Amazon.com, e-bay, Yahoo, the FBI, the United States Senate, the Defense Department, the White House and NASA.[75] If teenagers can break into these superior security systems, then how secure is a digital signature against this threat? The highest level of protection comes from a combination of security techniques. The strategy of using both biometric authentication and digital signatures ensures the best security one can assume from electronic transactions up to date.

D. CONFLICTS OF LAWS

One of the major problems with E-Sign is its ambiguous federal preemption section that has become "particularly problematic."[76] Legislative history revealed in the early drafts of E-Sign refers to concerns by the drafters over a "mind-numbing complexity of preemption provisions and the uncertainties that they raise with the Act's interface with . . . UETA."[77]

Since over 30 states have different laws on digital signatures, it is unclear what is subject to preemption by E-Sign, and this will remain a risk until each law is litigated. Hypothetically, each state could have a different answer on whether their law is preempted by E-Sign. One in-house counsel at a large insurance company recently stated that: "I was very excited about the E-SIGN Act when it passed. But once I worked through what was in it . . . well, just forget it."[78]

---

72. *Id.*

73. *Id.*

74. Jared Sommer, Note, *Electronic Signatures and the UETA: E-Commerce in an Insecure E-World*, 37 IDAHO L. REV. 507, 521 (2001).

75. *Id.*

76. Suzanna Sherry, *Haste Makes Waste, Congress and the Common Law in Cyberspace*, 55 VAND. L. REV. 309, 362 (2002). *See also* MacMillan, *supra* note 24.

77. MacMilan, *supra* note 24.

78. Smart, *supra* note 11, at 499.

The "consistency test" to determine whether a state law will be federally preempted by E-Sign is extremely nebulous,[79] creating the crux of the problem. It is unclear whether the preemption of E-Sign only applies to the non-conforming provisions or the entire version of the UETA. If a state law is basically modeled after the UETA, but with some additional language to protect consumers, there are three opposing interpretations that a court may utilize when determining federal preemption.[80] First, a court may find that the inconsistent non-uniform provisions are invalid, but the remaining sections would remain valid. Second, if there are any non-UETA provisions in the law, then the whole law must be checked for consistency with the E-Sign Act. Third, any non-uniform provision fails regardless of the consistency test.[81] It is impossible to tell how a court would rule when faced with a state law that does not comport to the UETA. Furthermore, no state thus far has enacted the exact version of NCCUSL's UETA.

Another problem with E-Sign is that in practice there are conflicting state laws on the subject of e-commerce. Each state has adopted its own version of the UETA, and when transacting online, it is impossible to tell in which state a consumer or business is consenting to litigation. For example, California established an electronic transactions law before the adoption of the E-Sign Act.[82]

The CA-UETA differs from the UETA in four areas. In its definition of electronic signatures, CA-UETA has more exclusions regarding its scope and adds a provision addressing standard form consent contracts, electronic records and signatures in reference to statements signed under the penalty of perjury.[83]

In comparison, New York's pre-E-Sign Act (Electronic Signatures and Records Act – SRA),[84] is a non-UETA law. ESRA's goal is to instill public confidence and to create fair technology regulation.[85] It specifies a higher standard for technology to be

79. *Id.* at 498-499.
80. *Id.* at 498.
81. CAL. CIV. CODE 1633.1-1633.17 (West 2002).
82. Smart, *supra* note 11, at 508.
83. *Id* at 509-510.
84. Mark Ustin & J. Kemp Hannon, *The New Electronic Signatures and Records Act,* N.Y.L.J., Oct. 26, 1999, at 5. The New York legislature decided to create their own model of the UETA.
85. Smart, *supra* note 11, at 516.

used in a transaction by narrowing the definition of an electronic signature.[86] Also, ESRA allows for greater consumer protection in the areas of record and consent.[87] To implement ESRA, the New York legislature also provides for the Office of Technology (OFT) to oversee and administer the Act. California and New York's version of electronic signature laws are plainly inconsistent with one another.[88] This is true of many other states, thus causing the "litigation nightmare."[89]

As a result of this uncertainty in preemption and conflicting state law, businesses and consumers are hesitant to form contracts over the Internet in other forum selection clauses.[90] In a Federal Trade Commission report published in June of 2001, "companies and individuals affected by E-Sign need to observe the law in application" before transacting in heavy e-commerce.[91] Congress' objective when enacting E-Sign was to foster growth in e-commerce, but the opposite has occurred. The ambiguous law stunts the potential consumer and business[92] by the threat of expensive litigation.[93]

E. REMEDIES

One possible cure for uncertainty in the law is to provide for an industry-wide standard regarding e-commerce.[94] Companies are eager to begin transacting online with consumers without the risk of litigation.[95] A group of financial services and e-commerce companies recently joined together to form a voluntary model Standards and Procedures for Electronic Records and Signatures (SPeRS).[96] The drafting committee is comprised of "Adobe, Dell Financial Services, Ernst & Young, Ford Motor Credit Company, FreddieMac, GE Capital Mortgage Corp., Intuit Inc.,

86. *Id.* at 516.
87. *Id.* at 517.
88. P. Reed, *supra* note 4.
89. MacMillan, *supra* note 24. *See generally* comment, Business Wire Inc., *Consumers Union Offers Tips Before You Sign Your Name on the Digital Line,* Sept. 28, 2000, *available at* NEXIS, Lexis, News Group File. (Author maintains article on file.)
90. MacMillan, *supra* note 24.
91. *Id.*
92. Roberts-Witt, *supra* note 43, at 69.
93. Roy Mark, *Council Developing Standards for Electronic Signatures,* March 19, 2002, *available at* http://www.internetnews.com/xSP/article.php/3411_994171 (last visited January 12, 2003).
94. Roberts-Witt, *supra* note 43, at 69.
95. Mark, *supra* note 93.
96. *Id.*

MassMutual Financial Group, PricewaterhouseCoopers, Wells Fargo and Zions Bank/Digital Signature Trust," to name a few companies.[97] The drafters for SPeRS are incorporating legislation from several different areas of law including the UETA and E-Sign.[98] Although the standard may not be guaranteed to hold up in court, at least companies can continue to transact with other companies on certain industry-wide assumptions, thus creating custom in the trade.

Joining the effort for clarity in e-commerce legislation, on May 1, 2002, LexisNexis™ announced a new Matthew Bender® treatise on electronic commerce and communications by Stephen Y. Chow, a principal authority on e-commerce.[99] "E-Commerce and Communications: Transactions in Digital Information" will further elucidate the law on electronic signatures and incorporate both the UETA and the Uniform Computer Information Transactions Act[100] (UCITA).[101] The treatise examines numerous topics including but not limited to identity, privacy and security, societal interests, transactions in digital information, trading on the Internet, and digital signature.[102]

IV. CONSUMER BURDENS, COMBATING FRAUD AND ALLOCATING RISK

Yet another difficulty with the UETA and E-Sign is the inadequacy of the statutes regarding the possibility of fraud in electronic signatures. Countless computer hackers are waiting to find the next new electronic security measure to breach.[103] With this Security threat always looming, legislation needs to be enacted to afford the consumer greater protection against fraud.

97. *Id.*

98. *Id.*

99. PR Newswire, May 1, 2002, *available at* LEXIS, Nexis library, PR Newswire file. (Author maintains article on file.)

100. Uniform Computer Information Transactions Act, *available at* http://www.cpsr.org/program/UCITA/ucita-fact.html [hereinafter UCITA] (last visited January 12, 2003). "UCITA is a [highly controversial] contract law statute that would apply to computer software, multimedia products, computer data and databases, online information, and other such products. It was designed to create a uniform commercial contract law for these products and calls itself "a cyberspace commercial statute." It covers contracts that are generally known as "shrink-wrap licenses."

101. *Id.*

102. PR Newswire, *supra* note 99.

103. Robert Longley, *E-Sign-Be Careful What You Ask For*, July 23, 2000, *available at* http://usgovinfo.about.com/library/weekly/aa072300a.htm (last visited January 12, 2003).

One commentator posed the question, "After a careful reading of the Digital Signatures Act, do you notice a warm-fuzzy feeling that after e-signing your e-name you will be safe from e-theft, e-fraud and e-forgery? Probable e-not."[104] He continues: "Besides premeditated, intentional criminal abuse, consider the accidental disasters that could come from e-signatures. With a click of a mouse, your kid could sell your house, or, worse yet, buy you 10,000 shares of stock in a brand new digital signature software company.[105]

As of today, the UETA and E-Sign place the burden on the consumer to prove that the fraud has occurred.[106] A major reason why the adoption of E-Sign has not catalyzed an unimpeded growth in e-commerce is that many consumers are not ready to trust digital certificates and technology online[107] without more protection.[108]

Electronic signatures are clearly in a separate category than handwritten signatures, particularly regarding attribution. It is a lot less expensive to prove that a handwritten signature is not attributed to a consumer.[109] For a consumer to prove electronic signature fraud, the consumer would have to hire a computer forensic expert to find the path of the hacker.[110] Companies now specialize in providing services including investigating fraud, offering testimony, and detecting faulty software. For a network technician to complete onsite work, the cost can approach $100/hr. (with no guarantee on how long the detection may take).[111] By comparison, handwriting analysis experts average about $85 per sample.[112]

---

104. *Id.*

105. *Id.*

106. Roberts-Witt, *supra* note 43, at 69.

107. Sommer, *supra* note 74, at 510.

108. *Id.*

109. *Id.*

110. Cybertrace Security Pricing *available at* http://www.cybertrace.com/pricing.htm (last visited January 12, 2003). Compare Rehman Technology Services, Inc. in Orlando specializes in forensic investigation for large companies. Their rates are $250/hr for computer forensics and $475/hr for expert testimony, *available at* http://www.surveil.com/rates.htm (last visited January 12, 2003).

111. *See* pricing at http://www.expertdocumentexaminer.com (last visited January 12, 2003) (price for handwriting analysis is $85) and http://www.myhandwriting.com/experts (last visited January 12, 2003) (also $85).

112. Sommer, *supra* note 74, at 509.

Consumers also have more trouble recognizing electronic fraud versus handwritten fraud.[113] A hacker could use someone's identity to buy books on Amazon.com, but the innocent consumer would not find out about this fraud until his next credit card statement is received and examined. With handwriting fraud, a consumer can usually differentiate between her own signature and someone else's forgery. Along with the innocent consumer, a jury is able to inspect a handwritten forgery visually and more readily determine whether a fraud has occurred.[114] In the case of the electronic signatures, the task for the jury is more difficult.

Handwritten signatures also have a "ceremonial psychology" surrounding the process that is lacking in electronic signatures.[115] There is a certain gravity when an individual signs a binding contract, particularly in the presence of a notary and witnesses, or with a seal of verification.[116] The signer intends to be bound by the transaction given the ritual nature of the signing. For example, when signing the E-Sign Act, the President used a smart card to sign the passing of the bill but also hand wrote a signature on the bill.[117] Regardless of whether his latter act was "just in case" or to make the bill "official," handwritten signatures show apparent intent.[118] With electronic signatures, there are usually no witnesses, no cameras and no notaries.[119] The "ceremonial" aspect of the fact that the consumer will be bound by the document is lost. With one simple click of a button, an action that any child could duplicate, the consumer may be bound, regardless of intent.

UETA states that attribution is determined by "the act of the person."[120] Section 9 continues to state what the best evidence[121] would be regarding attribution: The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to

113. *Id.*
114. *Id.*
115. *Id.*
116. Longley, *supra* at 105.
117. *Id.*
118. *Id.*
119. UETA § 9.
120. Sommer, *supra* 74, at 520.
121. UETA § 9(a).

which the electronic record or electronic signature was attributable.[122]

However, what happens is in the most common type of fraud, where a hacker assumes the victim's identity, breaks into a security system and manipulates the signature to maintain that it is attributable to the victim's identity.[123] Under UETA, if the security procedure is still intact and the signature still matches with the victim, then the signature is attributable to the victim and not the hacker.[124] Simply because a hacker abides by a security procedure does not mean that the signature is attributed to the victim.[125] In countless scenarios hackers have stolen passwords or obtained secret keys to forge the victim's signature.[126] Under UETA, the fact that the security procedure has not been breached on its face is enough to presume that the signature is attributable to the victim. In this situation the consumer faces two burdens. First, proof that a secure procedure was followed is evidence *against* the innocent consumer. Second, the consumer has the burden of proving that the signature was indeed a fraud.

Businesses are in a better position to take on the burden of proving attribution of electronic signatures because they have the ability to house more secure and reliable security systems.[127] Also, companies can set up systems to track trails left by hackers and interveners in e-commerce.[128] Businesses can allocate the risk by incorporating the costs of such tasks to the consumer. Consumers are usually willing to pay more for a product in exchange for greater consumer protection against fraud.

One suggestion is to use a third party. Certification Authorities (CA's) are companies that distribute digital signatures by offering PKI's (public key infrastructures). Since both the consumer and the business pay the CA to guarantee security, the CA should take on the burden of proving fraud once a consumer identifies it.[129] The CA is in the best position to trace a hacker because CA's already have the technology and system require-

122. Michael Lee, *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal,* 14, BERKELEY TECH. L.J. 839, 848 (1999).
123. Sommer, *supra* note 74, at 521.
124. *Id.* at 518-519.
125. Lee, *supra* note 122.
126. Sommer, *supra* note 74 at 520.
127. *Id.*
128. *Id.*
129. *Id.*

ments to trail possible hackers. It is comparatively easy for a CA to hire a few forensic experts to track fraud. CA's can allocate the risk by passing the extra cost to the consumer.[130] In addition, putting the burden on the CA will put a challenge out to any company interested in dominating the market to introduce the most secure technology there is to guarantee no breaches of security. The CA with the most secure procedures will have a great amount to gain since the demand is high for secure methods of transacting online. Putting the burden on the third party serves the goal of E-Sign because it facilitates growth in e-commerce by fostering an atmosphere of healthy competition.

V. CONCLUSION

The potential market for e-commerce and electronic signatures is virtually unlimited.[131] Companies are enthusiastic about switching to a digital age where they can eliminate paper and also reduce work time. To illustrate, Network Telephone recently decided to switch to electronic signatures to meet the growing demands of its customers. The results have far surpassed the expectations from the company.[132] GMAC Commercial Mortgage also made the switch and boasts an increase in its portfolio by $35 billion.[133] Documents that typically required weeks to complete were done in a matter of hours. The payoff for switching to electronic signatures is huge, but there is a calculated amount of risk involved.

Switching to an electronic standard is certainly achievable. Purchasing products and services online is an efficient and desirable method to transact business. Nevertheless, the law in the areas of e-commerce and electronic signatures needs to be more definitive as to consumer fraud and provide uniformity and predictability among courts. Companies and individuals should not have to fear potential litigation simply because the available statutes are broad and ambiguous. As with any other new area of law, cases will have to arise before the law will be perfected. Interested parties are hoping for sooner rather than later.

130. Lee, *supra* note 122, at 840.

131. Roberts-Witt, *supra* note 43, at 66.

132. *Id.* at 69.

133. *Id.*