Washington's Electronic Signature Act: An Anachronism in the New Millennium

Stephanie Curry
WASHINGTON’S ELECTRONIC SIGNATURE ACT: AN ANACHRONISM IN THE NEW MILLENNIUM

Stephanie Curry

Abstract: Today, electronic contracting is at the forefront of how consumers, governments, and businesses conduct their affairs. Over the last several decades, electronic contracting has taken on new forms that have raised doubts about contract formation and enforceability. In order to facilitate commerce, the federal government and forty-nine states have responded by passing legislation that gives broad legal recognition to electronic signatures. Washington State is currently the only state that has not updated its electronic signature statute to comport with modern technology and ways of doing business. As a result, Washington’s Electronic Authentication Act is likely preempted by federal law, and it presents an uncertain environment for electronic contracting. This Comment argues that Washington should join the overwhelming majority of states in adopting the Uniform Electronic Transactions Act to optimize its statutory framework for facilitating electronic contracting.

INTRODUCTION

Unique like a thumbprint, pen-and-paper signatures have historically been essential to creating binding legal documents and commercial transactions.1 Today, the forms that modern signatures take would be unrecognizable to our great-grandparents’ generation. The modern pledge may now be made by sending an email, clicking a button on a website, or using sophisticated asymmetric cryptography technology, among others.2

Congress and state legislatures have tried to keep pace with this technology in order to create parity between electronic and pen-and-paper signatures.3 Around the mid-1990s, states began adopting laws giving legal recognition to various forms of electronic signatures.4 States

1. JEREMIAH S. BUCKLEY ET AL., THE LAW OF ELECTRONIC SIGNATURES § 1:2 (2012–13 ed.) (“A signature can represent many legally significant functions in connection with a document or transaction. A signature may be used to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; and to associate that person with the content of a document.”).
2. Id. § 1:2(D).
4. Id.
like Utah and Washington only narrowly recognized “digital signatures” that followed specific security protocols to confirm a signer’s identity. Other states took a broader approach and gave legal recognition to any type of electronic signature. In response to this patchwork of state laws, the Uniform Law Commission issued a model state law in 1999, the Uniform Electronic Transactions Act (UETA), which broadly recognized all kinds of electronic signatures.

Despite the promulgation of UETA, the federal government feared that states would be slow to adopt UETA, and it sought to speed the adoption of a uniform, nationwide law. In 2000, Congress passed the Electronic Signatures in Global and National Commerce Act (ESIGN), which gives broad legal recognition to electronic signatures and governs all interstate and international electronic transactions. While ESIGN borrowed similar concepts and provisions from UETA, the two are not identical. For example, ESIGN adds heightened consumer consent requirements, but it lacks other guidelines found in UETA, such as provisions regarding attribution disputes. In light of these similarities and differences, Congress added a unique preemption provision to ESIGN: a state that enacts the official version of UETA is exempt from federal preemption under ESIGN; a state that enacts anything other than the official version of UETA is preempted to the extent that the law either conflicts with ESIGN or prefers certain technologies over others. 

7. BUCKLEY ET AL., supra note 1, § 2:4(A).
8. Id. § 2:4(B) (citing to Florida Electronic Signature Act of 1996, FLA. STAT. ANN. §§ 282.70–.75 (West 1996), renumbered as FL. STAT. ANN. §§ 668.001–.006 (West 2000)).
10. See id. § 2(8) (defining “electronic signature”).
14. Id. § 7001(a).
15. See infra Part III.A.
16. See id.
17. Wittie & Winn, supra note 3, at 297.
To date, all states have enacted UETA except for Illinois, New York, and Washington. Washington’s law was originally drafted to give legal effect to digital signatures—a subset of electronic signatures that uses specific, secure technology—and it has been amended only superficially to incorporate all types of electronic signatures. While Illinois and New York have laws that more closely mirror UETA and ESIGN respectively, Washington’s Electronic Authentication Act (WEAA) remains a relative outlier; this outlier status creates uncertainty as to whether the statute, if challenged, would survive a preemption analysis under ESIGN. Of particular concern to UETA advocates is that Washington State—home to such e-commerce pioneers as Amazon.com, Microsoft, and Expedia—trails behind all other states in its electronic signature laws. In light of these concerns, a bill was introduced in the Washington State legislature to adopt UETA in 2012, but it died in committee. As of this writing, no new legislation has been introduced on the matter.

Part I of this Comment reviews the development of electronic signatures and early state responses to modern electronic signatures. Part II reviews UETA, its approach to giving legal recognition to electronic signatures, and early state adoption of the model law. Part III outlines the federal response to electronic signatures through ESIGN and the peculiar preemption provisions contained therein. Part IV describes Washington’s electronic signature statute, the Electronic Authentication Act, and recent legislative efforts to adopt UETA. Finally, Part V argues that Washington’s Electronic Authentication Act is preempted by ESIGN. Instead of operating under the current status quo, Washington should clarify the state of the law and facilitate electronic commerce by adopting UETA.

I. THE RISE OF ELECTRONIC SIGNATURES INVITES A JUDICIAL AND LEGISLATIVE RESPONSE

Although electronic signatures have existed for many years, their use exploded with the rise of electronic contracting, creating new concerns about contract formation and enforcement. In response, states adopted varying laws to give legal recognition to e-signatures. Some of these laws favored “digital signatures,” a subset of electronic signatures that uses secure technology to verify the user’s identity and the integrity of the transaction. Other states took a more neutral approach and broadly recognized all types of electronic signatures. Still other states took an intermediate approach or simply did nothing at all.

A. Electronic Signatures Take Many Different Forms and Their Use Has Proliferated in Recent Years

Electronic signatures have existed for as long as the technology used to record them. As early as 1867, courts recognized a telegraphed signature to satisfy the Statute of Frauds. As new technologies were invented, courts followed by recognizing the legal validity of signatures communicated by telephone to an operator, via tape recordings of an oral agreement, and by facsimile.

26. See infra Part I.A; see also BUCKLEY ET AL., supra note 1, §§ 1:2(A)–(C).
27. See infra Part I.B; see also Wittie & Winn, supra note 3, at 294–96.
28. BUCKLEY ET AL., supra note 1, § 2:4(A); Wittie & Winn, supra note 3, at 295–96.
29. BUCKLEY ET AL., supra note 1, § 2:4(B); Wittie & Winn, supra note 3, at 295–96.
30. Wittie & Winn, supra note 3, at 296.
31. Trevor v. Wood, 36 N.Y. 307, 310 (1867); see also Howley v. Whipple, 48 N.H. 487, 488 (1869) (“[I]t makes no difference whether that operator writes the offer or the acceptance . . . with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by the use of the finger resting upon the pen; nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office.”). For a general account of the history of signatures, see generally CHRIS HAWKINS, A HISTORY OF SIGNATURES: FROM CAVE PAINTINGS TO ROBO-SIGNINGS (2011). For a history on the Statute of Frauds with regard to advances in technology, see Steven Domanowski, E-SIGN: Paperless Transactions in the New Millennium, 51 DEPAUL L. REV. 619, 622–36 (2001).
32. Selma Sav. Bank v. Webster Cnty. Bank, 206 S.W. 870, 874 (Ky. 1918) (holding that a contract is formed when telephone message is transmitted to telegraph operator).
Today, the use of electronic signatures in commercial transactions has exploded with the advent of computer technology. With ever-developing advances in hardware and software, the forms that an electronic signature can take are also constantly evolving. For example, in the early days of commercial computing, electronic data interchange (EDI) emerged as a means for communicating standardized forms such as purchase orders, invoices, and shipping notices between two businesses irrespective of the particular hardware or software implemented at either end of the transmission. EDI was particularly effective between businesses with an established trade relationship, as they could sign traditional paper agreements governing the exchange of electronic messages between themselves.

Another early form of computerized electronic signatures emerged in the 1970s: “digital signatures,” a kind of electronic signature that uses secure cryptographic technology known as public key infrastructure (PKI) to ensure authentication of sender identity, data integrity, and non-repudiation. Digital signatures do not look like traditional signatures and are better understood as a “signature by process to the document.” PKI technology today enables millions of consumers around the world to enter into online transactions, where, for example, a consumer logs on to a secure web site like eBay or Amazon to make a purchase. Although the underlying technology of digital signatures is beyond the scope of this Comment, it is important to understand that digital signatures—as opposed to electronic signatures generally—refer to technology that employs specific procedures and third-party entities to verify the authenticity of electronic communications.

36. HAWKINS, supra note 31, at 50–52.
38. Wittie & Winn, supra note 3, at 294.
41. Id. at 258.
digital signature technology ensures that a party contracting online, such as Amazon.com or eBay, is who they say they are, but digital signatures alone do not evidence assent to create a contract.\textsuperscript{44}

While EDI and PKI technology are important examples, they do not constitute the universe of electronic signatures. An electronic signature could be as simple as “a digitized image of paper signatures, typed notations such as ‘/s/ John Smith,’” or even an email signature block.\textsuperscript{45} As history shows, the possible forms that electronic signatures can take are limited only by the types of technologies that can record and transmit them.\textsuperscript{46}

\section*{B. State Legislatures Responded to the Rise of Electronic Transactions by Passing a Range of Electronic Signature Laws}

At common law, the form a signature takes is usually less important than the intent behind the signature to form a legally binding document.\textsuperscript{47} However, as business transactions began to move online, laws regarding fraud, contract formation, and breach of contract became less certain.\textsuperscript{48} Concerns about contract formation are particularly acute in online retail transactions where “the closest thing to a signature occurs  

\textsuperscript{44} Winn, \textit{supra} note 43, at 360–61 (“A major . . . problem lies in equating what asymmetric cryptography and [PKI] do in the online context with what a manual signature does in traditional contracting contexts. Traditional signatures play a surprisingly nuanced and complex role in traditional contracting practices that prove very difficult to map onto online security technology functions. Not all contracts require a signature to be enforceable, and not all signatures evidence a signers’ intent to enter into a binding legal relationship. To apply the term ‘signature’ to the processes performed using [PKI] is at best a metaphor and at worse [sic] simply misleading.”).


\textsuperscript{46} See \textit{supra} notes 31–42 and accompanying text; cf. UETA, \textit{supra} note 9, Prefatory Note (acknowledging the continued development of innovative technology to facilitate electronic transactions).

\textsuperscript{47} See, e.g., U.C.C, § 1-201(b)(37) (2011) (defining “signed” as “any symbol executed or adopted by a party with present intention to authenticate a writing”); see also id. cmt. (“This provision also makes it clear that, as the term ‘signed’ is used in the Uniform Commercial Code, a complete signature is not necessary. The symbol may be printed, stamped or written; it may be by initials or by thumbprint. . . . No catalog of possible situations can be complete and the court must use common sense and commercial experience in passing upon these matters. The question always is whether the symbol was executed or adopted by the party with present intention to [authenticate] the writing.”); Electronic Messaging Services Task Force, \textit{supra} note 37, at 1690-91 (stating that any symbols or codes affixed to or contained in covered records are signatures and are sufficient to verify the origin of the record).

\textsuperscript{48} Wittie & Winn, \textit{supra} note 3, at 294.
when the customer clicks a button labeled ‘I agree,’ ‘purchase now,’ or ‘buy now.’”49 Additionally, while fraudulent pen-and-paper signatures were rarely a problem in contract formation, the Internet raised new fears about how to determine the identity of a signature—was the signer the credit card holder or a hacker thousands of miles away?50

In response, early attempts at state legislation focused on giving legal recognition to digital signatures, a subset of electronic signatures. For example, Utah became the first state in 1995 to pass a law regarding electronic signatures, 51 and its stated goal was to both “facilitate commerce by means of computerized communications” and “minimize the incidence of forged digital signatures and enable the reliable authentication of computer-based information.”52 This Act, which has since been repealed, 53 required the use of “digital signatures.”54 By these terms, an electronic signature in Utah would only be at parity with a physical signature if it followed relatively complex authentication requirements,55 a substantial step away from the common law rule that the form of a signature is relatively unimportant in the eyes of the law.56 Several other states followed suit by passing legislation that also required technology-specific authentication procedures,57 including Minnesota,58 Mississippi,59 Missouri, 60 New Mexico, 61 and

50. Jay M. Zitter, Annotation, Construction and Application of Electronic Signatures in Global and National Commerce Act, 29 A.L.R. FED. 2D 519, § 2 (2008) (“[W]hile an actual signature can be proven to be that of the signer, proof of identity of the signer, and proof as to what was signed, are not as clear where an electronic or digital signature or consent is involved.”).
51. Wittie & Winn, supra note 3, at 294–95 (citing to UTAH CODE ANN. §§ 46-3-201 to -504 (1998)).
52. Utah Digital Signature Act, ch. 61, § 2, 1995 Utah Laws 284, 284 (codified as amended at UTAH CODE ANN. § 46-3-102 (West Supp. 1998) (repealed 2006)).
53. Repeal of Utah Digital Signature Act, ch. 21, 2006 Utah Laws 139.
55. See BUCKLEY ET AL., supra note 1, § 2:4(A).
56. See id. § 1:2(A).
57. Wittie & Winn, supra note 3, at 295.
Instead of following the Utah model, other states chose a "media-neutral" model that did not give preference to digital signatures. Still other states authorized electronic communications only in very specific contexts, such as "certain types of citizen-government communications." Finally, some states did nothing at all to pass electronic signature laws.

By the late 1990s, the patchwork of state laws surrounding electronic signatures posed a hurdle to the increasingly rapid expansion of electronic contracting.

II. UETA PROVIDES A FRAMEWORK TO CREATE UNIFORM ELECTRONIC SIGNATURE LAWS AMONG THE STATES

Faced with a growing patchwork of state laws, the Uniform Law Commission (ULC) decided to issue a uniform law that would provide consistency to state legislation. The ULC issued this model law, titled the Uniform Electronic Transactions Act (UETA), in July 1999.

By May 2002, forty-one states and the District of Columbia had enacted it, and it was under consideration in seven more. Of the time of this

64. Id. at 295–96 n.13 (citing Alabama Electronic Tax Return Filing Act, codified as amended at ALA. CODE §§ 40-30-1 to -6 (West 2000) (authorizing the filing of electronic tax returns)).
65. See id. at 296 n.14 (noting that Massachusetts and Michigan had not passed any electronic signature legislation as of August 2000).
writing, all but three states—New York, Illinois, and Washington—have adopted UETA.  

A. UETA Was Designed to Broadly Cover Electronic Transactions and to Create Parity with Pen-and-Paper Signatures

The stated goal of UETA is “to remove barriers to electronic commerce by validating and effectuating electronic records and signatures” so that the electronic signature or record is not “denied legal effect or enforceability solely because it is in electronic form.” UETA applies broadly to electronic records and signatures relating to consumer, business, commercial, and governmental transactions. Still, its scope is not without limits: UETA does not apply to wills, codicils, or testamentary trusts; large sections of the Uniform Commercial Code; or any other law identified by the enacting state. Additionally, UETA does not require parties to contract electronically, and it applies only to the extent that parties choose to do so. In practice, this means that UETA governs situations where a woman cancels her insurance coverage online with the click of a button, or where attorneys to a lawsuit reach a settlement agreement via an email exchange.

The effect of UETA is primarily procedural insofar as it leaves in place the substantive rules of contracts. For example, the Act defers to

---

2. See UETA, supra note 9, Prefatory Note.
3. Id. § 7(a).
4. Id. § 2(16) (defining “transaction”). Consumers are not explicitly listed in this definition, although the official comment to that section states that “[t]he term ‘transaction’ includes all interactions between people for business, commercial, including specifically consumer, or governmental purposes.” Id. § 2 cmt. 12. The comments make clear that UETA also applies between two individuals who may both qualify as consumers under other law; for example, two individuals who arrange the sale of a used car through an Internet auction site would be covered under UETA. Id.
5. Id. § 3(b).
6. See id. § 5(a).
7. Id. § 5(b).
10. See UETA, supra note 9, Prefatory Note; see also BUCKLEY ET AL., supra note 1, § 3:2 (“[UETA] recognizes the inherent flexibility and adaptability of the common law, and the wide variety of substantive statutes that already exist and will be just as applicable to electronic records as they are to written documents. For example, nothing in UETA alters UCC Article 2’s substantive rules applicable to a sale of goods.”).
state law regarding “(1) the meaning and effect of ‘sign’ . . . (2) the method and manner of displaying, transmitting and formatting information . . . (3) rules of attribution . . . and (4) the law of mistake . . . ”. These provisions ensure that electronic records and signatures mirror the treatment of hard copy records and pen-and-paper signatures under state law.

B. UETA Broadly Recognizes All Forms of Electronic Signatures

Significantly, UETA is technology-neutral in that it does not subscribe to any particular technological requirements to verify the identity of the parties and the integrity of the transaction. This approach directly contrasts with the early attempts of states like Utah and Washington to limit legal recognition to digital signatures. By defining the term “electronic” to broadly include any kind of “electrical, digital, magnetic, wireless, optical, [or] electromagnetic” technology, the UETA drafters signaled their intent to assure that the Act “will be applied broadly as new technologies develop . . . regardless of the medium used by the parties.” While most modern technologies fall within this definition, UETA also encourages courts to construe the term liberally so that the Act covers all “intangible media which are technologically capable of storing, transmitting and reproducing information in human perceivable form, but which lack the tangible aspect of paper, papyrus or stone.” By this methodology, markets and people are free to select technologies and business methods according to their needs without having to plan around legal strictures.

UETA’s definition for “electronic signatures” also helps reconceive what an electronic signature can be. While the term “signature” frequently connotes the signer’s name written in script, an electronic signature under UETA is “an electronic sound, symbol, or process

81. UETA, supra note 9, Prefatory Note.
82. See id.
83. See id. (“Nor is [UETA] a digital signature statute.”).
85. UETA, supra note 9, § 2(5).
86. Id. § 2 cmt. 4. Indeed, the drafters believed that the Act is not even limited by the term “electronic,” as UETA “is intended to apply to all records and signatures created, used and stored by any medium which permits the information to be retrieved in perceivable form.” Id.
87. Id.
89. HAWKINS, supra note 31, at 7.
attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.”90 Therefore, an electronic signature could consist of anything from a digitized picture of a handwritten signature to the process of “clicking through a series of screens to affirm intention to make an Internet purchase.”91 Under UETA, as under common law, the form the signature takes is less important than the intention to sign the record.92

C. UETA Provides Guidance for Addressing Attribution Issues

Early in the development of electronic signature laws, some state legislatures hesitated to recognize electronic signatures due to doubts about verifying the signer’s identity.93 Such concerns gave rise to Utah’s digital signature statute, which contained provisions for authenticating an electronic signature.94 In contrast, UETA’s approach is to recognize electronic signatures broadly, regardless of how verifiable they are.95 Should the validity of a signature or a record come into question, UETA allows the parties to prove the signer’s identity in “any manner, including . . . the efficacy of any security procedure . . . .”96

For example, UETA builds off of court rulings that a facsimile may be attributed to an individual by using information other than a signature, such as the letterhead or the information printed across the top of the page indicating the machine from which it was sent.97 Similarly, numerical codes, personal identification numbers, public and private key combinations, and other security procedures would all serve under UETA to establish the party to whom an electronic record should be attributed.98

In drafting UETA, the Committee deliberately declined to give legal preference to any particular security procedure.99 Instead, the strength of the security procedure affects only the weight to be accorded the

90. UETA, supra note 9, § 2(8) (emphasis added).
91. Fry, supra note 49, at 257 (internal quotation marks omitted).
92. BUCKLEY ET AL., supra note 1, § 1:2(A).
93. See supra Part I.B.
95. See UETA, supra note 9, § 2(8).
96. Id. § 9(a).
97. Id. § 9 cmt. 3.
98. Id. § 2(14) (defining “security procedure”); id. § 9 cmt. 4.
evidence as tending to establish attribution. 100 This approach creates flexibility among the parties to allow future technological development without influence from legal requirements. 101 As a result, transacting parties have the freedom “to select procedures that combine the appropriate blend of assurance with costs.” 102 To the extent that a dispute arises, any technological or contextual evidence would be admissible to prove the identification of the signing party. 103

D. All States Have Adopted UETA Except for Illinois, New York, and Washington

Adoption of UETA was fast and near-universal. 104 Within a year after UETA was finalized, eighteen states had enacted UETA, and it was under consideration in eleven more. 105 Of the states that originally passed a digital signature statute, 106 all but Washington adopted UETA by the end of 2001. 107 By 2002, forty-one states and the District of Columbia had adopted UETA. 108

Today, only Illinois, New York, and Washington have not adopted UETA. 109 However, both Illinois and New York have adopted broad definitions of “electronic signature” that parallel UETA’s definition. 110 The Illinois Electronic Commerce Security Act, 111 which was adopted in

100. UETA, supra note 9, § 9 cmt. 4.
101. Id. § 2 cmt. 11 (regarding security procedures).
102. Fry, supra note 49, at 258.
103. UETA, supra note 9, § 9; see also Fry, supra note 49, at 258.
104. BUCKLEY ET AL., supra note 1, § 3:3 (“Since the statute was only made available to the states in the latter part of 1999 and constitutes a significant departure from existing law, this is a remarkably rapid enactment rate.”).
105. Wittie & Winn, supra note 3, at 296.
106. Utah, Minnesota, Mississippi, Missouri, New Mexico, and Washington gave legal recognition only to digital signatures. Wittie & Winn, supra note 3, at 298 n.24.
107. See Duhaime, supra note 70, at 535–44.
108. Id.
110. Compare 5 ILL. COMP. STAT. 175/5-105 (defining “electronic” and “electronic signature” to include “electrical, digital, magnetic, optical, electromagnetic, or any other form . . . that entails capabilities similar to these technologies”), and N.Y. STATE TECH. LAW §§ 102(1), (2) (McKinney 2003) (defining “electronic” and “electronic signature” to mean “technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities”), with UETA, supra note 9, §§ 2(5), (8) (defining “electronic” and “electronic signature” to mean “technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities”).
1998 before the issuance of UETA, broadly recognizes “electrical, digital, magnetic, optical, [and] electromagnetic” signatures. Although Illinois has not amended its law since the passage of either UETA or ESIGN, it has adopted the Uniform Real Property Electronic Recording Act, which borrows from UETA’s definitions.

New York first passed its Electronic Signatures and Records Act in 1999, which originally defined “electronic signature” to mean “an electronic identifier, including without limitation a digital signature . . . .” In 2002, the New York legislature broadened that definition to match ESIGN’s definition of “electronic signature” to avoid a potential preemption challenge. Those amendments were introduced at the request of the New York Office for Technology, and the question of whether to adopt UETA was not then before the legislature. The reason New York still has not adopted UETA may be


114. See 765 Ill. Comp. Stat. Ann. 33/2(4) (West 2013) (defining “electronic signature” in UETA terms); id. § 33/3(a) (“If a law requires, as a condition for recording, that a document be an original, be on paper or another tangible medium, or be in writing, the requirement is satisfied by an electronic document . . . .”); id. § 33/3(b) (“If a law requires, as a condition for recording, that a document be signed, the requirement is satisfied by an electronic signature.”).


117. Act of Aug. 6, 2002, ch. 314, 2002 N.Y. Laws 3144. The New York legislature indicated that its intent was to have the state law “work in tandem” with the federal ESIGN law. Id. § 1, 2002 N.Y. Laws at 3144.

118. Letter from Sen. Kemp Hannon to James McGuire, Counsel to the Governor, dated Aug. 6, 2002, Bill Jacket, S.B. 7289, ch. 314, at 3–4. For more information on the federal law ESIGN and preemption analysis, see infra Part III.B.

attributable to an overall delay in the legislature’s adoption of uniform laws.\textsuperscript{120} For example, New York is the only state that has not enacted the 1990 revised version of UCC Articles 3 and 4.\textsuperscript{121}

III. ESIGN PROVIDES A FEDERAL FRAMEWORK FOR UNIFORM ELECTRONIC SIGNATURE LAWS

At the turn of the millennia, Congress entered the debate to promote uniformity amongst the states with regard to electronic signature laws.\textsuperscript{122} High-tech and financial services industries in particular were concerned about the length of time it would likely take the states to uniformly adopt UETA, especially in light of states making significant non-uniform amendments to UETA.\textsuperscript{123} The federal response to these concerns was the Electronic Signatures in Global and National Commerce Act (ESIGN).\textsuperscript{124}

A. Similar to UETA, ESIGN Was Designed to Give Broad Recognition to Electronic Signatures and to Facilitate Electronic Contracting

ESIGN was enacted in 2000 on the simple premise that “[a]ny requirement in law that a contract be signed or that a document be in writing can be met by an electronically signed contract or an electronic document.”\textsuperscript{125} In other words, the goal was to give “the electronic medium the same legal effect and enforceability as the medium of paper.”\textsuperscript{126} Like UETA, ESIGN does not require parties to transact in an electronic medium,\textsuperscript{127} and it is ultimately a procedural law that does not


\textsuperscript{121} Id.


\textsuperscript{123} Jeremiah S. Buckley & R. Colgate Selden, Federal Preemption Under the ESIGN Act, ELECTRONIC BANKING L. & COM. REP. (Glasser LegalWorks, Little Falls, N.J.), Feb. 2005, at 6. For one example of a state making significant, non-uniform amendments to UETA, see California’s Uniform Electronic Transactions Act, codified at CAL. CIV. CODE §§ 1633.1–.17 (West Supp. 2011) (excluding a large number of state laws from the scope of UETA).


\textsuperscript{126} Id.; see also 15 U.S.C. § 7001(a).

\textsuperscript{127} Id. § 7001(b)(2) (“[This title] does not . . . require any person to agree to use or accept
otherwise affect the rights or obligations of the contracting parties.\textsuperscript{128} The jurisdictional scope of ESIGN has broad reach, sweeping into its purview any transaction “in or affecting interstate or foreign commerce.”\textsuperscript{129} That said, ESIGN does not apply to state governments where the state itself is a party to a contract.\textsuperscript{130}

Like UETA, ESIGN also exempts certain substantive areas of laws from its ambit: adoption, divorce, or other matters of family law; laws governing the creation and execution of wills, codicils, or testamentary trusts; and most provisions of the UCC.\textsuperscript{131} Additionally, ESIGN contains consumer consent protections that limit the use of some e-records where other law requires that information be made available to consumers in writing,\textsuperscript{132} constituting one of the most substantial differences between ESIGN and UETA.\textsuperscript{133}

In language almost identical to UETA, ESIGN also defines “electronic,”\textsuperscript{134} “electronic signature,”\textsuperscript{135} and “electronic record”\textsuperscript{136} in electronic records or electronic signatures . . . .

\textsuperscript{128} Id. § 7001(b)(1) (“[This title] 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 under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form . . . .”). UETA reaches the same substantive result. UETA, supra note 9, § 3(d) (“A transaction subject to this [Act] is also subject to other applicable substantive law.”). For example, “all of the elements of a contract (such as offer, acceptance, capacity and consideration) must be present in an electronic context.” Buckley & Selden, supra note 123.

\textsuperscript{129} Pub. L. No. 106-229 (“An Act To [sic] facilitate the use of electronic records and signatures in interstate or foreign commerce.”). This Comment does not explore the outer limit of ESIGN’s jurisdictional reach, but at least one court has noted that ESIGN could potentially reach transactions that would normally be governed by state law if the transaction had an economic effect on interstate commerce. See People v. McFarlan, 744 N.Y.S.2d 287, 294 n.8 (Sup. Ct 2002) (citing Wickard v. Filburn, 317 U.S. 111 (1942)).

\textsuperscript{130} 15 U.S.C. §§ 7001(b)(2), 7002(b).

\textsuperscript{131} Id. § 7003(a).

\textsuperscript{132} Id. § 7003(b)(2) (excluding notices of cancellation of utility services; default, acceleration, repossession, foreclosure, or eviction for a primary residence of an individual; health or life insurance cancellations or benefit changes; and a product recall). “Tangible documents are required in these instances because of the importance to life, home, and safety.” Lillie, supra note 112, at 24.

\textsuperscript{133} Wittie & Winn, supra note 3, at 332.

\textsuperscript{134} 5 U.S.C. § 7006(2) (“The term ‘electronic’ means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.”).

\textsuperscript{135} Id. § 7006(5) (“The term ‘electronic signature’ means 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.”).

\textsuperscript{136} Id. § 7006(4) (“The term ‘electronic record’ means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.”).
broad, technologically neutral terms. This is not a coincidence: the ESIGN drafters followed many of the same UETA definitions to help create uniformity of laws and to advance the legislative goal of facilitating electronic transactions.

B. ESIGN's Unique Preemption Provisions Allow Some States' Laws to Preempt Federal Law

As part of its legislative goal to encourage broad recognition of electronic signatures, Congress added unique preemption provisions to ESIGN that allow states to “modify, limit or supersede [some] provisions of . . . the Act” if, and only if, certain conditions are met.

State law can supersede ESIGN if: (1) the state enacts the official version of UETA as passed by the ULC in 1999; or (2) the state’s law is consistent with ESIGN and is technologically neutral.

This unique preemption language reflects the competing legislative priorities Congress faced as it drafted ESIGN. On the one hand, Congress wanted to encourage nationwide recognition of electronic signatures and records. Federal action was seen as a necessary response to states that were slow to enact electronic signature laws, or to states that had made significant amendments to their UETA laws. On the other hand, the ULC had already spent several years drafting UETA, and many states had adopted some variation of it. If ESIGN had entirely preempted UETA just as the states were adopting it, Congress could have faced criticism for injecting federal law into an area traditionally reserved for the states. Deference to the ULC was also

---

137. Compare id. § 7006, with UETA, supra note 9, § 2. “Technological neutrality” is a term used throughout this Comment. It refers to laws that broadly recognize all kinds of electronic signatures, regardless of their form. In contrast, a law that prescribes a particular technology—such as a digital signature—is not technologically neutral. See supra Part I.B.


139. 15 U.S.C. § 7002(a) (providing for the preemption of section 7001 of that title); Buckley & Selden, supra note 123.


141. Id. § 7002(a)(2)(A)(i).

142. Id. § 7002(a)(2)(A)(ii). Additionally, if a state enacts an electronic signature law other than UETA after the passage of ESIGN, the law must make specific reference to ESIGN. Id. § 7002(a)(2)(B).

143. Buckley & Selden, supra note 123, at 4.

144. Wittie & Winn, supra note 3, at 325.

145. Id. at 296.

146. Id. at 325.

147. Buckley & Selden, supra note 123, at 4.
politically advisable as the organization has a long history of producing high-quality uniform laws for state enactment.\textsuperscript{148} Indeed, congressional deference to UETA is apparent in ESIGN insofar as ESIGN borrows heavily from UETA’s conceptual underpinnings and adopts nearly identical provisions from certain portions of the text, including sections that broadly define “electronic signatures” and “electronic records.”\textsuperscript{149}

1. ESIGN Allows the Official Version of UETA to Supersede Federal Law

Instead of outright preempting UETA, the ESIGN drafters encouraged its adoption as the national standard by allowing UETA to supersede ESIGN as long as a state adopts the official version of UETA.\textsuperscript{150} Any state modification to UETA therefore raises significant interpretive issues as to whether the modification or ESIGN governs.\textsuperscript{151} A key question of interpretation is whether ESIGN preempts only those state modifications that are inconsistent with federal law, or if the state modification means that the entire text of the state’s UETA law must undergo a preemption analysis for inconsistent provisions.\textsuperscript{152} This preemption analysis may also depend on whether (a) the state makes only stylistic changes to its UETA law; (b) the state enacts UETA but adds provisions; or (c) the state enacts UETA but omits provisions.\textsuperscript{153} Under the first category, a state’s stylistic changes, which do not otherwise affect the substance of UETA, would arguably withstand a preemption challenge.\textsuperscript{154} Similarly, if the state adopts UETA but adds

\textsuperscript{148.} Id.

\textsuperscript{149.} Id. (referring to sections 101 and 106 of UETA).

\textsuperscript{150.} Id. at 6.

\textsuperscript{151.} 146 Cong. Rec. H4353 (daily ed. June 14, 2000) available at http://www.gpo.gov/fdsys/pkg/CREC-2000-06-14/pdf/CREC-2000-06-14-pt1-PgH4346-7.pdf (“It is intended that any State that enacts or adopts UETA in its State to remove itself from Federal preemption pursuant to subsection (a)(1) shall be required to enact or adopt UETA without amendment. Any variation or derivation from the exact UETA document reported and recommended for enactment by [ULC] shall not qualify under subsection (a)(1). Instead, such efforts and any other effort may or may not be eligible under subsection (a)(2). Thus, a State that enacted a modified version of UETA would not be preempted to the extent that the enactment or adoption by a State met the conditions imposed in subsection (a)(2).”); Wittie & Winn, supra note 3, at 329–30.

\textsuperscript{152.} Wittie & Winn, supra note 3, at 329–30; see also Shea C. Meehan & D. Benjamin Beard, What Hath Congress Wrought: E-SIGN, the UETA, and the Question of Preemption, 37 Idaho L. Rev. 389, 400–05 (2001) (discussing this interpretive dilemma as applied to various state enactments of UETA).

\textsuperscript{153.} Buckley & Selden, supra note 123, at 6–7 (referring to sections 101 and 106 of UETA).

\textsuperscript{154.} Id.
provisions that do not affect the substance of UETA, those additions could be considered separate legislative enactments that do not trigger ESIGN’s preemption provisions. However, a state that significantly alters the substance of UETA, either through additions or omissions, accordingly surrenders the right to claim exemption from ESIGN and would be subject to the preemption provisions of ESIGN governing consistency and technological neutrality. This would most likely threaten UETA provisions that directly conflict with ESIGN, most notably ESIGN’s consumer consent provisions.

2. Alternatively, a State’s Electronic Signature Law Supersedes ESIGN if It Is Consistent with ESIGN and Is Technologically Neutral

If a state does not adopt the official text of UETA, a state law may still adopt alternative procedures as long as they are consistent with ESIGN and they are technologically neutral. More than ten years after the enactment of ESIGN, these unique preemption provisions remain largely untested in the courts. This lack of preemption litigation may be due, in part, to the reality that there is significant substantive overlap between ESIGN and the various state laws, and so

155. Id.

156. Id.

157. Meehan & Beard, supra note 152, at 411–12; Wittie & Winn, supra note 3, at 332.

158. 15 U.S.C. § 7002(a)(2)(A)(ii) (2006). A state law can be consistent with ESIGN in one of two ways: either the state law imposes the same substantive rule as ESIGN, or it covers a subject area that is not addressed by ESIGN. Meehan & Beard, supra note 152, at 410; Wittie & Winn, supra note 3, at 331. For example, a state may still enact an e-signature law that contains provisions that are outside the scope of ESIGN, such as provisions governing attribution of electronic signatures, the time when messages are deemed sent or received, the effect of change or error in an electronic record, and admissibility of electronic records and signatures in evidence, or the transferability of records. Id.

159. 15 U.S.C. § 7002(a)(2)(A)(ii). The legislative history regarding technological neutrality shows that Congress “intended to prevent a state from giving a leg up or impos[ing] an additional burden on one technology or technical specification that is not applicable to all others . . . .” 146 CONG. REC. S5285 (daily ed. June 16, 2000) (statement of Sen. Abraham). This provision directly implicates state laws that specify a particular technology, such as Utah’s former Digital Signature Act, which gives legal significance only to digital signatures that meet certain security procedures. Utah Digital Signature Act, UTAH CODE ANN. §§ 46-3-101 to -504 (West Supp. 1998) (repealed 2006).

160. D. Benjamin Beard, 10 Hawkland UCC Series UETA § 3.3 (“Perhaps the difficult and convoluted analyses seemingly required to determine whether a state law, including an enactment of UETA, has been preempted by E-Sign is not as significant an issue as may first have appeared . . . [I]n the vast majority of situations, there will be no difference between an outcome under E-Sign and UETA. Therefore, the question of preemption will in almost all cases be moot.”).
the preemption question can generally be avoided. Still, for parties who are interested in planning their transactions in accordance with state and federal law, it is relevant to examine whether a state’s e-signature law is in conflict with ESIGN.

IV. DESPITE THE RISE OF ESIGN AND UETA, WASHINGTON STATE HAS RETAINED ITS ELECTRONIC AUTHENTICATION ACT

Washington State was one of the first to adopt a digital signature law with the passage of the Washington Electronic Authentication Act (WEAA). A digital signature—a subset of the broader category of electronic signatures—refers to specific security protocols utilizing PKI technology. Since WEAA’s initial passage, the Washington legislature has taken several steps to modernize its law by amending WEAA to include electronic signatures, but it has not taken the further step of adopting UETA or synchronizing its law with ESIGN. Today, WEAA remains the law of Washington.

A. Washington’s Law Still Reflects Its Digital Signature Roots Despite Amendments to Incorporate Electronic Signatures

Concerned about potential fraud in electronic transactions, the Washington legislature enacted WEAA in 1996, which initially gave legal recognition only to digital signatures that met specific security procedures. In 1999, the same year that UETA was issued, Washington State amended its law to cover electronic signatures, but it left untouched many substantive provisions regarding digital signatures.

161. Id.; see also People v. McFarlan, 744 N.Y.S.2d 287, 294 (N.Y. Sup. Ct. 2002) (“Although there are clear conflicts between E Sign and [the New York statute, ESRA,] for many purposes, the same result would obtain in this case whether E-Sign or ESRA applies, and accordingly, the constitutional and preemption issues need not be reached in rendering this decision.”).
163. See supra Part I.A.
165. See infra Part IV.C.
166. See WASH. REV. CODE § 19.34.010–.903 (2012).
1. In 1996, Washington Adopted a Digital Signature Statute that Gave Preference to Certain Secure Technologies

Before UETA and ESIGN were ever on the drawing board, Washington State enacted WEAA in 1996. Its original stated purpose was fourfold: (1) to facilitate commerce by means of reliable electronic messages; (2) to minimize the incidence of forged digital signatures and fraud in electronic commerce; (3) to legally implement the import of relevant standards; and (4) to establish uniform rules with other states regarding the authentication and reliability of electronic messages.

In line with these goals, the original WEAA gave legal significance only to digital signatures that followed specific security protocols pursuant to a state-run licensing program. For example, WEAA provides rules for the secretary of state to license “certification authorities” that in turn issue a “certificate,” which contains public and private keys to confirm a subscriber’s electronic identity. In order to issue a certificate, the certification authority must confirm the accuracy of the information in the certificate by making a reasonable inquiry as to the subscriber’s identity, and it must meet technical requirements to ensure that the private and public keys correspond and are capable of creating a digital signature.

170. Id. § 102.
171. Id. § 401 (“Where a rule of law requires a signature . . . that rule is satisfied by a digital signature . . . .”) (codified at WASH. REV. CODE § 19.34.300(1)).
172. Id. § 103(10) (codified at WASH. REV. CODE § 19.34.020(11)) (defining “digital signature” as “a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer’s public key can accurately determine: (a) whether the transformation was created using the private key that corresponds to the signer’s public key; and (b) whether the initial message has been altered since the transformation was made”).
173. WASH. REV. CODE § 19.34.030.
174. Id. § 19.34.020(5) (defining “certification authority” to mean “a person who issues a certificate”).
175. Id. § 19.34.020(4) (defining “certificate” as “a computer-based record that: (a) Identifies the certification authority issuing it; (b) Names or identifies its subscriber; (c) Contains the subscriber’s public key; and (d) Is digitally signed by the certification authority issuing it”); see also id. § 19.34.020(38) (defining “subscriber” as “a person who (a) Is the subject listed in the certificate; (b) Applies for or accepts the certificate; and (c) Holds a private key that corresponds to a public key listed in that certificate”).
176. Id. § 19.34.210(1)(b), (2).
177. Id. § 19.34.210(1)(iv)–(vi); see also S. COMM. ON JUDICIARY, SENATE BILL REPORT SB 6069, S. 62-6069, Reg. Sess., at 2 (Wash. 2012) for a summation of the current law: “WEAA prescribes rules for various electronic transactions: (1) issuing certificates, which are computer-based records that identify the certification authority issuing it, names or identifies the subscriber,
2. **The 1999 Amendments Make New Provisions for Electronic Signatures**

In May 1999, the legislature amended WEAA to allow for additional technologies beyond digital signatures. First, the scope of the Act was broadened to “ensure that electronic signatures are not denied legal recognition solely because they are in electronic form.” The terms “electronic” and “electronic signature” were added, with “electronic” defined broadly as an “electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies.” “Electronic signature” was defined as “a signature in electronic form attached to or logically associated with an electronic record, including but not limited to a digital signature.”

Second, the licensing mechanism for digital signature certification authorities, described above, was re-designated as a voluntary system for private enterprises. State and local government entities, on the other hand, were still required to use digital signatures when conducting official business.

Third, the legislature designated special recognition for digital signatures by providing that presumptions of validity, reasonableness of conduct, and the limitations of liability do not apply to electronic signatures except for digital signatures created in conformance with the Act. Additionally, the legislature provided that a digitally signed message—as opposed to an electronically signed one—shall be deemed contains the subscriber’s public key, and is digitally signed by the certification authority issuing it; (2) issuing, enforcing, suspending, and revoking licenses to certification authorities, persons who are issued certificates; (3) issuing certificates to subscribers and the representations and duties that correspond with the acceptance of the certificate; and (4) satisfying signature requirements.”

179. Id. § 3, 1999 Wash. Sess. Laws at 1207 (codified as amended at WASH. REV. CODE § 19.34.010(2)).
180. Id. § 2(12), 1999 Wash. Sess. Laws at 1204 (codified as amended at WASH. REV. CODE § 19.34.020(12)).
181. Id. § 2(14), 1999 Wash. Sess. Laws at 1204 (codified as amended at WASH. REV. CODE § 19.34.020(14)).
182. Id. § 1(3), 1999 Wash. Sess. Laws at 1203; id. § 12(1), 1999 Wash. Sess. Laws at 1215 (requiring local or state governments to become subscribers to a licensed certification authority for purposes of conducting official business); see also id. § 1(4), 1999 Wash. Sess. Laws at 1203 (providing that the Act’s purpose is to establish procedures governing the use of digital signatures for official public business).
Finally, the 1999 amendments are also significant for what they did not change: the legislature declined to replace “digital signature” with “electronic signature” throughout the Electronic Authentication Act. For example, RCW 19.34.300 still provides that “where a rule of law requires a signature . . . that rule is satisfied by a digital signature . . . .” RCW 19.34.320 similarly states that “[a] message is as valid, enforceable, and effective as if it had been written on paper, if it . . . [b]ears in its entirety a digital signature . . . .” Additionally, RCW 19.34.321 still provides that “[a] person may not refuse to honor, accept, or act upon a court order, writ, or warrant upon the basis that it is electronic in form and signed with a digital signature.” Thus, the legislature broadened the stated purpose of the Act to include “electronic signatures,” but it otherwise did not change the underlying substantive commands of the Act that give legal recognition to digital signatures.

3. **The 2011 Amendments Rendered WEAA Optional for State and Local Governments**

In 2011, the state legislature responded to a request from the Washington Secretary of State’s office regarding the mandated use of digital signatures and their onerous certification requirements. Instead of requiring state and local governments to use digital signatures, the legislature amended WEAA to provide that the government “may” use digital signatures. Accordingly, Washington’s complicated digital signature schema is now an entirely voluntary system for both public and private parties.

---

186. WASH. REV. CODE § 19.34.300(1).
187. *Id.* § 19.34.320.
188. *Id.* § 19.34.321.
190. **See** WASH. REV. CODE § 19.34.300(1).
B. In 1999, the Washington State Bar Association’s Cyberspace Committee Recommended Against Adopting UETA

Although WEAA has been the law in Washington since 1996, two attempts have been made to adopt UETA. The first attempt was in 1999—several months after the passage of UETA—when the Washington State Bar Association’s Law of Commerce in Cyberspace Committee considered whether to recommend its adoption to the state legislature. At the time of its recommendation, UETA was untested: only California had adopted it, and in doing so it had made substantial amendments to the text. Believing UETA to be flawed, the Cyberspace Committee recommended against enactment of UETA because it unintentionally did more to disable electronic commerce than to enable it. In total, the Cyberspace Committee’s report identified thirteen primary problems with UETA. The Committee feared that many of UETA’s provisions were ambiguous, created additional burdens on electronic transacting, or should be cut entirely from

---

193. LAW OF COMMERCE IN CYBERSPACE COMM. BUS. LAW SECTION, WASH. ST. BAR ASS’N, Report on the Uniform Electronic Transactions Act (“UETA”) by the Law of Commerce in Cyberspace Committee (Nov. 6, 1999) [hereinafter CYBERSPACE REPORT] (on file with Washington Law Review). The Business Law Section of the Washington State Bar Association (WSBA) “established the Law of Commerce in Cyberspace Committee to address the global challenges resulting from the use of networks to conduct business transactions.” Law of Commerce in Cyberspace Committee, WSBA BUSINESS LAW, www.wabuslaw.org/CyberspaceCommittee.asp (last visited Apr. 28, 2013). The Cyberspace Committee analyzes “the increasingly complex agenda of issues emerging from the convergence of electronic commerce, infrastructure and information technologies.” Id. The 1999 Cyberspace Report cited in this section was approved by the Executive Committee of the Business Law Section of the WSBA, but it was not reviewed by the WSBA Legislative Committee or the Board of Governors, and therefore it does not represent an official position of the WSBA. Id.

194. CAL. CIV. CODE §§ 1633.1–.17 (West 2011); see also Duhaime, supra note 70, at 535; Wittie & Winn, supra note 3, at 296 n.17.

195. CYBERSPACE REPORT, supra note 193, § A(1).

196. Id. § C.

197. For example, the Committee was concerned that the definition of “electronic signature” confused the concepts of signature and consent, id. § C(1) (citing to UETA, supra note 9, § 2(8)); that the definition for “transaction” did not explicitly state whether consumer transactions were covered, id. § C(2) (citing to UETA, supra note 9, § 2(16)); and that UETA’s attribution provisions suggested, but did not clearly provide, that parties could agree on a method for proving attribution, id. § C(8) (citing to UETA, supra note 9, § 9).

198. For example, the Committee questioned whether under UETA, contracting parties would be forced to create a master trading agreement before contracting electronically, id. § C(3) (citing to UETA, supra note 9, § 5(b)), or whether UETA would require compliance with certain other provisions of law that are infeasible in an electronic context, id. § C(6) (citing to UETA, supra note 9, §§ 8(b)–(c)).
UETA. 199 The subsequent passage of ESIGN, which borrows many of its substantive provisions from UETA, renders many of these early concerns moot. 200

Although the report focuses on line-by-line concerns with UETA, 201 the underlying goals of the Cyberspace Committee reflect the stated objectives of UETA: to promote uniformity, and to treat paper and electronic transactions equally. 202 In acknowledging UETA’s goals, the Committee noted that it would undertake to review UETA again if the ULC made uniform amendments that addressed the Committee’s concerns. 203 Today, the ULC has not updated UETA, 204 and the Cyberspace Committee has not changed its official stance on UETA. 205

C. The Washington State Senate Recently Introduced a Bill to Adopt UETA

In January 2012, the Judiciary Committee of the Washington State Senate introduced a bill to adopt the official version of UETA. 206 As proposed, the draft bill sought to eliminate all other references to “digital signatures” throughout the Revised Code of Washington, 207 and it completely repealed WEAA. 208

In response to the proposed adoption of UETA, the Washington State Bar Association’s Cyberspace Committee Chair testified at a public hearing that the Committee was not ready to change its 1999 recommendation that the legislature not adopt UETA. 209 As an

199. E.g., id. § C(10) (citing to UETA, supra note 9, § 10).
200. See supra Part III.A.
201. See generally CYBERSPACE REPORT, supra note 193, § C.
202. Compare id. §§ D(1), (3) (discussing twin goals of uniformity and parity), with UETA, supra note 9, §§ 6(1), (3) (providing that the Act should facilitate electronic transactions consistent with other applicable law and in a uniform manner among the states).
203. CYBERSPACE REPORT, supra note 193, § B.
207. Id. §§ 21–27.
208. Id. § 28 (repealing all of WASH. REV. CODE § 19.34).
alternative to UETA, the Cyberspace Committee Chair suggested that the legislature pass a state version of ESIGN that would apply to governmental entities and intrastate commerce.  

Following the hearing, the Senate Committee on the Judiciary recommended the UETA bill for passage without amendment, and it proceeded to the Senate Rules Committee for a second reading before it was placed in an “X-File” in February 2012. The bill was reintroduced in both the first and second special sessions of 2012 with no further action taken by the end of the 2011–12 legislative cycle. To date, no new legislation has been proposed to adopt UETA or a state version of ESIGN.

V. WASHINGTON STATE’S ELECTRONIC AUTHENTICATION ACT IS UNCLEAR AND THE LEGISLATURE SHOULD ADOPT UETA TO REPLACE IT

Washington’s current law provides an uncertain statutory framework for parties transacting with electronic—as opposed to digital—signatures. Because WEAA is likely not technologically neutral, interstate transactions would be preempted by ESIGN. Washington should clarify this confusing area of law and encourage the growth of electronic transacting by adopting UETA, a preferable option to the alternative of adopting a state version of ESIGN.

A. WEAA Is Unclear and Outdated, and It Has Created a Murky Legal Regime for Parties Contracting Electronically

Washington’s Electronic Authentication Act is an anachronism from a technological past. Drafted in 1996, it was created before notable developments in the law of electronic signatures, including the passage

210. Id.


of UETA and ESIGN. WEAA originally created a framework for giving legal recognition to digital signatures that used a cumbersome certification process regulated by the State. That certification process proved so limiting that today it has been rendered an entirely voluntary system for both private parties and state and local governments.

Despite the voluntary nature of Washington’s digital signature certification system, the statute gives ambiguous legal effect to electronic signatures. On the one hand, the legislature amended WEAA in 1999 so that its stated goal is “[t]o ensure that electronic signatures are not denied legal recognition solely because they are in electronic form.” This would signal that the legislature wanted to give broad legal recognition to all kinds of electronic signatures. On the other hand, WEAA’s roots as a digital signature statute are still apparent. For example, “digital signature” remains a defined term that incorporates specific certification procedures, and it is not interchangeable with WEAA’s definition of “electronic signature.” WEAA still provides that “[w]here a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature . . . .” Similarly, “[a] message is as valid, enforceable, and effective as if it had been written on paper, if it . . . [b]ears in its entirety a digital signature . . . .” WEAA thus fails to give the same explicit grant of recognition to electronic signatures as it does to digital signatures, leaving an open question for the courts to determine whether WEAA actually gives legal parity to electronic and paper signatures.

This statutory conundrum is further compounded by Neuson v. Macy’s Department Stores Inc., a 2011 decision where a Washington appellate court ruled that an electronic signature was neither “the same

214. UETA, supra note 9.
216. See supra Part IV.A.1.
217. See supra Part IV.A.3.
220. Compare id. (defining “digital signature”), with id. § 19.34.020(14) (defining “electronic signature”).
221. Id. § 19.34.300(1).
222. Id. § 19.34.320.
223. See supra Part IV.A.2.
as [n]or better than a traditional signature."²²⁵ In that case, an employee’s social security number, birth date, and zip code were used to generate an electronic signature on an arbitration contract. The court found that the e-signature was not reliable because the employer had access to the employee’s identifying information.²²⁶ Because the parties in that case did not brief the court on the existence of either WEAA or ESIGN,²²⁷ the court likely did not fully consider the issue, and its ruling was arguably erroneous. Even so, this case creates more murkiness in an area of law that is already unclear. In response, the case has prompted at least one firm to publicly recommend against employers using electronic signatures in Washington.²²⁸

Out of fifty states, Washington is a true outlier in this regard. Forty-seven states have adopted UETA, which clearly recognizes electronic signatures. Illinois and New York, the only other UETA holdouts, also explicitly recognize electronic signatures in their statutes. Washington State alone has failed to provide clarity in what should otherwise be a straightforward grant of recognition to electronic signatures.

B. WEAA Is Likely Preempted by ESIGN

Regardless of how WEAA is interpreted in isolation, it must also pass a preemption analysis under ESIGN for transactions affecting or occurring in interstate commerce.²²⁹ ESIGN preempts state laws to the extent that the state law is not technologically neutral or it is inconsistent with ESIGN, unless the state has adopted the official version of UETA.²³⁰ If the language of WEAA gives legal preference to digital signatures—which it appears to do in numerous references to digital signatures at the exclusion of electronic signatures²³¹—the Act is not technologically neutral, and ESIGN is by default the law governing interstate transactions in Washington State.

Although ESIGN likely preempts WEAA for interstate transactions,

²²⁵. Id. at 796, 249 P.3d at 1058.
²²⁶. Id.
²³⁰. Id. § 7002(a).
²³¹. See supra Part V.A.
ESIGN does not apply to purely intrastate transactions or to transactions where the state or local government itself acts as a market participant. Because ESIGN does not apply to these parties, courts may return to WEAA to provide the relevant law. This could prove troublesome for parties seeking recognition of electronic signatures under WEAA: as discussed above, WEAA does not clearly protect parties that use electronic signatures other than digital signatures. Thus, for intrastate transactions or where state or local governments act as market participants, there is no certain statutory framework to support the transaction.

C. To Encourage a More Stable Contracting Environment, Washington Should Clarify Its Law and Adopt UETA

In the absence of a clear statutory framework, Washington should adopt UETA in its official form. First, adoption of UETA would bring Washington in line with forty-seven other states, thus creating a more predictable environment for facilitating electronic contracting. Because Washington’s current statute for electronic signatures is unpredictable and untested by the courts, those who seek to do business here may assign a high degree of risk to any decision that is affected by the current law. It is unfortunate that Washington, home to e-commerce behemoths like Amazon.com and Expedia, continues to facilitate an environment that is potentially risky and untested for technology-forward businesses. To this end, the question of whether UETA is a perfect law becomes irrelevant—a major benefit of the law is that it is uniform and provides a predictable framework for transacting business.

Second, UETA effectively enables electronic contracting. UETA’s broad recognition of electronic signatures and records leaves no room for confusion as to whether a particular signature merits legal

---

233. See id. §§ 7001(b)(2), 7002(b).
234. See supra Part V.A.
236. Id.
237. See Buckley & Selden, supra note 123, at 1 (“For those who are seeking to promote the electronic delivery of financial services, availability of national standards is crucial. A patchwork of inconsistent state rules for doing business electronically has the potential to hobble the use of electronic media.”).
recognition: a significant improvement on WEAA, which is potentially open to attack on this front. States that have adopted UETA have interpreted it liberally to give it effect.  

Third, early doubts about UETA have largely been answered in the ten years since it was issued. When the Washington State Bar Association’s Cyberspace Committee last evaluated UETA, it did so only months after it had been issued.  

Today, many of the Committee’s concerns have been put to rest through the development of case law and the passage of ESIGN, which incorporates many of UETA’s provisions.  

Whatever doubts may still linger about UETA should be balanced against its overall benefits. Importantly, adoption of UETA would foster uniformity of laws across state lines, and transacting parties could benefit from a growing body of nation-wide case law that may serve as persuasive authority from one jurisdiction to another. A review of case law shows that courts have been adept at interpreting UETA, and their decisions provide an additional source of law for parties to interpret their contracts.  

This development of case law—even if it may only be persuasive authority across jurisdictions—creates a richer, more fully tested transacting environment that provides an extra level of predictability to contracting parties.

D. UETA Is Preferable to a State Version of ESIGN

In response to recent legislative attempts to adopt UETA in 2012, the Washington State Bar Association’s Cyberspace Committee suggested that the legislature adopt a state version of ESIGN that would clearly

238. See, e.g., Int’l Casings Group, Inc. v. Premium Standard Farms, Inc., 358 F. Supp. 2d 863 (W.D. Mo. 2005) (allowing emails to satisfy statute of frauds requirements under UETA); Crestwood Shops v. Hilkene, 197 S.W.3d 641, 651 (Mo. Ct. App. 2006) (ruling that e-mail acceptance of offer to terminate lease was enforceable under UETA).

239. See CYBERSPACE REPORT, supra note 193.

240. For example, the Cyberspace Committee doubted whether UETA requires parties to execute a separate written agreement before contracting electronically. Id. § C(3) (discussing UETA, supra note 9, § 5). Courts have inferred that intent from the parties’ use of electronic media. See, e.g., Alliance Laundry Sys. LLC v. Thyssenkrupp Materials, 570 F. Supp. 2d 1061, 1066 n.3, 1068 (E.D. WI 2008); Hilkene, 197 S.W.3d at 651.

241. See supra Part III.A.

242. There are dozens of cases interpreting UETA. See, e.g., Waddle v. Elrod, 367 S.W.3d 217, 228 (Tenn. 2012) (holding that under UETA an attorney’s typed name on the bottom of an email satisfied the statute of frauds where the parties manifested intent to finalize settlement negotiations through electronic means); Cunningham v. Zurich Am. Ins. Co., 352 S.W.3d 519, 529 (Tex. App. 2011) (holding that UETA only applies when parties intend to sign the record using an electronic signature); Powell v. City of Newton, 703 S.E.2d 723, 728 (N.C. 2010) (same).
apply to intrastate transactions as well as to state and local governments. This solution is arguably an easy fix for replacing Washington’s current statutory schema, and it neatly avoids a complicated preemption analysis.

Although this proposal is certainly an improvement on the current state of affairs in Washington, it omits several important provisions of UETA, which is the more comprehensive statute of the two. UETA, unlike ESIGN, contains provisions relating to the attribution of electronic signatures, the time when messages are deemed to have been sent and received, mistakes in electronic contracting, or the parties’ ability to modify UETA by the terms of their agreement. For example, UETA’s attribution provisions could have provided guidance to the appellate court in Neuson, which struggled to weigh the validity of an electronic signature that had been created using the employee’s social security number, birth date, and zip code. These UETA provisions add clarity and predictability in navigating potential contract disputes because they provide default language where parties may not otherwise have contracted for those protections. By providing a more complete statutory framework, UETA better enables transacting parties to anticipate how a court will resolve potential disputes, thereby reducing the need for litigation.

Additionally, UETA contains more extensive substantive provisions to encourage the transferability of records that are notes under UCC Article 3 or documents under UCC Article 7. In comparison, ESIGN


245. UETA, supra note 9, § 9. For a helpful comparison of UETA and ESIGN, see Fry, supra note 244.

246. UETA, supra note 9, § 13.

247. Id. § 10.

248. Id. § 9 (referring to the parties’ agreement as a factor in determining the effect of an electronic record); id. § 10 (referring to the parties’ agreement to use security procedures).


250. UETA, supra note 9, § 16. The UETA Drafting Committee recognized that the law of electronic contracting could not easily apply to negotiable instruments, which are writings that
only gives legal recognition to transferable records that are notes under Article 3 relating to a loan secured by real property. At the time that UETA and ESIGN were drafted, the technology needed to support the integrity of transferable records did not exist, and the difference between UETA and ESIGN in this regard was theoretical. Today, technology has successfully developed to facilitate transferable records, making UETA’s broader provisions more suited for encouraging the transfer of electronic negotiable instruments and documents under UCC Articles 3 and 7, not just those related to real property. Washington State should adopt UETA to benefit from these significant substantive provisions.

Finally, adopting a state-version of ESIGN would impede uniformity across state lines. Washington would once again be an outlier to the forty-seven other states that have adopted UETA, and it could potentially create uncertainty for parties who are unsure of how a contract dispute may be litigated if, for example, there was a question regarding the attribution of an electronic signature or the transferability of an electronic record. To this end, uniformity can be better achieved through the adoption of UETA than through adoption of a state-version of ESIGN. Uniformity and predictability, in turn, promote the growth of electronic contracting by creating a familiar and tested legal framework for transacting business. This should be no small consideration if Washington State wants to promote its reputation as a technology and business friendly environment.

CONCLUSION

Washington’s Electronic Authentication Act is an anachronism that creates confusion for parties engaged in both intra- and interstate transactions. Instead of maintaining the current status quo, which potentially discourages the development of electronic contracting, the
Washington legislature should adopt the official version of UETA. Adopting UETA provides important statutory protections, brings Washington in line with forty-seven other states, and creates a uniform environment across state lines. It would be a worthy step towards maintaining the vibrancy of Washington’s economy.