The John Marshall Law Review

Volume 31 | Issue 3 Article 12

Spring 1998

The Impact of Technology on the Notary Process, 31 J. Marshall L. Rev. 911 (1998)

Glen-Peter Ahlers Sr.

THE IMPACT OF TECHNOLOGY ON THE NOTARY PROCESS

GLEN-PETER AHLERS, SR.*

INTRODUCTION

Technology, in particular, telecommunications, shrinks the earth as people conduct immediate, dynamic conversations across expanses that once took days, weeks, even months, to cross with one-way communications. Today's computer video efficiency enables the world to conduct its affairs in an increasingly rapid manner as communications are delivered on-line and let people appear in more than one place at one time. As computer technology helps spin the globe more rapidly, why do people continue to cling to paper notions of formality?

Gutenberg's press was fine for print, but the digital press of the information age, the computer, creates dynamic documents that might contain text, but just as well might contain digitized sound, pictures, and video information. Additionally, with the correct wiring, although wires are not necessary anymore, a document can be instantly delivered, or "published" around the world.

---

* Professor Glen-Peter Ahlers, Sr. became Library Director and Associate Professor at the University of Arkansas School of Law in 1992. He went to Fayetteville from Washington, D.C., after creating an academic law library at the new District of Columbia School of Law.

He has over twenty years of library experience, including seventeen years in the law libraries of Wake Forest University, Washburn University, the University of New Mexico, and the District of Columbia School of Law. He obtained his Masters in Library Science degree from the University of South Florida in 1983, and his law degree from Washburn in 1987. Professor Ahlers served as President of the Southwestern Association of Law Libraries, and in addition to being Scribes Executive Director, he has edited the *Scrivener*, the Scribes newsletter, since 1992. Additional recent publications include *Election Laws of the United States*, a four-part loose-leaf set published by Oceana which is now in three volumes, a chapter on law school libraries in *History of Legal Education* to be published by Anderson Publishing Company, and *The Effect of Technology on the Notary Process*, which has been prepublished on the Internet for comments.

When he's not writing, editing, speaking, or running law libraries, Professor Ahlers spends time with his other loves: his wife Sondra and their four children: his namesake, who was born on daddy's birthday, Sandia, named for the mountains outside Albuquerque, Gavin Patrick, named for two of mom's favorite uncles, and Sierra Le Ann Rose, named for an aunt and grandma.

Technology today melds the telephone, television, and personal computer. These forms of media can provide dynamic ongoing documents as well as more traditional published or completed "whole" documents.

In the paper information age we sought paper acknowledgments to lend confidence to the integrity of inked signatures. At first blush it might seem that a notary's purpose, to note the identity of one who signs a document, is rendered moot in the digital age since computers and not people will be generating documents. But perhaps the greater complexity and more fluid consistency of today's technological documents should demand a greater effort to identify the person at the keyboard who signs or acknowledges an electronic document. Instead of causing the death of notaries public, technology might instead increase their importance. After all, who is going to organize and manage the many bits, the ones and zeros, of digital code orbiting around the globe? Ken Gilpatric, a Justice Department lawyer working on the National Performance Review team believes a digital notary is necessary "to make electronic commerce easy and trustworthy."[1] The American Bar Association coined the term "CyberNotary" in their Digital Signature Guidelines,[2] and Michael Closen believes notaries "have the opportunity to play a central role verifying documents on-line, taking the more sophisticated form of 'cybernotorizations.'"[3]

> Because the CyberNotary concept combines a novel legal specialization that does not currently exist with a technical competency that is also unheard of, there has been no small degree of confusion as to exactly what the CyberNotary is. Indeed, the involvement of the overseas notarial associations in this effort is largely a reflection of their desire to understand what the technical competency of this specialization might be, so that they can bring their members up to a level comparable to that of the CyberNotary. Accordingly, the [United States Council for International Business] and the [American Bar Association] are working together to increase the level of awareness in the legal community about the proposed specialization, how U.S. lawyers might become CyberNotaries, and the benefits that they can expect to accrue for their clients.[4]

---

1. Walter R. Houser, *The View From Inside: Electronic Notaries Can Provide Safe Transmission*, GOV'T COMPUTER NEWS, Mar. 17, 1977, at 34.

2. AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE 31 (1996) [hereinafter ABA GUIDELINES].

3. Michael L. Closen & R. Jason Richards, *Notary Publics–Lost in Cyberspace, or Key Business Professionals of the Future?*, 15 J. MARSHALL J. COMPUTER & INFO. L. J. 703, 704 (1997) [hereinafter *Lost in Cyberspace*].

4. Theodore Barassi, *The CyberNotary: A New U.S. Legal Specialization for Facilitating International Electronic Commerce*, BULL. L. SCIENCE, TECH., April 1995 at 5, 7.

Utah was the first state to create certification authorities[5] to track electronic names and addresses. Also, Florida addresses the internationalization of notaries public.[6] Only attorneys who have practiced law for at least five years, and who are admitted to practice in Florida may be appointed "Florida international notar[ies]" by the Florida Secretary of State.[7] Florida international notaries are "authorized to issue authentication instruments for use in non-United States jurisdictions."[8] The jurisdictions must have diplomatic relations with the United States, must not be terrorist countries, and trade with the jurisdiction must not be prohibited.[9] One curious provision of the statute provides that "authentication instruments of a Florida international notary shall not be considered authentication instruments within the borders of the United States and shall have no consequences or effects as authentication instruments in the United States."[10]

One wonders why the legislature, in going through the trouble of creating an office of international notary, would geographically limit the effect of the officer's authentications. Perhaps the rules and regulations, developed by the Florida Secretary of State will answer the question. Authentication instruments executed by Florida international notaries must reference the state statute, and must contain the transacting parties' particulars and capacities to act.[11] Additionally, this instrument must include "a confirmation of the full text" of the document, the signatures (or legal equivalents) of the parties, and the signature and seal of the international notary.[12] California[13] and Washington [14] also require certification authorities.

This article addresses the potential impact technology might have upon traditional face-to-face notarial encounters. While notaries may be authorized to perform various functions,[15] the focus of

5. UTAH CODE ANN. §§ 46-3-103(4), 46-3-201 to 204 (1997).
6. FLA. STAT. ANN. § 118.10 (West Supp. 1997).
7. *Id.* § (1)(b).
8. *Id.* § (3).
9. *Id.*
10. *Id.* § (4).
11. *Id.* § (1)(a).
12. FLA. STAT. ANN. § 118.10(1)(a).
13. California Digital Signature Regulations were promulgated pursuant to CAL. GOV'T CODE § 16.5 (West Supp. 1998). The regulations, not the act, define certification authority. *See Summary of Electronic Commerce and Digital Signature Legislation* (visited March 10, 1998) <http://www.mbc.com/legis/ californiahtml#calregulations> (stating rules defining certification authority as well as rules on the utilization of digital signatures in transactions involving public entities).
14. WASH. REV. CODE § 19.34 (1997).
15. The Model Notary Act authorizes four acts: taking acknowledgments, administering oaths and affirmations, executing jurats, and supplying copy certifications. MICHAEL L. CLOSEN ET AL., NOTARY LAW & PRACTICE: CASES & MATERIALS 187 (National Notary Association eds., 1997) [hereinafter NOTARY

this article is the most familiar notarial function of certifying, or authenticating signatures.[16] Section I of this article describes the notary's duties in the authentication process, the purpose of authentication, and how information technology plays a vital role daily in everyone's life. Section II addresses how encryption software encodes a message and the application of a digital signature to a document using this technology. Lastly, Section III analyzes whether emerging interactive video will be used in the electronic authentication process.

I. THE CURRENT ROLE OF THE NOTARY AND POSSIBLE USES OF TECHNOLOGY IN THE AUTHENTICATION PROCESS

People use notaries daily to create confidence that a signature, in fact, belongs to the person to whom it purports to belong. The idea of writing or memorializing a transaction, traced to the statute of frauds,[17] creates a confidence in transactions by minimizing chances for fraud. Written documents containing signatures[18] reveal

---

LAW]. Other tasks sometimes authorized by statute include noting protests, presiding at depositions, consecrating marriages, and opening safe deposit boxes. *Id.*

16. "The most important function of the notary is to help assure the integrity of written documents, so that such documents can be trusted in governmental and commercial settings." *Id.* at 10. "[T]oday the most important responsibility of notaries is the determination of the true identity of document signors. . . ." Vincent Gnoffo, *Notary Law and Practice for the 21st Century: Suggested Modifications for the Model Notary Act*, 30 J. MARSHALL L. REV. 1063, 1069 (1997).

17. 29 CAR. II C. 3 (1677).

18. There has been much written about what constitutes a signature. A name can be printed, typed, or written, or a mark can be used. What is important is that by signing, the signer must mean to identify the writing accompanying her signature as her own, or mean to adopt (authenticate) the writing. *See* REST. (SECOND) OF TORTS § 134 (1979); Hessenthafer v. Farzin, 564 A.2d 990, 993 (Pa. Super. Ct. 1989):

> Courts have refused to require a specific form of signature, so long as there is some indication that the "signer" intended to authenticate the memorandum. *See, e.g.*, Denunzio Fruit Co. v. Crane, 79 F. Supp. 117, 128-29 (S.D. Cal. 1948), *aff'd* 188 F.2d 569 (9th Cir. 1951), *cert. denied* 342 U.S. 820 (1951) (holding that when an agent agrees to a sale by teletype, writing bearing the mark of the agent satisfies the Statute of Frauds); Smith v. Ostly, 347 P.2d 684, 686 (Cal. 1959) (stating that the printed name ordinarily may be adopted as signature, and need not necessarily appear at end of document); Irving v. Goodimate Co., 70 N.E.2d 414, 417 (Mass. 1946) (holding that a memorandum is sufficient under statute if signed by person to be charged by printed, stamped, or typewritten signature, and if in signing he meant to authenticate paper as his act); Radke v. Brenon, 134 N.W.2d 887, 890 (Minn. 1965) (holding that in an action for specific performance of alleged oral contract a written memorandum containing parties' names, maps of land and terms of offer satisfied the statute); Hansen v. Hill, 340 N.W.2d 8, 12-13 (Neb. 1983) (holding that a typewritten signature may satisfy the statute if the signers's intent to authenticate memorandum is shown); Matthews v. Deane, 493 A.2d 632, 633 (N.J. Super. Ct. Ch. Div. 1984) (stating that

that both parties to the agreement acknowledge the document. Seals and stamps and notarial authentications increase confidence in the signature. "[T]o achieve this level of genuine trust of the authenticity of a document, the usual procedure has been that the document be signed by one or more parties, that the identity of each signer be confirmed by the notary, and that the notary memorialize the notarization. . . ."[19]

Technology has already changed the way transactions are protected. Paper enabled us to use a quill, fountain and ball-point pens, wax and embossed seals, and inked and self-inking stamps.[20] Yet, all of the previous technological advances still rely upon the notary and the person signing the document to meet face-to-face, either at the time the document is signed, or later when the signor appears before the notary to acknowledge the signature.[21] Until recently, face-to-face has meant "in the same place at the same time." Technology enables one to appear face-to-face with someone across town, across the country, and across the globe. Today, people send scrambled electronic documents "sealed" to prevent unauthorized access to the contents and to alert the rightful recipients to alterations. Document recipients, even total strangers, can quickly verify an electronic signature[22] and determine the integrity of the document.[23]

---

although the statute does not define "signature," signature is that which party intends to be to be his signature); Weber v. DeCecco, 61 A.2d 651, 653 (N.J. Super. Ct. Ch. Div. 1948) (stating that "typewritten or printed names, signatures in ink or pencil, or any name or symbol used by a party with the intention of constituting it his signature, is sufficient to comply with the statutory requirements"); Frohn v. Central Trust Co., 72 N.E.2d 303, 304 (Ohio Ct. App. 1946) (stating that for purposes of the Statute of Frauds, an instrument may be validated by a party in any manner which indicates an intention to be bound thereby, and may be signed with a typewriter if the intention is to sign it).

Hessenthafer v. Farzin, 564 A.2d 990, 993 (Pa. Super. Ct. 1989).

19. NOTARY LAW, *supra* note 15, at 10-11.

20. *See* Gnoffo, *supra* note 16, at 1064-65 (discussing the biggest technological advance in 150 years is the self-inking stamp); *see also Lost in Cyberspace*, *supra* note 3, at 727 (discussing that the waxen seal gave way to metal embosser, which gave way to the ink stamp seal, which gave way to self-inking stamp.) Some statutes require ink stamps instead of embossed stamps because ink stamps reproduce better in photocopies; Gnoffo, *supra* note 16, at 1096 (discussing that electronic notarizations "may one day supersede the ink seal as the ink seal has replaced the embosser and the embosser has supplanted wax").

21. Michael L. Closen & G. Grant Dixon III, *Notaries Public From the Time of the Roman Empire to the United States Today, and Tomorrow*, 68 N.D. L. REV. 873, 883-84 (1992).

22.

> An electronic signature can be as simple as a signature on a document sent via fax. It also can be a name or some other identifier included in an e-mail message. Other forms of authentication may include the use of tokens such as smart cards . . . or [a] particularly secure type of electronic signature, known as a digital signature . . . .

William E. Wyrough & Ron Klein, *The Electronic Signature Act of 1996: Breaking Down Barriers to Widespread Electronic Commerce in Florida*, 24 FLA. ST.

> [A digital] signature is never "visibly" the same, it is only deeply mathematically the same. It responds to the same verification, even though the actual value is different. To make the signature different each time, other elements beyond the password must be thrown into the mix. One convenient way to accomplish this is to perform an algorithm using the text of the document being signed. This results in a unique, but valid, digital signature, and it also provides a way to verify that the document has not been changed after the signature was affixed. The signature itself works also as a checksum on the document. This makes a signed contract un-modifiable.[24]

One question still remains: how soon will the new technological advances gain acceptance and enjoy the same confidence as paper, the quill, the fountain pen's nib, wax and embossed seals, or ink and self-inked stamped seals? As the public gains confidence in the integrity of today's digital information technologies, they will increasingly use the new technologies, and notaries have to evolve to meet the challenge.[25] The requirement of face-to-face meetings will be questioned, or at least more broadly construed. And as the globe shrinks, the boundaries of the notary's authority should expand. Two emerging technologies of particular importance are encryption programs including digital signatures[26] and interactive video.[27] The Internet is also important. Dirt roads between towns once carried commerce. Railroad tracks and superhighways that spanned continents, and ships that crossed the seas then surpassed the dirt road. Presently, electrical bits of information that instantly travel world-

---

U. L. REV. 407, 421 (1997) (citations omitted).

23. This is true if an asymmetric cryptosystem is used. *See infra* note 26 (discussing asymmetric cryptosystem). Private key or symmetric systems share a key, and do not allow verification of the integrity of the data because anyone with the key can alter the content. Wyrough & Klein *supra* note 22, at 422-23. Asymmetric or public key systems do allow verification of the integrity of a document because the public key allows one to read and verify the contents of a document, but not alter the document unnoticed. *Id.*

24. Karen Coil, *Digital Signatures: Identity in Cyberspace*," 2 ALA SPECTRUM, Dec. 1997, at 8.

25. Gnoffo, *supra* note 16, at 1065.

26.

> Digital Signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use what is known as "PUBLIC KEY CRYPTOGRAPHY," which employs an algorithm using two different but mathematically related "KEYS," one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively termed an "ASYMMETRIC CRYPTOSYSTEM."

ABA GUIDELINES, *supra* note 2, at 8 (footnote omitted).

27. Interactive video includes the ability to see and hear what is occurring in another location. Video phones and technologies such as cu (?) see me over the Internet are two examples.

wide on the information highway deliver today's precious commodity, information.

> The Internet is already being used for all sorts of exchanges: the purchase of goods and services; the payment of bills; the give and take of confidential information; and even international gambling. Almost any exchange you can think of can be conducted over the NET or "improved" by using the Internet. Before this happens, however, the Internet still needs to pass a simple test. Users must be able to perform transactions that not only satisfy all parties involved, but are legal and binding. Just as laws and statutes outline how the postal system may be used to provide official notice or conduct government business, policymakers must address similar concerns with regard to the Internet.[28]

Currently, the United States government has enacted procurement policies and procedures to help it buy millions of dollars of goods without replicating the wave of paper documents.[29] The guidelines provide for digital exchanges to include a string of characters that verify the legitimacy of the order. The federal government must use the Federal Acquisition Computer Network (FACNET) "whenever practicable or cost effective."[30] Before using FACNET for electronic commerce,[31] the system used to transfer data between computers must ensure "authentication and confidentiality commensurate with the risk and magnitude of the harm from loss, misuse, or unauthorized access to or modification of the information."[32] Note that notaries used to provide authentications. The government has mandated FACNET capability for seventy-five percent of appropriate contracts by January 1, 2000.[33] Additional efforts to use digital signature technology include initiatives by the Internal Revenue

---

28. Richard J. Varn & Rusty Martin, *Unpredictable Opportunities*, STATE LEGISLATURES, Mar. 1, 1996, at 24, 26.

29. These regulations pertaining to the Federal Computer Acquisition Network, as required by section 30 of the Office of Federal Procurement Policy Act are codified at 41 U.S.C. § 426 (1998) and appear at 48 C.F.R. § 4.5000 (1998). President Clinton issued a memorandum October 26, 1993 instructing federal agencies to implement electronic procurement procedures. Memorandum to the Heads of Executive Departments and Agencies on Streamlining Procurement Through Electronic Commerce, 29 WEEKLY COMP. PRES. DOC. 2174-75 (Oct. 26, 1993).

30. 48 C.F.R. § 4.502(a).

31. *Id.* § 4.501. Electronic commerce means:

> a paperless process including electronic mail, electronic bulletin boards, electronic funds transfer, electronic data interchange, and similar techniques for accomplishing business transactions. The use of terms commonly associated with paper transactions (e.g., 'copy', 'document', 'page', 'printed', 'sealed envelope' and 'stamped') shall not be interpreted to restrict the use of electronic commerce.

Id.

32. *Id.* § 4.502(b).

33. 41 U.S.C. § 426(a)(3); 426a(b); 48 C.F.R. § 4.505-3.

Service, the U.S. Postal Service, and the General Services Administration. The Postal Service's opportunity to become a certification authority is particularly interesting.[34] Encryption software is one of the mediums to employ digital signature technology.

II. ENCRYPTION SOFTWARE

Electronic commerce became possible with the advent of simple and effective methods to send and receive secure electronic communications. Encryption technology allows one not only to encode a message, but also to apply a digital signature to the document, which is also encoded. While the digital message might be intercepted by others, only someone holding the correct key can unwrap the signature package to verify the signor, unwrap the encoded message, and verify that the contents of the original package have not been tampered with since being sent into the electronic stream. According to the ABA Signature Guidelines, digital signatures "should indicate who signed a document, message, or record, and should be difficult for another person to produce without authorization."[35] The signature should also identify what is signed, making it impracticable to falsify or alter either the signed matter or the signature without detection.[36] There is a wonderful tutorial on how digital technology works in the ABA Signature Guidelines.[37] Creating and

---

34. *See* James M. Smith, *Mail No One Can Steam Open: Postal Service Will Lock Messages in Electronic Envelopes for Security*, GOV'T COMPUTER NEWS, July 31, 1995, at 90 (quoting Postal Service Vice President Robert Reisner as stating that the Postal Service hopes to become a certification authority); *see also* William Jackson, *Postal Service Gives Signatures a Dry Run In-House*, GOV'T COMPUTER NEWS, Aug. 21, 1995, at 8, (discussing Postal Service plans to become a certification authority).

35. ABA GUIDELINES, *supra* note 2, at 6 (footnotes omitted).

36. *Id.* at 6-7 (footnotes omitted). The omitted footnotes make the point that "paper signature[s] identif[y] the signed matter less than perfectly." *Id.* at 6 n.15.

37. *Id.* at 8-13.

> Electronic signatures are formed by an encryption process. In executing an electronic or digital "signature," special software "reads" a document and "signs" it with a string of electronic numbers known only to the person signing the document. When the document is received, corresponding software "reads" the signature and verifies its authenticity. More technically, a datafile is reduced into a unique number or sequence of bits representing that file, using a mathematical algorithm. When the original file is modified, a unique number is generated and encrypted, using an individual's private key. The result (the electronic signature) is sent with the document. Generating the electronic signature may be accomplished by clicking on an on-screen icon or executing a simple command– the software performs the encryption process.

Richard Raysman & Peter Brown, *Electronic Signatures*, N.Y.L.J., Oct. 30, 1995, at 3, col. 1; *see also* Randy Sabett, *International Harmonization in Electronic Commerce and Electronic Data Interchange: A Proposed Step Toward Signing on the Digital Dotted Line*, 46 AM. U.L. REV. 511, 519 (1996) (discussing the superi-

verifying electronic signatures parallels the legal effects of paper signatures.

> SIGNER AUTHENTICATION: If a public and private key pair is associated with an identified signer, the digital signature attributes the message to the signer. The digital signature cannot be forged, unless the signer loses control of the private key. . .
>
> MESSAGE AUTHENTICATION: The digital signature also identifies the signed message, typically with far greater certainty and precision than paper signatures. Verification reveals any tampering, since the comparison . . . shows whether the message is the same as when signed.
>
> AFFIRMATIVE ACT: Creating a digital signature requires the signor to use the signer's private key. This act can perform the "ceremonial" function of alerting the signer to the fact that the signer is consummating a transaction with legal consequences.
>
> EFFICIENCY: The processes of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuinely the signer's . . . the creation and verification processes are capable of complete automation [and compared] to paper methods such as checking specimen signature cards . . . digital signatures yield a high degree of assurance . . . .[38]

So, who is going safeguard all these public keys and private keys? CyberNotaries, according to the American Bar Association,[39] and certification authorities, according to the States of Florida[40] and Utah.[41] The State statutes envision depositories of keys, where trustees are empowered to verify that a certain key belongs to a certain individual or corporation.[42] The American Bar Association envisions attorneys serving these functions,[43] and others agree:

---

ority of public key cryptography over secret key cryptography).

38. ABA GUIDELINES, *supra* note 2, at 11-12 (footnote omitted). The footnote omitted notes that mechanization of entire process might weaken the ceremonial function. *Id.* at 12 n.28.

39. *Id.* at 31. *See also* David Sommer, *New Legal Code: Sign it by Modem*, TAMPA TRIB., June 3, 1996, at 1 (discussing that the ABA committee predicts cybernotaries will become the "elite among the legal profession").

40. FLA. STAT. ANN. § 282.72 (West Supp. 1997).

41. UTAH STAT. ANN. § 46-3-103, 201 (1997).

42. FLA. STAT. ANN. § 282.72; UTAH STAT. ANN. § 46-3-103. "[N]early forty states have discussed digital signature legislation and 31 have passed at least one piece of legislation relating to digital signatures. Karen Coil, *Digital Signatures: Identity in Cyberspace*, 2 ALA SPECTRUM 8, 9 (Dec. 1997) (citing Albert Gidar & John P. Morgan, *Survey of Electronic and Digital Signature Legislative Initiatives in the United States* (visited March 10, 1998) <http://www.ilpf.org /digsig/digrep.htm>.

43. Actually, the Guidelines provide that "any person who undertakes the functions of a certification authority under these guidelines may become a certification authority." ABA GUIDELINES, *supra* note 2, at 31. But they also provide: "CyberNotaries are attorneys at law admitted to practice in the United States

> [t]he cybernotary will be in a position of heightened responsibility and consequently prestige. These notaries must command the technological knowledge and expertise required to perform computerized notarizations unlike today's notaries who presumably only have to know how to operate a rubber stamp. Similarly, cybernotaries must possess the integrity necessary to conduct on-line interstate and international transactions which, because of their nature, are usually of greater value and consequence than every-day transactions. For these reasons, there is a possibility that only lawyers should fill the role of cybernotary.[44]

Some have suggested that increased technological expertise required of cybernotaries and certification authorities may curtail the number of people needed to authenticate today's digital documents.[45]

> Individuals involved in issuing keys and identifying key recipients, already being called "Certification Authorities" (CAs), will be quite different from yesterday's notary. They will have to be computer knowledgeable and have access to sophisticated computer systems in order to perform their duties. Given these minimum requirements, it is unlikely many of today's notaries will qualify for or have the supporting computer systems necessary to fulfill the CA role. No doubt this will lead to a concentration of digital signature notarial services in the hands of a few highly qualified certification Authorities.[46]

The role of the notary public has not been taken seriously for sometime in the United States. In Latin America and Europe, the notary is held in the same esteem as an attorney or judge.[47] Utah requires certification authorities to be "a human being or any organization capable of signing a document, either legally or as a matter of fact.[48] The certification authority issues a computer-based record which identifies the issuer, names or identifies the subscriber, contains the subscribers public key, and is digitally signed by the certification authority.[49] Certification authorities need not be attorneys. Florida's certification authorities are defined only as a person

---

and qualified to act as a CyberNotary pursuant to specialization rules currently under development in the CyberNotary Committee, Section of Science and Technology of the American Bar Association." *Id.*

44. Gnoffo, supra note 16, at 1096-97 (footnotes omitted); *see also* Shinichi Tsuchiya, *A Comparative Study of the System and Function of the Notary Public in Japan and the United States*, NAT'L NOTARY ASS'N, Jan. 1997, at 18 (stating that cybernotaries should be acquainted with relevant law as well as technology).

45. NOTARY LAW, *supra* note 15, at 500.

46. *Id.*

47. *See* Meg Nugent, *Little-Known, Oft-Needed Notaries Fall Short of Seal of Approval*, STAR-LEDGER, NEWARK, N.J., Feb. 25, 1995, at B1 (quoting Carol Eisman, a spokesman for the National Notary Association).

48. UTAH CODE ANN. § 46-3-103(4), (21) (1997).

49. *Id.* Florida's definition of a certificate is identical. *See* FLA. STAT. ANN. § 282.72(1) (West Supp. 1997) (utilization the same definition as Utah).

who issues a certificate.[50] Germany's Digital Signature Law provides that a certifier "is a natural or legal person which attests to the attribution of public signature keys to natural persons . . . ."[51] The Malaysian Digital Signature Act does not define certification authorities, leaving the definition to regulations.[52] The Act does provide that when a certification authority issues a certificate, the certification authority must "cause the application for the certificate to be certified by a notary public duly appointed . . . ."[53]

International business transactions are increasing. Technology has increased the pace. One might think that the internationalization of business, and the resulting shrinking of the globe, could serve to mitigate the need for notaries. Perhaps, because businesses can rapidly conduct transactions across great distances, often "face-to-face" with sufficient confidence in the identity of the participants, perhaps a notary's authentication may not be necessary. Conversely, international business transactions often involve high stakes, and when opposing parties require authentication in the course of a major transaction, the integrity of each party's identity is paramount. Thus, American notaries will need to become aware of international notarial processes.[54] Notaries in the United States, both paper and cyber will begin to conform to the more stringent requirements of foreign notaries.

> Since notaries play an important role in commerce and law in many foreign countries, the commissioning standards in those nations tend to be much higher than the United States. This is understandable given that the notary position is much more prestigious in those countries. Foreign notaries may well have training in business-related disciplines such as international and contract law. The higher education requirement is necessitated by the duties conferred upon them. The disparity of the notary status in the international arena is a serious issue that must be addressed. Commercial transactions will suffer if foreign businessmen and lawyers continue to look askance at our notarizations. Some curative action

---

50. FLA. STAT. ANN. § 282.72(2).

51. *German Signature Law*, (trans. Christopher Kuner) (visited March 11, 1998) <http://ourworld.compuserv.com/homepages/ckuner/digsig2.htm>.

52. *Digital Signature Bill of 1997* § 5 (visited March 10, 1998) <http://www.jaring.my/webpres/cyberbills/digi2.html#4>.

53. *Id.* § 6(3).

54. Comment, 61 NAT'L NOTARY, Jan. 1998 at 3.

> Every year international notarization issues become more critical as the marketplace expands and the electronic transfer of documents across oceans and continents becomes commonplace. The [National Notary Association] is keenly aware that continuous communication with foreign Notaries is imperative, so that we are all well informed of each other's practices and procedures.

Id. The column goes on to state that the 1998 Conference of Notaries Public to be held in Washington D.C. in May, is entitled "Integrity in the Global Community." *Id.*

might be in order.

> In response, perhaps a special class of notaries certified to deal in international transactions might be created in the United States. The certification could be structured similarly to the Patent Bar. Notaries with the requisite practical experience and educational background could sit for an International Notary Exam. Upon successful completion, a special United States International Notary commission would be granted. Such a system might prosper if it gained international support. Then uniform prerequisites, commissioning standards, and testing services sanctioned by an international body could ensure worldwide acceptance of notarial acts.[55]

III. INTERACTIVE VIDEO

The ability to secure text-based documents with electronic signatures is likely to increase the value of the modern United States notary. It is still unclear whether emerging video technologies will similarly boost the need for electronic authentication expertise. Video magic is more prevalent. Text-based documents and audio-based "documents" such as music on compact discs and other recordings reduced to digital audio technology (DAT) are continually being developed and perfected. To the computer, a bit of information is a bit of information. Computers do not distinguish between bits that make up the text of a document, bits that make up sounds, bits that comprise pictures, and bits that create video. The difference between other forms of media is that reproducing text requires relatively few bits of information, while sound, pictures, and video require even more bits. The density of the medium has slowed the pace of advancing video technology, but technology is rapidly improving. As the ability to move an increasing number of bits of information improves, then video technology–transferring video signals--will improve. Presently, one law professor simultaneously teaches classes to students in separate locations across the United States over the Internet. This type of teaching environment only requires inexpensive software and hardware. The audio is "wanting" and the video is spasmodic, but the classes are successfully being taught.[56]

Today's television is on the brink of extinction as were black-and-white sets yielding to the suddenly colorful NBC peacock in the early 1950s. Digital television programmed in computer code instead of analog signals has been developed. Standards have been adopted, and digital broadcasts are forecasted to begin in some markets by

55. NOTARY LAW, *supra* note 15, at 501.

56. Professor Peter Martin has been teaching such classes for three years. Distance learning is happening throughout the University. A library employee at the University of Arkansas earns his Library degree in part by participating, from Fayetteville, Arkansas, in a class offered in Tulsa, Oklahoma.

the end of 1998. The advent of digital television makes a tremendous stride towards the ultimate merger of the telephone, the computer, and the television into one information center or information utility. The center may have various ports, such as the multiple phone or cable television outlets in our homes today, but the "Information Utility" will combine entertainment and telecommunication functions.

So what? That is the question. So what happens when video moves about the earth with the speed of a telefax? Well, there will be an impact on commerce, and there will be an impact on notaries. The question is: what impact will it have on a notary's acknowledgment responsibilities? We know parties to a transaction are more confident in the transaction when they know the signatures on the document were applied or acknowledged in front of a notary public. The added confidence is because the notary will have taken some steps to determine that the person signing the document (or acknowledging an earlier signature) is who they purport to be. Video technology allows people to see and interact with others anywhere on earth; not as viewing the President on the evening news, but as verbal communication between family, friends, and neighbors on the phone. Callers participate in today's audio phone conversations while viewers only watch a television news program. The opening scenes in Stanley Kubrick's *2001: A Space Odyssey shows a* daddy traveling aboard a spacecraft to the moon calling his daughter to say he is sorry for having to miss her birthday.[57] Daddy and the little girl see and talk to one another. As video technology advances here on earth, it will enable us to participate in distant meetings, just as we now participate in phone calls. We will, in a sense, "be there." Meetings among several people in different locations throughout the country and the world will become routine.

Where will the notary be? Will a notary in Brussels be able to acknowledge an inked signature on a paper copy of a contract in Boise, Idaho? Can the notary see the application of the signature? Well, the answer probably depends upon how comfortable society becomes with the technology. How does one know that the location being viewed is really Boise? How does one know if the person viewed is Sam and not some actor signing Sam's name? How does one know that the whole transmission has not been altered to show Sam signing a contract? Until video signature technology parallel to digital signatures for text is developed, one might always have doubts about the integrity of what appears on the screen. But then, there has always been, and will always remain, a possibility of forgery. Even digital signatures can be compromised if someone gains access to another's private key.

Video conferences routinely occur around the world. In order to

57. 2001: A SPACE ODYSSEY (Metro-Goldwyn-Mayer 1968).

receive a conference's audio-video signal, the receiving station programs their equipment to a pre-ordained "satellite station" much as one may tune a television set to a station to receive ABC's, CBS's, or NBC's evening news. Conference proceedings are often sold; organizers receive payment and provide the satellite address to paying customers. Also, much like premium cable channels scramble television signals today, the conference signal can be scrambled to prevent freeloaders from intercepting the signal, or to prevent unauthorized access to sensitive data. If video technology develops along a similar path, when one receives a video signal by calling up a preordained address, a video phone instead of an audio phone, then people's confidence in the technology should soon parallel our confidence in today's telephone technology. When calling our neighbors, friends, and family, people are confident that they are in fact talking to their intended party. As more and more "face-to-face" interactive discussions occur across the miles, society will gain confidence in the new video technologies. When one "calls" someone in Rome, one will see and hear them in their home or office--just as the little girl heard and saw her daddy on the way to the moon in *2001*.[58]

While contracts generally, and large contracts particularly, are not consummated over the phone often because of Statutes of Fraud concerns, (although to be sure, deals are made over the phone regularly), perhaps in the future when one can see and hear the other party, video calls might allow the completion of long distance contracts. The authentication of the transaction will need to be perfected. One way to accomplish this task might be to electronically capture the signing of an agreement, digitally signing the video in a manner that shows the parties entering into the transaction, and simultaneously locking the image so that any tampering would be detected.

The record of the transaction need not be the equivalent of a video-tape of the signing of documents. With enough speed, interactive video technology will enable corporate counselors for "Megacorp USA" to communicate through video with "Dynaco Incorporated's" attorneys in New Zealand, and together "attend" one meeting. After discussions back and forth, computers will produce text agreeable to both sides, digitally sign the "document," and immediately transmit an electronic copy to both parties. The computer could also capture the visual portion of the meeting when the counselors all agreed to the transaction, and digitally wrap the video portion up with the text.

IV. CONCLUSION

Electronic technology, particularly the ability to quickly alter and move text, audio, and video across the globe, has begun to re-

58. *Id.*

shape the authentication process historically provided by notaries public. Today's commodity is information, and today's notaries must evolve to situate themselves in a position to verify the identities of the information providers. A familiarity with computer technology is a necessity. While much of the digital signature technology can be automated and does not require an engineering degree to operate, a basic understanding of how computers transfer data among other computers is required.

Notaries will also need to keep aware of what is changing internationally. As the globe shrinks, more and more countries may begin to require similar or identical requirements for notary publics. Because more and more transactions will be international in scope, notaries must keep abreast to keep from falling behind.

Finally, while the biggest challenges facing American notaries today is how information has moved from paper to digital formats, and how the shrinking globe may require additional educational and licensing requirements, there still remains many paper documents needing traditional notarial attention. Notaries need to continually improve ways to identify people who ask for their services. For example, one old technology increasingly being used by notaries to identify people is fingerprinting. Once available only to law enforcement agencies, today inexpensive kits are available so that every notary could fingerprint everyone who comes to them for notarial services. Notaries must continue to develop solutions to keep the integrity of signatures on paper documents, while keeping abreast of the changes brought on by the digitization of documents. On all fronts, notaries must continue their vigilance that has kept American commerce relatively safe for over 200 years.