THE DIGITAL SIGNATURE: THE NEXT STEP IN ITS EVOLUTION

*Alcolya J. L. Lester**

I. INTRODUCTION

As we approach the end of the first year of the new millenium, we see a rapid growth in the enactment and evolution of legislation regarding the use and validity of digital signatures in countries throughout the world. Digital signature legislation has been established with the purpose of giving digital signatures the same validity and effect as handwritten signatures.[1] Digital signatures are alluring to those involved in international e-commerce, because through their use, parties are able to significantly minimize the distance and physical obstacles associated with international transactions.[2] Unlike other forms of electronic signatures, a digital signature is a secure communication, which can ensure that electronic documents signed by one party and sent electronically to another are done without a compromise of security.[3] However, the differences in various laws create a problem for the use of digital signatures across national boundaries.[4] "The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure operability at a global level, agreements on multilateral rules

---

* J.D. Candidate, Class of 2002, Nova Southeastern University Shepard Broad Law Center, Fort Lauderdale, Florida.

1. *See* S. Res. 761, 106th Cong. (2000) (enacted); Council Directive 99/93 of 13 December 1999 on a Community Framework for Electronic Signatures, art. 5, 1999 O.J. (L 13) 15; *See generally* Draft guide to enactment of the UNCITRAL Uniform Rules on Electronic Signatures, U.N. UNCITRAL, 37th Sess., art. 6 (2000), *available at* http://thomas.loc.gov (last visited Sep. 13, 2000).

2. W. Everett Lupton, *The Digital Signature: Your Identity by the Numbers*, 6 RICH. J.L. & TECH. 10 (1999).

3. *Id.*

4. *Id.*

with third countries on mutual recognition of certification services could be beneficial."[5] In order for the use of digital signatures to be a success in the international forum, several barriers must be tackled. This article will focus on three barriers: 1) the conflicting technical requirements of digital signatures; 2) the ability to limit potential liability of Certificate Authorities; and 3) the conflicting legal requirements regulating digital signatures and contracts.

The creation and verification of digital signatures is done through cryptography, with the use of mathematics, which transforms messages.[6] Digital signatures generally require the use of two keys, a "private key" and a "public key."[7] The signatory uses the "private key" exclusively in the creation of the digital signature, while the "public key," which can be widely known, is used by the party relying on the signature to verify the authenticity of the digital signature.[8] The private key is the tool used by the signatory to encrypt the text of the document.[9] Then, the recipient of the document uses the public key to decrypt and verify the authenticity of the document.[10] The encrypting and decrypting of the document occurs through a mathematical relationship between the two keys, which makes it "computationally infeasible to deduce the private key solely from knowledge of the public key."[11]

Another process used in the creation and verification of a digital signature is a hash function. "A hash function is an algorithm which creates a digital representation or 'fingerprint' in the form of a 'hash value' or 'hash result' of a standard length which is usually much smaller than the message but nevertheless substantially unique to it."[12] This process creates a digest, which is a string of characters that maps the text.[13] This ensures that if any portion of the original message is changed, the digest will also be changed.[14] These keys

---

5. Council Directive 99/93 of 13 December 1999 on a Community Framework for Electronic Signatures, art. 23, 1999 O.J. (L 13) 13 [hereinafter Electronic Sign].

6. American Bar Association, *Digital Signature Guidelines Tutorial, at* http://www.abanet.org/scitech/ec /isc/dsg-tutorial.html (last visited Sep. 4, 2000).

7. *Id.*

8. *Draft Guide to Enactment of the UNCITRAL Uniform Rules on Electronic Signatures*, U.N. UNCITRAL, 37th Sess. (2000). [hereinafter *Draft Guide*].

9. Sanu K. Thomas, *The Protection and Promotion of E-Commerce: Should There be a Global Regulatory Scheme for Digital Signatures?*, 22 FORDHAM INT'L L.J. 1002, 1013 (1999), *relying on* R.R. Jueneman & R.J. Robertson Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 JURIMETRICS J. 427 n.26 (1998).

10. *Id., relying on* Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1219 (1998).

11. *Id., relying on* R.R. Jueneman & R.J. Robertson Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 JURIMETRICS J. 427 n.26 (1998).

12. American Bar Association, *supra* note 6.

13. Lupton, *supra* note 2.

14. *Id.*

are issued by a trusted third party, generally referred to as a Certification Authority.[15] Digital signatures can be described as the use of cryptography and a hash function to transform a message.[16] Whoever is in possession of the initial message and the public key of the signer can accurately verify that the transformation was done through the use of the private key of the signer, and whether the original message has in any way been altered.[17] A digital signature is not a handwritten signature electronically stored; it is a secure communication used to verify a signatory.[18]

II. CONFLICTING TECHNICAL REQUIREMENTS OF DIGITAL SIGNATURES

Digital signature laws provide for different technological requirements in various areas of the world. Legislation has been enacted in several jurisdictions, which either recognizes or regulates the use of digital signatures.[19] However, the approach taken regarding the legal and technical issues has been significantly different in each jurisdiction.[20] While some countries focus on only the technical standards, others have touched on a wide variety of issues, including the establishment of a regulatory agency whose function is to oversee Certificate Authorities.[21] Different jurisdictions have set up different requirements for a Certification Authority. For example, Singapore has a Controller of Certification Authorities whose responsibilities include licensing, certifying, monitoring, and overseeing certification.[22] However, the Singapore law does not require that all Certification Authorities be licensed; it simply provides for a greater assumption of validity and limitation on liability.[23] In contrast, a valid digital signature in Italy must be certified by a Certification Authority that has been accredited through the fulfillment of specific conditions set by the law.[24] Additionally, the European Union encourages Certificate Authorities to include in their certificates the name, address, social-security

---

15. Draft Guide, *supra* note 8.

16. Lupton, *supra* note 2 (defining digital signatures and explaining the procedures associated with the issuance and usage of digital signatures).

17. *Id.*

18. *Id.*

19. Thomas, *supra* note 9, at 1026.

20. *Id.*

21. Internet Law & Policy Forum, *Survey of International Electronic and Digital Signature Initiatives.*, *at* http://ilpf.org/digsig/survey.htm (last visited Sep. 13, 2000) [hereinafter *Digital Signature*].

22. 1998 Singapore Electronic Transactions Act, June 29, 1998, *available at* http://mbc.com/eommerce/legis/sigapore.html.

23. *Id.*

24. Interdisciplinary centre for Law & Information Technology, *The Legal Aspects of Digital Signatures*, *at* http://www.law.kuleuven.ac.be/icri/projects/report.data/executive.htm, (last visited July 25, 2000).

number, tax and credit information, and specific licenses and certifications.[25] The European Union's goal is to have the Certificate Authorities offer a wider variety of services.[26]

With so many different variations of requirements for Certification Authorities, it will be difficult to conduct international transactions through the use of digital signatures. In order to be successful across international borders, Certification Authorities will be required to fulfill the requirements set forth by every area in which it will conduct its business. For a Certification Authority to be successful internationally, it would quite possibly have to acquire licenses in several jurisdictions, a task that would prove to be expensive.[27] The costly price of acquiring licenses in different jurisdictions would be shifted to the consumers of the Certificate Authority. This would discourage the use of digital signatures on the international level, and quite possibly stifle growth and progression. Due to the varying conditions of licensing, becoming licensed in different jurisdictions could be virtually impossible. Additionally, some laws regarding the requirements for Certification Authorities are unclear, making the task more difficult.[28] A harmonization of the licensing requirements of Certification Authorities must come about in order to secure a future for international digital signatures.

III. THE ABILITY TO LIMIT LIABILITY OF CERTIFICATION AUTHORITIES

Anyone can download digital signature Software on the Internet and create a digital signature.[29] For this reason, any message using a digital signature should be authenticated by a Certification Authority to minimize the occurrence of fraud.[30] It is the duty of the Certification Authority to ensure the identity of the user, and verify that both the public key and private key used belong to that individual.[31] The Certificate Authority will then issue a certificate, which gives the digital signature a presumption of validity.[32] Upon issuance of a certificate, the Certificate Authority could possibly be held liable for negligence in performing its functions by providing certificates that contain false or misleading information, and breach of contract.[33]

---

25. Lupton, *supra* note 2, *relying on* European Commission, European Parliament and Council Directive On a Common Framework for Electronic Signatures, Explanatory Memorandum, at I, *available at* http://www.ispo.cec.be/eif/policy/com98297.html (last visited Oct. 14, 1999).

26. *Id.*

27. *Digital Signature, supra* note 21.

28. *Id.*

29. Lupton, *supra* note 2.

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.*

The next barrier to the international progression of digital signatures is the ability of Certification Authorities to limit their liability. A Certification Authority is subject to strict liability for failure to follow issuance requirements and for losses caused by reliance on an inaccurate certificate under the European Union Directive.[34] However, the European Union allows a Certification Authority to limit its liability.[35] The European Union Directive allows Certification Authorities to limit their liability by indicating the beginning and end period of a valid certificate, limiting the scope and use of a certificate, and the value of transactions in which the certificate can be used.[36]

Other areas, such as Singapore and Malaysia, require that a Certification Authority be licensed in order to place a limitation on its liability for the certificates it issues.[37] The major problem with this requirement is whether being licensed or accredited should be a prerequisite for Certification Authorities to place a limit on their liability. While some jurisdictions require licensing and some do not, several jurisdictions have not addressed the issue of liability at all.[38] Some assert that addressing the issue at this stage is premature, while others are simply opposed to the idea of a system based on strict liability, which permits Certification Authorities to state limitations on liability.[39]

With so many conflicting views on how and when a Certificate Authority can limit its liability, difficulties will arise for Certificate Authorities and users of digital signatures. With these conflicting views and laws, Certificate Authorities will be hesitant to converge into the spectrum of cross-border transactions. For example, there could be instances in which one jurisdiction requires that a Certificate Authority complete a step that another jurisdiction prohibits.[40] In an instance such as this, there is no easy solution to this problem, but only the creation of more complexities. The conflicting laws in the various jurisdictions would expose Certificate Authorities to possible unlimited liability. With the uncertainty of liability exposure, Certificate Authorities would be unable to determine how much liability they would accrue when they become involved in cross-border transactions.

---

34. *Digital Signature*, *supra* note 21.
35. *Id.*
36. Electronic Signatures, *supra* note 5, at 18.
37. *Digital Signature*, *supra* note 21.
38. *Id.*
39. *Id.*
40. Raymond T. Nimmer, *International Information Transactions: An Essay on Law in an Information Society*, 26 BROOKLYN J. INT'L L. 5, 20 (2000).

IV. THE CONFLICTING LEGAL REQUIREMENTS RELATING TO DIGITAL SIGNATURES AND CONTRACTS

In almost every jurisdiction, legislatures are enacting laws regarding the use and regulation of digital signatures. The enactment of these laws will lead to confusion and complications in the use of digital signatures at the international level. Supporters of the enactment of international regulations for digital signatures assert that such regulations will provide certainty and guidance, thus promoting e-commerce and eliminating conflicting laws.[41] In contrast, opponents argue that the enactment of such laws would bring about burdensome regulations that would inhibit e-commerce transactions.[42]

The main purpose of digital signature legislation is to give equal legal effect to digital signatures as to handwritten signatures.[43] The ability to bind parties to contracts and agreements online in much the same way as handwritten signatures is the greatest strength of the digital signature.[44] The differences among the laws of different jurisdictions pose a problem for use and acceptance of the technology at the international level.[45] Some jurisdictions have laws, either enacted or proposed, which require that the states be significantly involved in the regulation of digital signatures.[46] Other jurisdictions have enacted more lenient, flexible standards.[47] Although some jurisdictions may have similar laws enacted, the manner in which the courts interpret and apply those laws could be significantly inconsistent.[48] Additionally, the absence of regulations in other jurisdictions also poses a problem. The jurisdiction of the courts and revenue, regulatory, and government authorities of a country are usually confined to the physical boundaries of that country.[49] Currently, it is not clear when one country has the authority to assert jurisdiction over an Internet user located in another country.[50] The use of digital signatures and the Internet dispel the idea that the jurisdiction of a country stops at the country's borders because they allow people to interact with one another while in

---

41. Thomas, *supra* note 9, at 1044, *relying on* Ira H. Parker, *Why Digital Signatrues Matter*, 1 ELEC. BANKINGL. & COM. REP. Z (1997).

42. *Id.*

43. *Supra* note 1.

44. Kalama M. Lui-Kwan, *Digital signatures: Recent Developments in Digital Signature Legislation and Electronic Commerce*, 14 BERKELEY TECH. L.J. 463, 468 (1999).

45. *See id.*

46. Thomas, *supra* note 9, at 1006, *relying on* Kimberly B. Kiefer, *Developments Abroad May Influence U.S. Policy on Electronic Banking*, 17 No. 4 BANKING POL'Y REP. 1, 8 (1998).

47. *Id.*

48. *Id.* at 1007.

49. Peter Steyn, Tech Werks (Technology Law News) *available at* http://www.mbendi.co.za/werksmns/techwks3.htm (last updated Jul. 21, 1998).

50. *Id.*

different countries.[51] This poses the question: how does one determine what laws guide international transactions over the Internet?

Generally, the location of a transaction, location of performance, and the location of an effect are used to determine what law applies to international transactions.[52] However, these elements are virtually irrelevant because of the fact that physical location in e-commerce has minute importance.[53] It is presently unclear exactly how to determine what laws the user will be subjected to when conducting transactions over the Internet through the use of digital signatures. For example, in Taiwan, the law provides that in the case of Internet transactions, the laws of the country in which the offer of a contract originated should govern the contract.[54] However, it is not always clear when an offer is made, and who actually made the offer. Additionally, the law in Taiwan grants only limited recognition to acts of persons twenty-years and younger.[55] This is different from the United States, in which the age of majority is eighteen-years of age. These differences create a problem for not only a Certification Authority, but also for anyone in an area outside of Taiwan, in which the age of majority is less than twenty-years old.

First, a Certification Authority would be required to know all of the laws of majority in every jurisdiction in which it wishes to conduct business. This is not only time consuming, but also quite costly. Second, suppose a citizen of the United States accepts an offer through the use of a digital signature from a nineteen-year-old in Taiwan. The law of Taiwan requires the nineteen-year-old to have a legal representative act for him or her, or else the contract is unenforceable.[56] In this situation, where the offer originated in Taiwan, the law of Taiwan would be binding on the contract. Thus, the contract will be unenforceable and the Certificate Authority would not be liable because, in this situation, the Certificate Authority only issued a digital signature to the United States citizen, and would not be responsible for the inability of the nineteen-year old to fulfill the terms of the contract. Suppose that the legal representative of the nineteen-year old acquired a digital signature for the nineteen-year old, but did not act on behalf of him or her or approve the contract. The problem is that the digital signature was acquired from the Certificate Authority and issued by them rightfully to the legal representative. However, the minor used it without the approval of the representative. Who would be liable in this

51. Lui-Kwan, *supra* note 44, at 468.

52. Nimmer, *supra* note 40, at 19.

53. *Id.*

54. George C.C. Chen, *A Cyberspace Perspective on Governance, Standards, and Control: Electronic Commerce on the Internet: Legal Developments in Taiwan*, 16 J. MARSHALL J. COMPUTER & INFO. L. 77, 89 (1997).

55. *Id.* at 82.

56. *Id.*

instance? There is no clear answer to this question. It appears that to some extent, the Certificate Authority could be held liable. However, one way in which the Certificate Authority could limit its liability in this instance is to provide a limitation on the use of the digital signature. The limitation could contain a notice that the representative must first approve the use of the digital signature. This would put the other party on notice that the nineteen-year old is not able to act on his or her own.

These variations of laws in different jurisdictions will cause a reluctance to use digital signatures in the formation of contracts on an international level. One possible solution to this problem is through a choice of law clause in the agreement. If the parties can select the law that will govern their agreement, and be confident that the courts will uphold their choice, the transaction costs will decline.[57] For example, if a Certificate Authority can include a choice of law provision stating that it will abide by the rules of the United States, this could eliminate the need to know the laws of all of the other jurisdictions in which its certificates will be used. Although a choice of law provision can be a tool to limit liability, this does not solve the Certificate Authority's problem of fulfilling all the requirements necessary to issue a valid certificate in the different jurisdictions.

Although one can acquire some protection by specifying which country's law will govern the contract, a country may still assume jurisdiction when the interests of a citizen or the country are affected.[58] One instance is the mandatory rule of the Uniform Commercial Code (UCC), which states that the laws of the country in which an online merchant is established will regulate the online merchant.[59] Some jurisdictions have rules that are mandatory and can not be contracted around through the use of a choice of law provision.[60] In contrast, under European laws, those engaged in commercial transactions are allowed to agree to what laws will govern their contract.[61] However, in Europe, choice of law clauses in consumer agreements are invalid and the law of the consumer's residence or the place of the transaction will govern these agreements. Although there is the possibility of using a choice of law clause, it is still necessary to have some grasp of the laws in the jurisdiction in which agreements are made. It is important to know if there are any laws or rules that cannot be circumvented through the use of choice of law provisions.

---

57. Maureen A. O'Rourke, *Progressing Towards a Uniform Commercial Code for Electronic Commerce or Racing Towards Nonuniformity?*, 14 BERKELEY TECH. L.J. 635, 654 (1999).

58. Steyn, *supra* note 49.

59. O'Rourke, *supra* note 57, at 654, *relying on* Mathew S. Yeo & Marco Berliri, *Conflict Looms Over Choice of Law in Internet Transactions*, ELECTRONIC COM. & L. Rep. (BNA) No. 4, at 87 (1999).

60. *Id.*, (*quoting* U.C.C. 2B-107(a) (Dec. 1998 Draft).

61. Nimmer, *supra* note 40, at 22.

In the face of conflicting laws governing to the use digital signatures, the various jurisdictions should recognize and enforce the choice of law provisions of an electronic transaction.[62] The only instance in which a government should be reluctant to, or refuse to not enforce such an agreement is to prevent abuses or to protect public policy.[63] However, absent these instances, a choice of law provision designating that a particular state should govern the contract should be recognized and enforced.[64]

It is clear that there is a need for international harmonization of the laws and rules that govern the use digital signatures. However, the lack of consensus regarding the various elements of the rules and requirements of digital signatures will prove to be a significant obstacle in the creation of international standards.[65] There are various suggestions for ways to go about creating uniform legislation for the use of digital signatures in cyberspace. The ideal digital signature legislation would encourage the development of electronic commerce by addressing the needs of companies, as well as protecting the privacy of consumers who engage in online transactions.[66]

The United Nations has agreed that the uniform rules of digital signatures should deal with the issues of 1) the legal basis of the certification process; 2) applicability of the certification process; 3) how risks and liabilities should be allocated among users, providers and third parties; 4) use of registries for certification; and 5) incorporation.[67]

With these issues in mind, the United Nations Commission on International Trade Law Working Group on Electronic Commerce (UNCITRAL) drafted the UNCITRAL Uniform Rules on Electronic Signatures.[68] Although the work of UNCITRAL has proven to be extremely beneficial when drafting national digital signature legislation, governments are not obligated to follow UNCITRAL.[69] The UNCITRAL rules could possibly evolve into the basis for international harmonization for the use of digital signatures. However, these rules, if enacted, would only be enforceable on its signatories. It is highly unlikely that all jurisdictions will be signatories to these rules. Because digital signature legislation is such a new area, it is possible that it may take some time and persuasion for countries to be comfortable enough to agree to the legislation set up by UNCITRAL.

---

62. *Id.* at 21.
63. *Id.*
64. *Id.*
65. Digital Signature, *supra* note 21.
66. LuiKwan, *supra* note 44, at 477.
67. *Supra* note 8, *Relying on* Official Records of the General Assembly, 50th Sess., Supp. no. 17 (A/51/17), paras. 380-383.
68. *See generally id.*
69. Digital Signature, *supra* note 21.

Another approach to legislation is the "admiral" approach.[70] "The Internet can be analogized to the high seas: 'Just as the territory a ship traverses is not subject to any one state's exclusive jurisdiction, so too the user in cyberspace traverses a sovereignless region that is not subject to any state's exclusive jurisdiction."[71] Following this approach, the location of the physical jurisdiction of the access provider would decide choice of law on the Internet.[72] Unfortunately, this is not helpful if the parties have different service providers.[73] The physical jurisdiction in which the Certificate Authority is located could govern the contract. By following this approach, not only would the governing jurisdiction be clear, but the transaction costs could be reduced.

For example, suppose a citizen of the United States wanted to contract with a citizen of Italy. Both parties obtain a digital signature for this transaction from a Certificate Authority in European Union. There are clearly three different nations involved in this example. By using the "admiralty" approach, the jurisdiction of the Certificate Authority would govern the contract.[74] There are several advantages to this way of deciding what jurisdiction will govern. First, the Certificate Authority would only be required to know the laws of the jurisdiction in which it is physically located. This eliminates the cost of the Certificate Authority to know the laws of every jurisdiction in which it has customers. By cutting the cost to the Certificate Authority, the costs to the consumer are also reduced. Second, the consumers will clearly know what jurisdiction will govern. This gives the consumer the option of finding a Certificate Authority in the jurisdiction in which they want the terms of the contract to govern. Last, the rules that govern the agreement can be easily ascertained. The Certificate Authority should be able to provide the users of its digital signatures with the terms, conditions, and prevalent law pertaining to their transaction. This provides an ease of acquiring information regarding the rules of the jurisdiction in which the Certificate Authority is located.

Unfortunately, this approach has its flaws. A problem would arise if the parties chose to use different Certificate Authorities located in different jurisdictions; there would be no clear way to determine jurisdiction. Additionally, it is likely that there will be some Certificate Authorities physically located in more than one jurisdiction. The Certificate Authority could have several physical locations, several principal places of business, and could be incorporated in different jurisdictions. Although this would not create a major problem

---

70. Henrique de Azevedo Ferreira Franca, *Legal Aspects of Internet Securities Transactions*, 5 B.U. J. SCI. & TECH. L. 4, (1999).

71. *Id.*, quoting Matthew R. Burnstein, Note, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT'L L. 75, 78 n.6. (1999).

72. *Id.*

73. *Id.*

74. *See generally id.*

for the Certificate Authority, it could cause some confusion for those consumers that utilized its digital signatures.

Perhaps the only solution to this dilemma is the enactment of a globally recognized scheme for digital signatures.[75] Such a scheme could supplant conflicting rules and provide legislation for areas where none exist.[76] Adequate clarity and guidance for the use of digital signatures is needed to promote growth in international e-commerce transactions.[77] Ideal international legislation for digital signatures would provide uniform rules and encourage the development of e-commerce. Any legislation related to digital signatures must consider that barriers such as border patrols, customs, and oceans are almost eliminated through electronic commerce.[78] The European Union has suggested that the legislation for digital signatures should have technology-neutral standards.[79] In order to allow the movement of goods and services through e-commerce transactions, conflicting laws regarding digital signatures must be eliminated.[80] The conflicting laws bring about uncertainty, risk, and an inability to comply with the rules, not to mention significant costs.[81] The need to reduce these costs and provide a harmonization of the laws is what drives the crusade for uniform international laws.[82]

Despite the conflicting laws, some critics argue that the establishment of uniform international rules regarding digital signatures would not be beneficial. These critics argue that it would only lead to unnecessary governmental regulations that would restrict the use of digital signatures.[83] Further, the critics believe that the implementation of such regulations would only stifle the development and expansion of e-commerce, and that e-commerce should develop naturally.[84] Additionally, they contend that legislation on digital signatures could possibly distort an infant industry, lock in business models that are harmful to consumers and hamper further e-commerce developments.[85]

Critics to uniform digital signature legislation also address the issue of liability to Certificate Authorities and their consumers. They believe that prior to the implementation of additional legislation regarding liability, there must be

---

75. *See generally* Thomas, *supra* note 9, (discussing the need for a global regulatory scheme).

76. Nimmer, *supra* note 40, at 21.

77. *Id.*

78. Lupton, *supra* note 2.

79. *Id.*

80. *See id.*

81. Nimmer, *supra* note 40, at 20.

82. *Id.*

83. *See* Thomas, *supra* note 9, at 1007 (discussing the objections raised by those opposed to the enactment of a global legal framework for the use of digital signatures).

84. *Id.* at 1053.

85. *Id.*

an understanding of the risks and implications associated with the use of digital signatures.[86] The critics go on to argue that currently, legislation shifts the risk to the users while protecting the Certification Authorities, which they feel harms not only the users, but will harm the developers eventually.[87]

The main concern of the critics to uniform digital signature legislation appears to be the possibility of over regulation. This concern rests on the fact that at this point, policy makers lack knowledge about the technology and its possible uses because it is such a new area.[88] Additionally, critics argue that the enactment of internationally recognized regulations will be difficult because there may be conflicts between the local and state laws, and the proposed international laws.[89] While this is a strong argument, it could also be an argument in support of the enactment of international regulations, since there are so many different laws which often conflict with one another. This creates problems for both the Certificate Authority and their consumers. Another problem with international legislation is that it generally takes years to negotiate, draft, and pass.[90] Although these arguments focus on some important points, it is clear that there is a need for international legislation of digital signatures.

V. CONCLUSION

Digital signatures can either prove to be the necessary tool required to help stimulate the growth of e-commerce, or it can be the beginning of the end of e-commerce. So far, it appears as if digital signatures are contributing to the growth and progression of e-commerce by providing a way in which parties can securely form contracts on the Internet. The new legislation, in most areas of the world, which gives digital signatures the same legal effect and recognition as traditional hand-written signatures is another contribution.

Unfortunately, with these great advances in technology comes the problems associated with the uncertainty of an area in which there is no legal authority. Consequently, different jurisdictions are approaching the issue in completely different ways. Laws enacted by the different jurisdictions are totally different from each other, creating much conflict. These conflicts have led to different views about what approach should be taken to resolve them. The conflicts surrounding digital signatures range from how to create a set of uniform laws to regulate and guide the use of digital signatures on the

86. *Id.* at 1055.

87. *Id.*

88. Thomas, *supra* note 9, at 1058, *relying on* Robert G. Ballen & Thomas A. Fox, *Electronic Banking Products and Services: The New Legal Issues*, 115 Banking L.J. 334, 343 (1998).

89. *Id.*

90. *Id.*

international level, to the way in which Certificate Authorities should be allowed to limit their liability.

To resolve these conflicts, the issue becomes whether there should be an international global scheme regulating digital signatures.[91] While there are those opposed to the enactment of international regulations, without it, more problems will arise.[92] There is a need for standard rules regarding the administration and regulation of Certificate Authorities. Without standards rules for Certificate Authorities, the laws of the different jurisdictions will continue to clash, and cause the transaction costs of using digital signatures to rise. The conflicting laws not only create additional costs for the Certificate Authorities; but inevitably create additional cost for the consumers.

Additionally, there is the problem with the overall conflict regarding digital signatures. As previously mentioned, there are several laws in effect in different jurisdictions which lay the groundwork for digital signatures and e-commerce. However, these laws tend to conflict with one another. In order for a party to contract through the use of e-commerce, it is necessary to know the laws of the country and state in which the other party is located. Although the parties can provide for a choice of law clause in the contract, there are certain areas in which these clauses have no legal effect.[93] Thus, a party can become subject to the laws of another country or state. These situations have the potential to discourage international use of digital signatures and e-commerce. While opponents of an international regulation of digital signatures propose that it will stifle the development and growth of e-commerce, it is obvious that uncertainty about what laws govern tremendously limits the expansion of e-commerce.[94]

Clearly, the task of developing and enacting global legislation for digital signatures will take time. However, it is a task that should be undertaken in order to promote e-commerce's continued growth. The ease of contracting through the use of digital signatures could lead to a huge expansion in international trade. Thus, steps must be taken to ensure that consumers can be certain of their rights and the consequences of their actions when contracting internationally through e-commerce. Digital signature could be the tool used to promote the use of e-commerce and international trading to the next level. But in order for digital signatures to be a successful it must be is clear which laws govern these types of transactions. The obvious solution is the implementation of a universal set of general standards which establish the roles and

---

91. *See generally id.*

92. *Id.*

93. *See generally* Nimmer, *supra* note 40.

94. *See generally* Thomas, *supra* note 9 (discussing the arguments supporting and against a global scheme for digital signatures).

liabilities of a Certificate Authority, states clearly the terms and conditions of the use of digital signatures, and the liability to consumers. Without an international agreement laying the groundwork for digital signatures, the various laws in different jurisdictions will further confusion and frustration with this technology. If this continues, the progression of e-commerce and the use of digital signatures will come to an abrupt halt.

One proposal is the continuation of the development of the UNCITRAL Uniform Rules on Electronic Signature.[95] This will allow the different jurisdictions to help in the creation of a set of international uniform rules. However, the rules must be drafted in a way that will influence the acceptance of nations. Another proposal is to utilize the framework of rules established by particular countries, such as the European Union Directive or the Electronic Signatures in Global and National Commerce Act enacted in the United States.[96] Following this type of legal framework will provide a general set of rules that will inform parties of their rights and responsibilities. At the same time, it would still allow individual jurisdictions the ability to create and maintain their own specific regulations for the progress and growth of e-commerce. Either of these proposals will aid in clearing up the confusion surrounding the use of digital signature internationally. More importantly, they can provide the legal certainty that is desperately needed to further the growth of e-commerce and encourage the use of digital signatures.

95. Draft Guide, *supra* note 8.

96. *See generally supra* note 5; *see also* S. Res. 761, 106th Cong. (2000) (enacted). *See generally* Electronic Signatures, *supra* note 5.