ELECTRONIC SIGNATURES IN LAW (THIRD EDITION)

Stephen Mason
Cambridge University Press, 2012
408 pages, $215.00
ISBN-10: 1-10-7012295
ISBN-13: 978-1-10-7012295 Hardback

IDENTITY IN LAW

Reviewed by Timothy S. Reiniger*

In this analysis and critique of electronic signature forms and laws as they are developing around the world, Stephen Mason explains the authentication, evidentiary, and authority purposes of electronic signatures and their historical antecedents in signature law generally. This is not intended to be simply a "how to" guide for everyday practitioners. Instead, Mason's mission is to remind policy makers and judges that electronic signatures are yet another technology that must be governed by existing legal principles and made to serve human needs. Technology and systems must not be allowed to supersede or change an "ancient protocol" of law.[1]

Without attempting to be prescriptive, Mason presents electronic signa tures as being essential to establish identity relationships and determine legal responsibility in the information economy. Electronic signatures are not only the primary method of authentication in law, they also represent or symbolize identity relationships in a given context.[2] To study this book is to study the law of identity.

*Timothy Reiniger is an attorney specializing in information security and digital evidence, and is a member of the California, the District of Columbia, and New Hampshire Bars. As Execu tive Director of the National Notary Association, he contributed a chapter on electronic notariza tion in George L. Paul's *Foundations of Digital Evidence* (A.B.A. 2008). Currently, he is Director of the Digital Services Group at FutureLaw, LLC, in Richmond, Virginia. URL: http://www.future law.net/digital-services-group.htm.

1. STEPHEN MASON, ELECTRONIC SIGNATURES IN LAW, at v (Cambridge University Press 3rd ed. 2012) (referencing new prologue Haiku written by Mason).

2. *Id.* at 2; Nicholas Bohm & Stephen Mason, *Identity and Its Verification*, 26 COMPUTER L. & SECURITY REV. 43, 43–51 (2010).

I. LEGAL CONTEXT AND IMPORTANCE OF THE BOOK

The rise of the digital network-based information economy, and the cyber netic theories upon which it is based, has produced identity deficit or increased absence of the person.[3]For law, cybernetics[4]governance principles and com puting machines have caused profound policy crises related to authentication, authenticity, and authority. Specifically, cybernetics raises important legal considerations with respect to the manner in which information and actions are linked to persons, genuineness is proven, and responsibility is determined in systems.[5]

Signature law has historically been the primary method by which law links acts to human intent and identity. Hence, the treatment of electronic signatures necessarily assumes a central role in establishing and resolving such links in the information economy. Stephen Mason's analysis of electronic signatures provides timely and essential insights that may help resolve three main crises and address the absence of persons resulting from computing ma chines and information systems.

The first ongoing crisis involves the capability of authenticating identity in digital or online environments.[6] The network-based economy and systems each require trust in the capability to identify and authenticate individuals who seek to obtain access to networks, share information, and sign documents. Therefore, proving the authentication of an act as that of a specific person is a main evidentiary concern. It is necessary to know who has access to the digital information and why.[7] A reflection of the authentication crisis is the *National Strategy for Trusted Identities in Cyberspace (NSTIC)*,[8] which recognizes the

3. *See, e.g.*, VACLAV HAVEL, DISTURBING THE PEACE: A CONVERSATION WITH KAREL HVÍŽ ALA 10, 195–96 (Paul Wilson trans., 1990) (referencing "identity that is decaying, col lapsing, dissipating, vanishing" in the face of "impersonal, anonymous, irresponsible" power); GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 92 (2008) ("Fundamental to any discus sion about proof of digital identity is an understanding that information systems have no intrinsic way of knowing the identity of entities that participate in the systems' reading and writing games."); JOSEPH VINING, FROM NEWTON'S SLEEP 248 (1995) ("[T]he personal disappears in process and system.").

4. NORBERT WIENER, THE HUMAN USE OF HUMAN BEINGS: CYBERNETICS AND SOCIETY 15, 27 (1954) (defining cybernetics as the study of messages to explain purposive behavior in ma chines and how they regulate themselves in changing environments and systems).

5. *Id.* at 17–18, 25–27 (suggesting that cybernetics reduces all activity to processes, which consist of two ingredients: information and feedback). *See also* PETER F. DRUCKER, THE AGE OF DISCONTINUITY: GUIDELINES TO OUR CHANGING SOCIETY 38 (1969) ("Underlying [the infor mation industry] is a new perception: the perception of 'systems.'").

6. MASON, *supra* note 1, at 268–69 ("The function of attaching an electronic signature to a document or message is not understood in the same way as the use of manuscript signatures, partly because the signature can be applied to the document without any action by the individual to whom the signature is attributed, or without their knowledge.").

7. *See also* WIENER, *supra* note 4, at 18 (providing some historical context to the importance of communication and control). *See generally* PETER F. DRUCKER, MANAGEMENT CHALLENGES FOR THE 21ST CENTURY 124–28 (1999) (describing how the key to productivity in the knowledge society is the flow of information).

8. NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, http://www.nist.gov/nstic/ (last visited Dec. 14, 2012).

need to ensure all industries can rely on trusted digital identity credentials for access control purposes.[9]

The second crisis involves the capability of proving the authenticity of data.[10] Distinguishing authentic digital records from those that are forged is a central evidentiary concern. This concern is complicated by the untestable and ephemeral nature of digital data, the ease and pervasiveness of copying digital information, and ubiquity of network access to digital documents. Within virtual reality, how is genuineness established? Electronic signatures need to link persons to actions and thereby provide a necessary immutable reference for proving the authenticity of digital information over time.[11]

The third recent crisis involves dealing with authority and control over electronic signatures and identity in the context of information systems and network communications.[12] What is the source of authority for creating and managing digital identities? No person or entity is in charge of digital net works. Law and technology now compete to be the authority or authoritative source for enabling identity relationships and determining responsibility. Technology in closed systems seeks to create stability and order by means of quantifying life into bits of information or amounts of entropy.[13]In contrast, electronic signature law, by placing function over form, values greater empha sis on human choice and intent.[14]

9. THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE 5–8, 33–34 (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf. *See also* WORKING PARTY ON INFO. SEC. & PRIVACY, ORGANISATION FOR ECON. CO-OPERATION & DEV., THE ROLE OF DIGITAL IDENTITY MANAGEMENT IN THE INTERNET ECONOMY: A PRIMER FOR POLICY MAKERS 4 (2009), http://www.oecd.org/internet/interneteconomy/43091476.pdf.

10. PAUL, *supra* note 3, at xxvi ("Society must come to grips with whether it currently has an ability to learn the truth about everyday communications, agreements, transactions, and indeed all types of records of digital information. . . .[W]e currently exist in a regime of *untestability*."); George L. Paul, *The "Authenticity Crisis" in Real Evidence*, PRAC. LITIGATOR, Nov. 2004, at 45–46. For an historical comparison, see the discussion from the twelfth and thirteenth centuries regarding common law evidentiary proof standards for authenticating paper writings in M. T. CLANCHY, FROM MEMORY TO WRITTEN RECORD: ENGLAND 1066–1307, at 322 (2nd ed. 1993) ("Without defined standards of authenticity, there could be no definite criteria for distinguishing forgeries from authentic documents.").

11. MASON, *supra* note 1, at 265. Electronic signatures and networked communications are challenged by a lack of direct evidence in proving who clicked the button or caused the particular signature to be made. *Id.*

12. JEREMY RIFKIN, THE AGE OF ACCESS 11–15, 177–79 (2000); *see generally* VINING, *supra* note 3, at 36 ("[T]he very purpose and effect of authority is the maintenance of a sense of self against death or loss of self in the endless and meaningless processes of the world.").

13. WIENER, *supra* note 4, at 21–27 (describing the use of machines and feedback systems to stabilize performance and control the entropic tendency toward disorganization in nature and society). *See also* VINING, *supra* note 3, at 37–41.

> All in this view of the world and ourselves flows from the reduction of all to process and pattern, the first step in scientific thinking, and from the associated reduction of saying to doing. Everything depends upon these two assumptions, that the person or self can be collapsed into pattern and pro

cess, and that saying can be equated to doing or "behavior," permitting observation from the out side.

Id. at 41.

14. Warren Weaver, *The Mathematics of Communication*, 181 SCI. AM. 11, 13 (1949) ("In formation is . . . a measure of one's freedom of choice in selecting a message. The greater this

II. AUTHENTICATION: FUNCTION VERSUS FORM

Mason emphasizes that, based on the historical treatment of signatures in case law, determination of the validity of electronic signatures must be based on the legal functions of the signature and not the form.[15] In turn, the function of the electronic signature will depend on the "nature and content of the doc ument" or data to which it is attached.[16]

The use of an electronic signature has three authentication functions: access, attribution, and adoption.[17] First, an electronic signature can be used as, in effect, a key to allow authorized individuals to electronically obtain *access* to secure networks such as public registries. Second, an electronic sig nature should *attribute* the origin of a message so that the recipient can better trust the integrity and identity of the sender as an approved member of a net work or federation. Strong and generally reliable integrity and identity assur ance protocols are vital to secure information exchange. Third, an electronic signature provides a legal means for an owner to *adopt* the contents of a doc ument and enables proof of intent to perform the act of signing.

The act of signing, as a method of authentication, actualizes identity and intent.[18] The electronic signature attempts to bind the identity of a person to an act.[19] As Mason suggests:

> While an electronic signature does not have the same characteristics as a manuscript signature, it is the equivalent of a manuscript signature when it performs a similar function. The better view is to consider an electronic sig nature as a link between protocols of electronic devices that communicate via software, each with the other. The attention should be focused on the treat ment of messages before they are transmitted and after they are received.[20]

It is crucially important for a relying party to be able to trust the origin and integrity of the sender's electronic message, including the electronic sig nature.[21] "Whether an electronic signature merely acts to authenticate interac tions between protocols or to identify the sender will be determined by the ability to establish a connection between the signature and the person affixing

freedom of choice, and hence the greater the information, the greater is the uncertainty that the message actually is some particular one. Thus greater freedom of choice, greater uncertainty, greater information go hand in hand."). S*ee generally* VINING, *supra* note 3, at 281 ("Against the constant fading of the conditions of authority is what comes from law that pushes toward the personal and a context of decision making in which the personal can be recognized, recognition of the personal being the only entry to the experience of authority.").

15. MASON, *supra* note 1, at 1, 3, 16, 20, 102, 218, 240.

16. *Id.* at 3.

17. *Id.* at 267 ("Whether a signature is in manuscript form or electronic format, the purpose of the signature will not alter.").

18. *Id.* at 5–6, 9–10, 20, 82, 143, 189, 236, 244. S*ee generally* VINING, *supra* note 3, at 65 (With respect to an act in law being a actualization of mind and meaning, "[s]igning a name is the signal example . . . .").

19. MASON*, supra* note 1, at 9, 104, 143, 189, 329.

20. *Id.* at 141.

21. *Id.* at 96–98, 292.

the signature to the data."[22] An accurate digital identity, in turn, rests on the quality of the procedure used to obtain the identifying information during the credential registration and issuance process.[23]

Electronic signatures must be issued with clear and unambiguous manage ment policies regarding password control, unique number identifiers, hashing capabilities, and public revocation lists. Afterwards, relying parties anywhere in the world can have confidence that the individual's credential-based signa ture is actually being used by the electronic signature owner and not an im poster. "The most important point to be aware of is this: *the private key of a digital signature is only as good as the password that protects it*."[24]

Ideally, the electronic signature will add a layer of protection against for gery for the content of the document by means of encryption, hashing, and other content controls. "An electronic signature can only be defined within the operational boundaries of the binary numbers used by computers."[25]

Mason provides detailed arguments for practitioners looking to challenge a particular digital certificate or digital signature process in court.[26]"Befud dled by technicians, many politicians have been misled into the false promise that only digital signatures can be the legal equivalent of a manuscript signa ture, mainly because of the incorrect assurances that digital signatures are secure and safe from interference."[27]

III. AUTHENTICITY: PERSONS VERSUS MACHINES

For Mason, machine or system-made evidence should be neither auto matically deemed more reliable than human testimony, nor given evidentiary presumptions.[28] The legal control of information assets in digital networks must be based on fundamental evidentiary requirements for proving authen ticity and reliability.[29] This legal control is enabled by electronic signatures and, specifically, the capability of proving the legal *act* of signing whether a document, an e-mail, or upon accessing a network or service.[30]

22. *Id.* at 94.

23. Patrick McKenna, *The Probative Value of Digital Certificates: Information Assurance Is Critical to E-Identity Assurance*, 1 DIGITAL EVIDENCE & ELEC. SIGNATURE L. REV. 55, 55–60 (2004).

24. MASON, *supra* note 1, at 286.

25. *Id.* at 142.

26. *Id.* at 129–30, 137, 154, 189–90, 285–92, 305–06, 309–13, 317, 319.

27. *Id.* at 154.

28. *Id.* at 169, 344–47. "In the digital environment . . . it must be emphasized that the con nection between the human and the machine cannot be bridged, and the technology is fallible." *Id.* at 268.

29. *Id.* at 5–10.

> One presumption that may apply to computers is the presumption that a machine is presumed to be in working order. In the context of digital evidence, however, it is pertinent to be aware of the im perfections inherent in the way computers function, and how digital evidence is prone to alteration. Evidence derived from a computer must be admissible, authentic, accurate and complete in the same way as any other form of evidence.

Id at 347.

30. *Id.* at 12–14, 97, 215, 218, 221, 241.

A critical prerequisite before an electronic signature should be relied upon is the verification of its authenticity. This requires validation of the electronic signature with a third party issuer or an existing registry, both of which nor mally can be accomplished online at the time of use.[31] This concept has a tested foundation in the self-authenticating acts of the notary public. Third parties relying on electronic notarizations, for example, must be able to inde pendently verify that the notary's electronic signature and seal have been used only by the named notarial officer.[32]

Mason points out, as well, that the smartcard has reliability problems similar to that of the digital signature.[33] An example of an electronic signature housed on a smartcard is the Personal Identity Verification-Interoperable (PIV-I) card, which can be issued by nonfederal identity providers at high identity assurance levels.[34]

An aspect of the authenticity crisis is seen in the differing views of law yers and engineers toward the concept of non-repudiation. Mason asserts that non-repudiation "is a dangerous term, and one that lawyers should take partic ular care in understanding. It does not mean the system for non-repudiation is perfect, although some technical authors (and lawyers and academics) con tinue to assert that digital signatures are better than they actually are."[35]

The following extended passage reflects Mason's belief in the need to challenge technology applications in the context of evidentiary proof.

> When engineers use the term non-repudiation in an engineering technical sense, they mean that there is a high degree of probability that the protocol can demonstrate a document or message was sent or received by a particular computer, or to put it another way (perhaps more accurately), "Nonrepudia tion provides proof of the integrity and origin of data that can be verified by a third party." This logic is often extended from the engineering domain into the legal domain, by asserting that if the system can demonstrate a message or document was sent or received, then it should be for the recipient to demonstrate it was not sent or received by them. . . . It is important to ensure the technical meaning does not override the need to restrain the meaning within a legal context. Where engineers use the term, it should not be mis taken that they are using it in a legal context, despite a general misunder

31. INFO. SEC. COMM., AM. BAR ASS'N, DIGITAL SIGNATURE GUIDELINES 14–15, 32–33, 45–46, 49–50, 57–58 (1996). The certificate status information is included in the digital signature as either a time stamped Certificate Revocation List (CRL), which indicates indirectly that the certificate of the signatory was not revoked before the time the signature was created. *See also* MASON, *supra* note 1, at 317; PAUL, *supra* note 3, at 168–69. Relying parties also may use an On line Certificate Status Protocol (OCSP) response that checks the actual validity status of the sig natory's certificate.

32. Timothy S. Reiniger, *Evidentiary Requirements for Electronic Notarization and the Legalization of Certified Electronic Documents*, *in* GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE app. c, at 212–13 (2008).

33. MASON, *supra* note 1, at 123–24, 137.

34. SMART CARD ALLIANCE, PERSONAL IDENTITY VERIFICATION INTEROPERABILITY (PIV I) FOR NON-FEDERAL ISSUERS: TRUSTED IDENTITIES FOR CITIZENS ACROSS STATES, COUNTIES, CITIES, AND BUSINESSES 4 (2011), http://www.smartcardalliance.org/resources/lib/PIV-I_White_Paper_012811.pdf.

35. MASON, *supra* note 1, at 318.

> standing that the term, in the view of some engineers, should have a legal meaning. Just because the evidence demonstrates that a message or document was sent or received, it does not follow that the message was sent by the per son whose username or password (or both user name and password) was used at the material time.[36]

IV. AUTHORITY: LAW VERSUS TECHNOLOGY

For Mason, authority for the use, application, and proof of electronic signatures rests in legal principles and not in technology or systems theory.[37] "Judges have always been required to apply the law, regardless of the tech nology used, and the development of the networked world is no different."[38]

Electronic signature owners have legal responsibility for the control and use of electronic signatures and electronic signature creation devices.[39]"But the recipient cannot determine whether the sending party authorized the use of the digital signature; this is also true of any other form of electronic signa ture."[40] Therefore, it is necessary to recognize an electronic signature owner's authority in the context of identity relationships.[41] This enables relying parties to grant access to a person who is seeking use of a service.[42] Therefore, con siderations for determining liability and the allocation of risk necessarily re volve around the relationship of access control to the electronic signature.[43]

Determinations of legal rights and duties are necessarily *contextual* ac cording to the identity relationships, data ownership, and control and reliability of the electronic signature. "Whether an electronic signature has been added to digital data with authority is a matter for the law governing the relationship between the person whose actions affix the electronic signature and the legal entity."[44] The electronic signature in the form of a digital signature is consid ered to have a property of non-repudiation, with liability flowing to the owner as a result.[45] The issuer of the digital signature typically includes standard indemnification and holds harmless clauses in its contractual relationship with

36. *Id.* at 319 (citation omitted).

37. *Id.* at 1, 59, 100, 198, 244.

38. *Id.* at 1.

39. *Id.* at 286–90.

40. *Id.* at 286.

41. Anssi Hoikkanen et al., *New Challenges and Possible Policy Options for the Regulation of Electronic Identity*, 5 J. INT'L COM. L. & TECH. 1, 4 (2010). *See also* INT'L TELECOMM. UNION, RECOMMENDATION ITU-T X.1252: BASELINE IDENTITY MANAGEMENT TERMS AND DEFINITIONS 3 (2010), *available at* http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10440 ("[I]den tification: The process of recognizing an entity by contextual characteristics.").

42. *The Data Deluge: Businesses, Governments and Society Are Only Starting to Tap Its Vast Potential*, ECONOMIST, Feb. 27, 2010, at 11 ("Rather than owning and controlling their own personal data, people very often find that they have lost control of it.").

43. *See* Nicholas Bohm, *Watch What You Sign!*, 3 DIGITAL EVIDENCE & ELEC. SIGNATURE L. REV. 45, 45–49 (2006) (discussing the contextual nature of identity).

44. MASON, *supra* note 1, at 96.

45. *Id.* at 266.

the owner of the identity certificate to ward against fraudulent or unauthorized use.[46]

Where access is based on the issuance of electronic signatures by a third party, responsibility needs to be allocated among the owner, the issuer, and the relying party.[47] This allocation necessarily involves determining responsibility for the security of private keys and passwords.[48]"In reality, the reliance rests on the quality of the digital evidence that ties a presumed identity to a pre sumed act, and in turn the integrity of the password and the security in place to protect the password and private key. It is generally recognized that the pass word is an exceedingly weak mechanism. . . ."[49] Historically, this is analogous to legal control requirements around the use of seals and stamping devices.[50]

Mason recognizes and gives extended treatment to liability allocation as an important issue affecting electronic signatures.[51] Currently, risk allocation, and any attempted limitation of liability amongst electronic signature and identity credential providers, is achieved through contract and statutes.[52]In this regard, Mason recommends specific contractual boilerplate language to avoid disputes over authority amongst corporate employees to make subse quent binding contract modifications.[53]

V. OTHER OBSERVATIONS

The reader will be delighted to find that case citations are in a form native to each jurisdiction and that the table of cases is organized for each separate jurisdiction. Regrettably, there is no similar table of statutes. In comparing the second and third editions, the reader will notice the omission of chapters with detailed discussion of English contractual liability and disclaimers. Materials

from the chapters on the signature, the form of the electronic signature, digital signatures, and liability have been rearranged for greater logical flow. Finally, some important topics, such as the discussion of non-repudiation, have been expanded. Of course, case law has also been updated.

46. For examples of contractual language used by identity credential providers, see IDENTRUST SERV., LLC, CERTIFICATION PRACTICE STATEMENT (2007), *available at* https://secure.identrust.com/certificates/policy/ts/identrust_trustid_cps_v2.2_20070514.pdf; OPERATIONAL RESEARCH CONSULTANTS, INC., ACCESS CERTIFICATES FOR ELECTRONIC SERV. (ACES): CERTIFICATE PRACTICE STATEMENT SUMMARY (2005), *available at* http://aces.orc.com/docs/ ORCACEScpsSumV3_2.pdf; RSA ROOT SIGNING SERV., CERTIFICATION PRACTICE STATEMENT (2007), *available at* http://www.rsa.com/products/keon/repository/practices/RSA_KEON_ROOT_SIGNING_CA_CPS.pdf; SYMANTEC CORP., SYMANTEC TRUST NETWORK (STN) CERTIFICATION PRACTICES STATEMENT (2011), *available at* http://www.verisign.com/repository/CPSv3.8.6_final.pdf.

47. *See* MASON, *supra* note 1, at 332.

48. *Id.* at 289–92.

49. *Id.* at 287 (citations omitted).

50. *Id.* at 52, 338–39, 344–46. For a comparative description of the Jitsuin seal used in Japan, see *id.* at 340–44.

51. *Id.* at 96–98, 178–86; 303–13; THE WHITE HOUSE, *supra* note 9, at 31.

52. MASON, *supra* note 1, at 178–79, 274.

53. *Id.* at 213–15.

Book Review

In a future edition, the reviewer hopes that Mason will add discussion and analysis of cybernetics, information theory, and entropy in the context of various proposed forms of electronic signature and identity credential strategies. This would be a great addition to policy discussions around federated identity management, access control, trustworthy computing, and identity theft. Finally, a future edition would benefit from an expanded index.

Mason's book is strongly recommended for any legal practitioner, policy maker, or judicial officer who needs to assess the deployment and use of electronic signatures. Nonattorney professionals and technologists working in the areas of identity management and access control will also benefit greatly from this book. In the United States, active participants in the NSTIC process in particular would be well advised to understand identity law as it exists in signature law for both physical and electronic signatures.