The European Commission’s Directive on Electronic Signatures: Technological “Favoritism” Towards Digital Signatures

Andrew Barofsky

Follow this and additional works at: http://lawdigitalcommons.bc.edu/iclr
Part of the European Law Commons, and the Internet Law Commons

Recommended Citation
http://lawdigitalcommons.bc.edu/iclr/vol24/iss1/5

This Notes is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College International and Comparative Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.szydlowski@bc.edu.
THE EUROPEAN COMMISSION'S DIRECTIVE ON ELECTRONIC SIGNATURES: TECHNOLOGICAL "FAVORITISM" TOWARDS DIGITAL SIGNATURES

ANDREW BAROFSKY

Abstract: The increasing use of e-commerce generally is considered a positive trend that should be fostered. Yet, many lawmakers believe that laws requiring signatures to authenticate certain transactions represent obstacles to e-commerce and threaten to keep it from reaching its full potential. In the European Union, several Member States have drafted or enacted "electronic signature" laws to define the legal validity of electronic signatures. However, many of these laws are taking diverging approaches, thus creating an inconsistent framework for electronic signatures. In response, the European Commission recently adopted a directive to provide a common framework for electronic signatures. In its present form, the Signature Directive appears to favor the use of a particular type of electronic signature called a digital signature to the potential detriment of other current and future technologies. This Note examines the Signature Directive's approach to defining the legal validity of electronic signatures and concludes that the Commission should revise the Signature Directive to take a more technologically neutral approach.

INTRODUCTION

The volume of capital flowing through the veins of electronic commerce continually reaches new heights. By the year 2002, the total value of Internet transactions alone is expected to reach 446 billion U.S. dollars. This phenomenal growth of the Internet is radically impacting modern commercial and governmental practices. Organis-

2 Id.
zations worldwide are rearranging administrative and marketing strategies in order to exploit this powerful technology.  

Many consider Internet growth to be a positive development that should be fostered. Several lawmakers believe that certain legal "barriers" threaten to keep e-commerce from reaching its full commercial potential. This concern led to the development of many legal strategies aimed at removing legal obstacles to electronic commerce. The requirement that a "signature" authenticate certain transactions is one obstacle that receives a great deal of attention. Uncertainty exists about whether contracts made and "signed" through entirely electronic means will be deemed valid. Supporters argue that laws requiring signatures are "flexible and supportive of new commercial methods" and, therefore, electronic signatures should be recognized. However, due to persistent skepticism, most agree that some degree of legislative intervention is called-for.

In the European Union (EU), several Member States already have drafted or enacted "electronic signature" laws to define the legal validity of electronic signatures. Many of these laws take diverging approaches. The European Commission (Commission) believes this lack of uniformity endangers "the functioning of the Internal Market in the field of electronic signatures." Moreover, "[d]ivergent rules

---

4 See id.
6 Id. at 737.
8 See Benjamin Wright & Jane K. Winn, The Law of Electronic Commerce § 14.02 (3d ed. 1999); Smedinghoff & Bro, supra note 5, at 726.
9 Smedinghoff & Bro, supra note 5, at 732.
11 Wright & Winn, supra note 8, § 14.02.
14 Id.
concerning the legal effect attributed to electronic signatures are par­
ticularly detrimental to the further development of electronic com­
merce and, for this reason, to economic growth and employment in
the Community."\textsuperscript{15} In response, the Commission proposed a Directive
to provide a common framework for electronic signatures (Draft Di­
rective).\textsuperscript{16} The Draft Directive's primary aim is to create a "harmon­
ized and appropriate legal framework for the use of electronic signa­
tures within the Community and [to establish] a set of criteria which
form the basis for legal recognition of electronic signatures."\textsuperscript{17} The
European Council adopted the Signature Directive on December 13,
1999 (Signature Directive).\textsuperscript{18}

This Note examines the Signature Directive's approach to
defining the legal validity of electronic signatures. Part I presents a
background on E-commerce and electronic signatures. Part I also in­
troduces the Signature Directive, focusing on Article 5 which con­
centrates on legal validity, as well as other electronic signature laws
promulgated throughout Europe. Part II discusses the "technology­
neutral" and "digital signature" approaches to electronic signature
legislation, while Part III analyzes the issues raised by the Signature
Directive's approach for creating a harmonized standard for legal va­
lidity of electronic signatures. This Note concludes by arguing that
the Commission should revise the Signature Directive to take a more
technologically neutral approach.

I. HISTORY AND BACKGROUND

A. Signature Requirements

In civil and common law countries alike, the enforceability of
many types of contracts is subject to certain formalities.\textsuperscript{19} The most

\textsuperscript{15} Id.
\textsuperscript{16} Id.
\textsuperscript{17} Id.
\textsuperscript{18} Council Common Position EC) NO 28/1999 adopted by the Council on 28 June
1999 with a view to adopting Directive 1999/000/EC of the European Parliament and of
the Council of . . . on a Community framework for electronic signatures, 1999 O.J. (C 243)
33 [hereinafter Signature Directive]. Member States must comply with the Signature Di­
rective's provisions before July 19, 2001. Id.
\textsuperscript{19} See 1 Hein Kôtz, European Contract Law: Formation, Validity, and Content
of Contracts; Contract and Third Parties 78 (Tony Weir tr., Hein Kôtz & Axel
Flessner eds., 1997). Enforceability means that a party to the contract may bring a claim in
a court of law and obtain a judgement ordering performance or damages. Id.
common formality is the requirement of writing and signature. For example, many European countries require that all non-commercial transactions over the equivalence of 5000 Francs be in written or notarial form; otherwise, the evidence of witnesses is inadmissible. Similarly, most sales of land can “only be made in writing.”

Several reasons for formal requirements have been advanced, including preserving evidence, putting parties on notice, signaling the transition from negotiation to contract, and providing information. Conversely, several disadvantages to contract formalities also have been identified. These disadvantages include: (1) inhibiting freedom of contract, (2) slowing the “free flow of commerce,” and (3) allowing a party to defeat justified expectations. Of these three, the impediment to the “free flow of commerce” presents the greatest potential obstacle to e-commerce. Unless electronic documents are treated as “writings” which can be “signed,” paper records will have to supplement many electronic transactions, resulting in e-commerce that is “more expensive, less competitive, and less efficient.”

B. E-commerce and Electronic Signatures

Commercial data has been transferred between computers for several decades, primarily through Electronic Data Interchange (EDI). EDI technology typically involves transferring structured and coded messages, such as purchase orders and invoices, over secure network systems. The standards for structuring and coding the messages, as well as their legal consequences, are spelled out in paper-based contracts commonly referred to as “trading partner” agree-

20 See id. at 82; Wright & Winn, supra note 8, § 14.02; Joseph M. Perillo, The Statute of Frauds in the Light of the Functions and Dysfunctions of Form, 43 Fordham L. Rev. 39, 40 (1974).
22 Kötzt, supra note 19, at 83 & n.25.
23 Id. at 89.
25 See Robertson, supra note 24, at 812.
26 Id.
27 Id. at 814
28 Id.
29 Wright & Winn, supra note 8, § 2.05.
30 Robertson, supra note 24, at 790–91, 794.
EDI offers several advantages over conventional paper-based commerce. It eliminates paper “shuffling and storage,” allows for quicker response time, reduces human error, and decreases misunderstandings. Use of EDI, however, generally is limited to companies involved in ongoing commercial relationships. Accordingly, EDI lacks broad consumer access.

In contrast, Internet-based commerce can involve transactions between unfamiliar parties, including both businesses and consumers. This feature, coupled with a phenomenal expansion in the number of online participants, has made the Internet a worldwide marketplace. This marketplace, however, is a more hazardous environment than most EDI systems. Although both technologies involve the transfer of alterable digital messages, EDI transactions typically occur over secure networks and employ specially structured and coded messages. Moreover, trading partner contracts define the legal effects of EDI transactions. By contrast, messages transmitted over open networks, such as the Internet, can be intercepted and manipulated by third party users without detection. Furthermore, it is relatively difficult to identify the source of a message transmitted over the Internet. Finally, the holder of electronic records can “easily and undetectably” alter the records.

Despite the security risks, data routinely is transferred over the Internet throughout the commercial world. Paper is rapidly giving way to purely electronic forms of documentation. This trend includes the increased use of electronic documents in the formation of

32 Robertson, supra note 24, at 793–94.
33 Id.
34 Nimmer, supra note 31, at 213; Robertson, supra note 24, at 791.
35 Robertson, supra note 24, at 794.
36 Id. at 791.
38 See id. at 794–95.
39 Id.
40 Nimmer, supra note 31, at 214.
41 Robertson, supra note 24, at 796.
42 Id.
43 Id.
44 Statistics, supra note 1.
contracts. Electronic contracts, like their paper counterparts, are subject to contract formalities requiring "signatures." There are many ways to "sign" an electronic contract. A simple text signature closing an e-mail message is a common example. Another example is a "mouse click" that indicates the intent to be bound by certain legal terms on a web page. Although simple methods such as these theoretically may satisfy the formality of signature, they lack many of the "inherent security attributes" of signed paper documents, such as "semipermanence of ink embedded in paper, unique attributes of some printing processes, watermarks, the distinctiveness of individual signatures, and the limited ability to erase, interlineate, or otherwise modify words on paper." Furthermore, in order to overcome the Internet's inherent security risks, electronic signatures must serve three critical purposes, "[1] to identify the source or sender, [2] to indicate the sender's intent (for example, to be bound by the terms of a contract), and [3] to ensure the integrity of the document signed." Text e-mail signatures, mouse clicks, and the like apparently fail to serve these purposes.

Therefore, more sophisticated methods for securely authenticating electronic documents have been developed. The most popular is the "digital signature." Digital signatures are a special class of electronic signatures that use public key cryptography to give electronic signatories a unique digital identification. Used properly, digital sig-

46 See generally Nimmer, supra note 31; Robertson, supra note 24.
47 Wright & Winn, supra note 8, § 14.02.
48 See id.
49 Wright & Winn, supra note 8, §§ 14.02, 14.05[E]; see also Doherty v. Registry of Motor Vehicles, No. 97CV0050 (Mass. Dist. Ct. Suffolk Cty. May 28, 1997), at http://www.magnet.state.ma.us/itld/legal/case.htm (last visited Nov. 27, 1999). In Doherty, the Massachusetts District Court concluded "that a police officer who files or transmits (or who has another file or transmit) a report that is required by law to be made to the Registry of Motor Vehicles or to some other agency or individual by means of Email or some other electronic method in which there is a statement that identifies the officer making the report and a statement that it is 'made under the penalties of perjury' has 'signed' the document and is subject to a prosecution for perjury if the report is willfully false in a material manner even though the report does not contain a handwritten signature." Id.
50 Wright & Winn, supra note 8, § 14.02.
51 Robertson, supra note 24, at 796.
52 Boss, supra note 45, at 597–98; Smedinghoff & Bro, supra note 5, at 732.
53 See id.
54 See Boss, supra note 45, at 597–98.
55 Id.
56 Wright & Winn, supra note 8, § 3.06[D]; Boss, supra note 45, at 597–98.
natures identify the sender, ensure message integrity, and render the message non-repudiative.57

Cryptography is the process of communicating in secret writings.58 In conventional cryptography, identical keys are used to encrypt (i.e. “sign”) and decrypt messages.59 By contrast, public key cryptography is an asymmetric system in which a “private key” is issued to the key subscriber and a separate but mathematically linked “public key” is widely distributed.60 Only the holder of a linked private key can decipher a document “signed” with a public key.61 Conversely, if a document is signed with a private key, any holder of a corresponding public key can decipher the message.62 However, “it is technically impossible to derive a private key from a published public key.”63 In addition, the message’s integrity is verified by using special mathematical algorithms known as hash functions.64 Each encrypted or signed message has a unique hash result.65 If a message is tampered with, the hash result is altered and the signature invalidated.66 Systems that manage the keys are called Public Key Infrastructures (PKI).67 In a typical PKI, Certification Authorities (CA) issue keys and guarantee the identity of private key holders.68

Digital signatures are not, however, the only available form of secure electronic signature.69 “Signature dynamics” combines biometrics and cryptography to create signatures that securely attach unique characteristics of an actor’s character or behavior to an electronic document.70 Successful examples include the PenOp and SMART-pen.71 These devices capture an individual’s signature while simulta-

57 Biddle, supra note 10, at 1228.
59 Wright & Winn, supra note 8, § 3.06[C]. Conventional cryptography is also known as “symmetric cryptography.” Id.
60 Id.; Philip S. Corwin, Digital Signatures and Signature Dynamics: Some Issues to Consider, 17 BANKING POL’Y REP. 1, 10 no. 9 (1998).
61 Wright & Winn, supra note 8, § 3.06[C].
62 Id.
63 Corwin, supra note 60, at 10.
64 Id.
65 Id.
66 Id.
67 Id., § 3.06[D].
68 Corwin, supra note 60, at § 3.06[D].
69 Wright & Winn, supra note 8, § 3.06[B]; Corwin, supra note 60, at 9.
70 Corwin, supra note 60, at 9.
neously verifying the individual’s identity.\textsuperscript{72} Signature dynamic methods of authentication have the advantage of being bound to the signatory rather than to the document.\textsuperscript{73} This feature eliminates the need to go through a trusted third party or a CA to link an electronic signature to an individual.\textsuperscript{74} Not only do digital signature and signature dynamics overcome digital technology’s susceptibility to easy forgery and manipulation, these technologies make possible a degree of security far greater than that established by ink on paper.\textsuperscript{75}

C. European Electronic Signature Laws

In the EU, only Germany and Italy have enacted electronic signature legislation.\textsuperscript{76} Several other Member States, however, have legislative proposals under review or ready for adoption.\textsuperscript{77} A brief review of different European legal schemes highlights the different approaches taken to regulate electronic signatures.\textsuperscript{78}

On March 15, 1997, Italy passed the Bassini Law (Italian Law) which validates the use of digital signatures for legal transactions.\textsuperscript{79} The Italian Law is limited strictly to digital signatures.\textsuperscript{80} Notably, it treats a digital signature as the equivalent of a hand-written signature only if it is based on asymmetrically paired keys that are certified by an officially authorized CA.\textsuperscript{81} The Italian Law recognizes digital signatures from other Member States if they are based on “equivalent requirements.”\textsuperscript{82}

Germany passed digital signature legislation in August of 1997 (German Act).\textsuperscript{83} The German Act focuses on defining the “conditions

\textsuperscript{72} Corwin, supra note 60, at 10.
\textsuperscript{73} Id. at 11.
\textsuperscript{74} Id. at 15.
\textsuperscript{77} Baker & Yeo, supra note 12; EESSI Report, supra note 76, at 84-86.
\textsuperscript{78} Id. An up to date review can be found in Van der Hof, supra note 12, at http://cwis.kub.nl/~frw/people/hof/ds-lawsu.htm#esigdir (last visited Nov. 23 1999).
\textsuperscript{79} EESSI Report, supra note 76, at 81.
\textsuperscript{80} Id. at 83.
\textsuperscript{81} Id.
\textsuperscript{82} Id.
\textsuperscript{83} Id. at 80; Kuner & Miedbrodt, supra note 75.
under which digital signatures are deemed secure."\textsuperscript{84} Unlike the Italian Law, it does not grant digital signatures the legal equivalency of hand-written signatures.\textsuperscript{85} Rather, digital signatures meeting voluntary technical standards merely are presumed to be “secure” in a court of law.\textsuperscript{86} The principal effect of the German Act is that users of digital signatures may benefit from a legal presumption that is not attainable through the use of other types of electronic authentication technology.\textsuperscript{87}

In contrast to the Italian Law and the German Act, the United Kingdom is proposing an Electronic Communications Bill (English Bill) that will grant electronic signatures legal admissibility in court for the purpose of establishing the “authenticity” or “integrity” of communications.\textsuperscript{88} “Authenticity” refers to whether the communication or data comes from a particular person or other source or is accurately timed and dated.\textsuperscript{89} “Integrity” refers to “whether there has been any tampering with or other modification of the communication or data.”\textsuperscript{90} The English Bill is not tied to one particular technology and “leaves it up to the court[s] to decide in a particular case whether an electronic signature has been correctly used and what weight it should be given.”\textsuperscript{91}

D. Electronic Signature Directive

On June 18, 1999, the European Council reached a common position on the Signature Directive.\textsuperscript{92} The primary aim of the Signature Directive is to create a “harmonized and appropriate legal framework for the use of electronic signatures within the Community and [to establish] a set of criteria which form the basis for legal recognition of electronic signatures.”\textsuperscript{93} The Signature Directive defines an “elec-

\textsuperscript{84} Kuner & Miedbrodt, \textit{supra} note 75.
\textsuperscript{85} \textit{Id.}
\textsuperscript{86} \textit{Id.}
\textsuperscript{87} \textit{Id.}
\textsuperscript{88} House of Commons, \textit{Electronic Communications Bill}, cl. 7, \textit{at} \url{http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmbills/004/2000004.htm} (last visited Dec. 4, 1999). The Electronic Communications Bill was presented to the House of Commons on 18 November 1999. \textit{Id.}
\textsuperscript{89} \textit{Id.}, cl. 23(2).
\textsuperscript{90} \textit{Id.}
\textsuperscript{91} Department of Trade and Industry, Explanatory Notes to the Electronic Communications Bill, \textit{at} \url{http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmbills/004/en/00004x.htm} (last visited on Dec. 4, 1999).
\textsuperscript{92} Signature Directive, \textit{supra} note 18.
\textsuperscript{93} Draft Directive, \textit{supra} note 13.
tronic signature” as “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.”

According to the Signature Directive, an “advanced electronic signature” is an electronic signature if:

   a) it is uniquely linked to the signatory;
   b) it is capable of identifying the signatory;
   c) it is created using means that the signatory can maintain under his sole control; and
   d) it is linked to the data to which it relates in such a manner that any subsequent alteration of the data is detectable.

The Signature Directive takes a two-tiered approach in defining the legal effects of an electronic signature. The first tier requires Member States to “ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings” solely because it is a) not in electronic form, b) not based on a qualified certificate or not based on a qualified certificate issued by an accredited certification-service-provider, or c) not created by a secure signature-creation device. A “certificate” is an “electronic attestation which links signature-verification data to a person and confirms the identity of that person.”

A “qualified certificate” is a certificate that meets specific security standards and is issued by a qualified “certification-service-provider,” more commonly known as a CA. The Signature Directive lays down requirements for qualified certificates and CAs in Annexes I and II, respectively. Similarly, requirements for a “secure-signature-creation device” are laid down in Annex III.

The first level of legislation accepts most electronic signatures on a technologically-neutral basis.

The second tier of legal validation entitles qualified technologies to legal equivalency with handwritten signatures. The Signature Directive requires Member States to:

94 Signature Directive, supra note 18, art. 2(1).
95 Id., art. 2(2).
96 Baker & Yeo, supra note 12; see also EESSI Report, supra note 76, at 19.
97 Signature Directive, supra note 18, art. 5(2).
98 Id., art. 2(9).
99 Id., art. 2(10).
100 Id.
101 Id., art. 2(6).
102 Baker & Yeo, supra note 12.
103 Id.; see also EESSI Report, supra note 76, at 19.
ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data, and b) are admissible as evidence in legal proceedings.\textsuperscript{104}

II. DISCUSSION

The proliferation of electronic signature legislation, both in the United States and abroad, has fueled much scholarly debate.\textsuperscript{105} A central source of disagreement among scholars and lawmakers is whether the laws governing electronic signatures should remain neutral towards technology or attempt to specifically regulate currently favored technologies.\textsuperscript{106} At the time when the first electronic signature initiatives began to emerge, digital signatures were the most widely used and universally accepted means for securely authenticating electronic documents.\textsuperscript{107} Therefore, early electronic signature initiatives were limited to promoting and facilitating digital signature technology.\textsuperscript{108} The Utah Digital Signature Act, enacted in 1995, typifies this approach and is the foundation for subsequent initiatives, including the German and Italian digital signature laws.\textsuperscript{109} Supporters of the "technology movement," particularly the German Government, continue to believe that e-commerce legislation should be "limited to digital signatures, and thus to a technical concept for guaranteeing authenticity and integrity which can satisfy the high technical security standards required in electronic commerce."\textsuperscript{110} In jurisdictions that have enacted digital signature-specific laws, it is not be clear whether an

\textsuperscript{104} Signature Directive, \textit{supra} note 18, art 5(2).
\textsuperscript{106} Boss, \textit{supra} note 45, at 601; Baker & Yeo, \textit{supra} note 12.
\textsuperscript{107} Boss, \textit{supra} note 45, at 598; Baker & Yeo, \textit{supra} note 12.
\textsuperscript{108} Boss, \textit{supra} note 45, at 601.
\textsuperscript{109} Id. at 600, 606.
electronic message signed by any method other than a digital signature is valid.111

Laws favoring digital signatures have sparked much criticism.112 Critics argue that such legislative intervention is premature, overregulating, and interferes with the natural evolution of the market.113 "Favoritism" toward digital signatures risks excluding other possibly superior technologies from entering and competing in the marketplace.114

More recent electronic signature laws have parted with the "technology movement" in favor of more technology-neutral or "minimalist" legal frameworks.115 The goals of the "law revision movement" are to "remove the barriers to electronic commerce, treat electronic communications on a par with paper communications, and not to favor one technology over another (technology neutrality) nor one business model over another (implementation neutrality)."116 According to this theory, the law merely should enable the use of electronic signatures, so that parties are free to choose whatever "technology" and "implementation scheme" they deem most suitable for their particular transactions.117 Initiatives cast under this approach intentionally avoid regulating authentication techniques, such as digital signatures.118

"Minimalist" laws are criticized for failing to establish a reliable security infrastructure.119 Potential participants may forego engaging in e-commerce because of the absence of legally recognized security procedures.120 Moreover, the pervasive use of insecure electronic signatures may give rise to fraud, message tampering, and mistake, fur-

111 Robertson, supra note 24, at 821–22.
112 See Wright & Winn, supra note 8, ¶ 14.08[C]; Biddle, supra note 10, at 1226; Boss, supra note 45, at 624; Robertson, supra note 24, at 824–25.
114 See Wright & Winn, supra note 8, ¶ 14.08[C]; see Consensus Principles, supra note 113.
115 Baker & Yeo, supra note 12; Corwin, supra note 60, at 11.
116 Boss, supra note 45, at 601.
117 Id.
118 Baker & Yeo, supra note 12.
120 Boss, supra note 45, at 617.
ther decreasing confidence in e-commerce. Accordingly, in order for e-commerce to enjoy widespread use, critics argue, a reliable security infrastructure is needed.

III. Analysis

The Signature Directive’s two-tiered structure strives to reach a middle ground between technology-specific and enabling approaches. On the one hand, the Signature Directive enables the use of all electronic signatures by mandating their “legal effectiveness and admissibility as evidence in legal proceedings.” On the other hand, it promotes digital signature technology by creating a presumption that “advanced electronic signatures which are based on a qualified certificate . . . satisfy the legal requirements of a signature . . . in the same manner as a handwritten signature.” This presumption is limited functionally to digital signatures because qualified certificates are unique to PKI technology.

Under the Signature Directive, authentication methods that qualify as “advanced electronic signatures,” created by a “secure-signature-creation device” but not based on a qualified certificate, appear to fall short of presumptive equality with handwritten signatures. It follows that signatures created through signature dynamics would not enjoy the same presumptive validity as digital signatures because they provide direct proof of signer identity rather than relying on “a complex system of trusted third parties.” Thus, under the current Signature Directive, a business using an otherwise “secure” signature method that is not a digital signature subject to a qualified certificate risks creating an unenforceable or voidable contract. This is not “technological neutrality” but rather technological “favoritism.”

As Theodore Roosevelt said, “[I]t is difficult to make our material condition better by the best law, but it is easy enough to ruin it by bad laws.” As between the technology-specific and technology-neutral

---

121 Id.; Robertson, supra note 24, at 795.
122 Kuner, supra note 119.
123 Boss, supra note 45, at 604, 606; Baker & Yeo, supra note 12; see also Signature Directive, supra note 18, art. 5.
124 Signature Directive, supra note 18, art. 5(1).
125 Id., art. 5(2) (emphasis added).
126 WRIGHT & WINN, supra note 8, § 3.06[D].
127 Signature Directive, supra note 18, art. 5(2).
128 Id.; Corwin, supra note 60, at 15.
129 Id.
approaches, it is the latter that comports with the principles suggested by this maxim. Businesses that engage in sound commercial business practices will, as they currently do, choose methods for signing their computer documents that meet their commercial needs. Businesses should use digital signatures because they solve practical problems created by open network transactions, not because the law dictates their use. "[T]he technology implementation itself provides the necessary security and certainty necessary for electronic commerce without the need for legislative intervention." Thus, laws favoring digital signatures are not needed to create a "security infrastructure." Moreover, enacting technology-specific and technology-favoring laws risks precluding more favorable market-oriented solutions.

In its present form, the Signature Directive appears to favor digital signatures to the potential detriment of other current and future technologies. Encouraging the use of digital signatures is superfluous to achieving the Signature Directive's goals of Market harmonization. Simply validating currently held broad interpretations of what is a "writing" is sufficient to remove fears that electronic contracts will be held invalid. For example, Ireland is considering this better reasoned approach and recently unveiled an outline for electronic signature legislation. This outline borrows the Signature Directive's first tier of validation, but notably leaves out the second tier.

CONCLUSION

Statutes that merely extend legal recognition to electronic signatures can best foster electronic commerce on the Internet. Statutes

\[131\] See Boss, supra note 45, at 624; see also The Columbia Dictionary of Quotations, supra note 130.

\[132\] See Boss, supra note 45, at 624.

\[133\] See id.

\[134\] Id. at 623.

\[135\] See id.

\[136\] See id. at 607.

\[137\] See Signature Directive, supra note 18, art. 5.

\[138\] See Boss, supra note 45, at 624.

\[139\] See Wright & Winn, supra note 8, § 14.01; Wright, supra note 10.


\[141\] Id.
that, in the name of security, favor one emerging technology over another will hinder the natural growth of a burgeoning market. Under the Signature Directive, the fittest technology may not be given a chance to survive. The Commission should revise the Signature Directive to "enable" electronic signatures and to eliminate the special treatment granted to digital signatures.