Study K-500 June 26, 1995

Memorandum 95-34

Admissibility of Electronic Documents

INTRODUCTION

The amount of communication through electronic means is growing explosively. Personal computers, facsimiles, e-mail, and the Internet are now routine business tools, and are increasingly used for household purposes as well.

Is there any role for the Law Revision Commission in reforming the law to keep pace with these developments? Just over a year ago, attorney Gerald Genard wrote to the Commission and proposed several specific reforms regarding electronically recorded signatures. The Commission subsequently considered his letter in connection with its annual review of its agenda, and decided to look into the admissibility of electronically recorded documents and signatures as time and resources permitted. (See September 1994 Minutes.)

Having taken a preliminary look at the case law and literature on the topic, as well as pending reform efforts and legislation, it is clear to the staff that others are already active in the area of digital signatures and electronic evidence. As discussed below, however, the Commission may be able to play an important role by comprehensively reviewing the Evidence Code and drafting legislation updating the Code in a systematic manner to accommodate electronic evidence and other new technology.

GROWTH IN USE OF ELECTRONIC DATA

Electronic data is information that is stored in a digital, or electronic, form, such as in a personal computer. The use of electronic data has numerous advantages over a paper-based system, as Professor Hellman of Stanford University recently summarized:

> • *Speed:* Electronic messages move at the speed of light. Paper moves at the speed of the Postal Service, or if premium prices are acceptable, overnight.

> • *Cost:* Faxing a single page across the country costs as much as a first-class stamp. E-mail can send on the order of 100 pages for the same amount.
>
> • *Storage:* An 8-mm tape cartridge that sells for $10 is the size of an audio cassette and can store 10 Gbytes of data, equivalent to 10 million pages of text or a thousand file drawers, each stuffed to the gills.
>
> • *Access:* Electronic files can be accessed more rapidly and more conveniently than paper. When a copy is brought "on-screen," the original resides safely on disk, whereas a paper copy that is accessed is vulnerable to loss or misfiling when returned to storage.
>
> • *Content-Based Access:* Access based on content (e.g., "Find all documents containing the words *National Information Infrastructure*") is not economically feasible with paper documents, but can be accomplished inexpensively with computer-readable information.
>
> • *Reproducibility:* Each copy of a paper document is degraded somewhat, while a tenth-generation copy of a digital document is indistinguishable from the original.

M. Hellman, *Implications of Encryption Policy on the National Information Infrastructure,* The Computer Lawyer, Feb. 1994, at 28.

A dramatic example of the advantages of electronic data comes from a recent study, in which a paralegal was asked to retrieve 20 documents from a collection of 20,000 paper documents. After 67 hours of searching, the paralegal found only 15 of the 20 requested documents. In contrast, when the documents were stored electronically, all 20 of the documents were found within *three seconds.* J.E. Jessen, *Electronic data as evidence: a litigation tool,* 46 Wash. St. Bar News, Oct. 1992, at 40 & n.2.

These advantages are triggering a rapid switch from paper-based to electronic-based communications. "Not since the industrial revolution has the world in which we live seen such drastic, dizzying changes in the way we conduct our businesses and personal lives." Perry & Ballard, *A chip by any other name would still be a potato: the failure of the law and its definitions to keep pace with computer technology,* 24 Tex. Tech. L. Rev. 797, 798 (1993). The increasing use of electronic based communications is undermining a basic assumption underlying

the Uniform Commercial Code and many other legal rules: that commerce generally occurs on paper.

DANGERS OF ELECTRONIC DATA

Perhaps the most significant drawback of electronic data is also one of its chief advantages: an electronic document can be modified in virtually any manner almost instantaneously, with no tell-tale signs. "Because program changes or data manipulations can be accomplished without leaving any trace and without affecting the day-to-day operation of a computer system, both unintentional error and intentional fraud are difficult to discover behind a perfect-looking printout." Peritz, *Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence*, 80 Nw. U. L. Rev. 956, 960 (1986).

The dangers of manipulation are particularly acute with respect to digital signatures and digital photographs. Digital signatures may be placed on documents that the purported author never saw, much less prepared. Similarly, "[c]omputers can alter a photograph beyond recognition with detection nearly impossible." Note, *A Picture is Worth a Thousand Lies: Electronic Imaging and the Future of the Admissibility of Photographs Into Evidence*, 18 Rutgers Computer & Tech. L.J. 365, 374 (1992). For example, a recently settled lawsuit alleged that *Newsday* scanned another company's photo into a computer, electronically edited out certain parts of the landscape, seamlessly introduced new elements into the picture taken from other digitized photos, and then illegally used the altered photo to illustrate a front page article. *Newsday Settles Lawsuit for Digitally Scanned Image*, The Computer Lawyer, Dec.1994, at 21. Photography no longer is "a medium of truth and unassailable accuracy." Note, *supra*, 18 Rutgers Computer & Tech. L.J. at 365.

Electronic data is also vulnerable in other respects: For instance, e-mail messages can be scanned, intercepted and even duplicated, instantly and inexpensively, without any trace. "Approximately 10 billion words of computer-readable messages, such as e-mail, can be scanned for $1, so even if only one message in a million is of interest, $1 worth of scanning produces 10,000 interesting words!" M. Hellman, *supra*, The Computer Lawyer, Feb. 1994, at 28. Further, in computer recordkeeping, updating of records involves replacement and thus loss of intermediate records, unless special steps are taken to preserve

the intermediate data. Additionally, "[s]ince the computer performs a series of tasks as a single simultaneous operation, the number of persons familiar with the recordkeeping process diminishes drastically." Vergari, *Evidential Value and Acceptability of Computer Digital-Image Printouts,* 9 Rutgers Computer & Tech. L.J. 343, 345 (1983).

These drawbacks require consideration in reforming California law to accommodate electronic data, a process that the Legislature has already begun in many different areas. *See, e.g.,* Bus. & Prof. Code § 4036 (defining "electronic transmission prescription" and setting rules for such prescriptions); Code Civ. Proc. §§ 1010.5 (filing court papers by facsimile transmission), 1012.5 (authorizing Judicial Council to study use of facsimile transmission in judicial system), 1013(e), (f) (service of legal papers by facsimile transmission); Educ. Code §§ 51006 (computer education), 92580 *et seq.* (California Institute for Telecommunications and Information Policy Research); Elec. Code § 14950 (election computer vote count program); Fam. Code § 3830 (computer software for support calculations); Gov't Code §§ 6254.9 (computer software as public record), 7527 (contact information for computer-generated letters from state agencies), 10248 (providing legislative information in electronic form), 11700 *et seq.* (electronic data processing); Health & Safety Code §§ 10201.1 (use of computer and telephone facsimile technology for death records), 18080.7(b) (perfecting security interests in mobilehomes by electronic facsimile); Ins. Code § 1194.5 (investment of excess funds in electronic computer or data processing machine); Penal Code §§ 499c (theft of trade secrets on computer), 502 (unauthorized access to computers); Pub. Util. Code § 585 (access to computer models in rate proceedings); Rev. & Tax Code §§ 2503.1-2503.2 (payment of taxes through electronic fund transfers), 18431.2 (use of electronic technology in filing tax returns); Veh. Code § 34505.5(d) (inspection and maintenance records on computer).

EVIDENCE CODE: CHANGES ALREADY MADE TO ACCOMMODATE ELECTRONIC DATA

California's Evidence Code was enacted in 1965 on recommendation of the Law Revision Commission. *See Evidence Code,* 7 Cal. L. Revision Comm'n Reports 1 (1965), enacted as 1965 Cal. Stat. ch. 299. Today, the Code is very much the

same as when it was enacted, although the Legislature has made some changes, for a variety of reasons.

Changes reflecting increasing use of electronic data or other new technology include the following:

> **§ 255. "Original"**
>
> "Original" means the writing itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."
>
> (Added in 1977.)

> **§ 260. "Duplicate"**
>
> A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic rerecording, or by chemical reproduction, or by equivalent techniques which accurately reproduces the original.
>
> (Added in 1977.)

> **§ 1500.5. Computer printouts as best evidence**
>
> Notwithstanding the provisions of Section 1500, a printed representation of computer information or a computer program which is being used by or stored on a computer or computer readable storage media shall be admissible to prove the existence and content of the computer information or computer program.
>
> Computer recorded information or computer programs, or copies of computer recorded information or computer programs, shall not be rendered inadmissible by the best evidence rule. Printed representations of computer information and computer programs will be presumed to be accurate representations of the computer information or computer programs that they purport to represent. This presumption, however, will be a presumption affecting the burden of producing evidence only. If any party to a judicial proceeding introduces evidence that such a printed representation is inaccurate or unreliable, the party introducing it into evidence will have the burden of proving, by a preponderance of evidence, that the printed representation is the best available evidence of the existence and content of the computer information or computer programs that it purports to represent.
>
> (Added in 1983.)

§ 1550. Photographic copies made as business records

A *nonerasable optical image reproduction provided that additions, deletions, or changes to the original document are not permitted by the technology, a* photostatic, microfilm, microcard, miniature photographic, or other photographic copy or reproduction, or an enlargement thereof, of a writing is as admissible as the writing itself if *the* copy or reproduction was made and preserved as a part of the records of a business (as defined by Section 1270) in the regular course of *that* business. The introduction of *the* copy, reproduction, or enlargment does not preclude admission of the original writing if it is still in existence. *A court may require the introduction of a hard copy printout of the document.*

(Enacted in 1965. Amended in 1992 as shown in italics.)

§ 1551. Photographic copies where original destroyed or lost

A print, whether enlarged or not, from a photographic film (including a photographic plate, microphotographic film, photostatic negative, or similar reproduction) of an original writing destroyed or lost after such film was taken *or a reproduction from an electronic recording of video images on magnetic surfaces* is *** admissible as the original writing itself if, at the time of the taking of such film *or electronic recording,* the person under whose direction and control it was taken attached thereto, or to the sealed container in which it was placed and has been kept, or incorporated in the film *or electronic recording,* a certification complying with the provisions of Section 1531 and stating the date on which, and the fact that, it was so taken under his direction and control.

(Enacted in 1965. Amended in 1969 as shown in italics, with asterisks showing where material was deleted.)

EVIDENCE CODE: JUDICIAL RULINGS REGARDING ELECTRONIC DATA

Few reported California cases discuss the admissibility of electronic data. A number of these recite that computer printouts do not violate the best evidence rule. *See* Aguimatang v. California State Lottery, 234 Cal. App. 3d 769, 798, 286 Cal. Rptr. 57 (1991) ("The computer printout does not violate the best evidence rule, because a computer printout is considered an 'original.' (Evid. Code, § 255.)"); People v. Dunlap, 18 Cal. App. 4th 1468, 1477 n.6, 23 Cal. Rptr. 2d 204 (in effect, Evid. Code § 1500.5 "treats computer printouts as original documents for purposes of the best evidence rule").

These and other cases also discuss hearsay issues relating to computer printouts. In *Dunlap,* the court found that the computer printout of appellant's rap sheet met the requirements of Evidence Code Section 1280, the official

records exception to the hearsay rule. People v. Matthews, 229 Cal. App. 3d 930, 280 Cal. Rptr. 134 (1991), also involved computer printouts of rap sheets, but the court found that those rap sheets failed to meet the requirements of Evidence Code Section 1271, the business records exception to the hearsay rule. Neither *Dunlap* nor *Matthews* focuses on issues unique to computer evidence; in *Dunlap* the court made clear that "'the issue [was] not whether the computer can be trusted to reliably duplicate the rap sheet, but, whether the content of the rap sheet is reliable and trustworthy." 18 Cal. App. 4th at 1477 n.6.

In contrast, in People v. Lugashi, 205 Cal. App. 3d 632, 638, 252 Cal. Rptr. 434 (1988), the court considered at length whether "the proponent of computer evidence [must] introduce testimony on the acceptability and reliability of the particular hardware and software, as well as internal maintenance and accuracy checks, as a prerequisite to admissibility under Evidence Code section 1271." The court rejected that contention, explaining: "[W]ith due respect to the learned commentators who have analyzed this issue at their leisure, appellant's proposal could require production of a horde of witnesses representing each department of a company's data processing system, not to rebut an actual attack on the reliability of their data, but merely to meet the minimal requirement for admissibility." *Id.* at 640. The court observed that this would put an unwarranted burden on already crowded trial courts, as well as on small businesses. *Id.* at 640-41.

The court further stated that under appellant's proposal, "only a computer expert, who could personally perform the programming, inspect and maintain the software and hardware, and compare competing products, could supply the required testimony." *Id.* at 640. The court made clear that this was unnecessary: "[A] person who generally understands the system's operation and possesses sufficient knowledge and skill to properly use the system and explain the resultant data, even if unable to perform every task from initial design and programming to final printout, is a 'qualified witness' for purposes of Evidence Code section 1271." *Id.*

Aguimatang v. California State Lottery, 234 Cal. App. 3d 769, 286 Cal. Rptr. 57 (1991), refers to *Lugashi* with approval and resolves another issue relating to admission of computer printouts under the business records exception to the hearsay rule. The appellants in *Aguimatang* argued that certain computer printouts were inadmissible because they were not made at or near the time of the events reflected in the printouts. The court disagreed, pointing out that

although the printouts were not made at the time of the transactions, "the information contained on the computer's magnetic tapes, from which the [printout] is printed, is recorded daily as it is generated." *Id.* at 798. The court further explained:

> [A]lthough to qualify as a business record the "writing" must be made at or near the time of the event, "writing" is not limited to the commonly understood forms of writing but is defined very broadly to include all "means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof." (Evid. Code, § 250.) Here, the "writing" is the magnetic tape. The data entries on the magnetic tapes are made contemporaneously with the Lotto transactions, hence qualify as business records.

Id.

Although the discussions of admissibility of electronic data in *Lugashi* and *Aguimatang* leave many questions unanswered, they are the most thorough such discussions the staff has been able to find in California case law.

GENARD PROPOSAL

San Francisco attorney Gerald Genard wrote the Commission in 1994 regarding electronic signatures and confusion regarding whether such signatures satisfy the best evidence rule and are admissible in evidence. See Exhibit pp. 1-2. He commented:

> The current attempts to deal with admissibility of photographic and computer-generated copies of documents in the Evidence Code (see Sections 1500.5 and 1550) [set forth on pp. 5-6, *supra*] do not address the question of whether electronically recorded signatures (e.g., signatures directly on a remote computer screen or on a document transmitted via a facsimile (fax) machine) are "originals." Indeed, the language of the current Evidence Code sections is so specific in categorizing methods of creating electronic copies that its failure to specifically include the two examples just mentioned leaves doubt as to whether those sections permit such electronic signatures to be admitted into evidence.

He suggested that "given the widespread use of fax machines and the coming paperless environment and use of portable computers in business transactions,"

the Civil Code and Evidence Code should be amended to add sections indicating that

(1) "'written contracts' include contracts where signatures are obtained on computer screens or on faxed documents,"

(2) "in such cases, either a printout of such documentation, in the case of the computer screen example, or the fax received is the original document," and

(3) "the computer screen version or a printout or a fax document is admissible in evidence."

He further explained that "[i]n the use of a faxed document, the original ink signature of the party to be charged would not be needed as long as the other party has a faxed document showing the signature of the party to be charged." Under his proposal, "[t]he signature of each party, appearing on the fax, would be the original for the purpose of contract formation and also for the purpose of the best evidence rule.

PENDING LEGISLATION

AB 1577. Digital Signatures

Mr. Gennard's proposal initially sounds straightforward, but there are a number of complications. First, although the Commission is authorized to study "[w]hether the Evidence Code should be revised," it does not have authority to study contract formation.

More importantly, the Commission has no particular technological expertise and others are already very active in the area of contract formation using digital signatures. In particular, the ABA Information Security Committee is preparing model legislation regarding digital signatures, which would establish rules regarding digital encryption of such signatures. Digital encryption is a means of protecting electronic messages so that only the intended recipients can read them, and of signing such messages in a way permitting recipients to verify that it came from the sender. There are many digital encryption systems, providing varying degrees of security. For a further, but still brief and relatively understandable explanation of digital encryption, see the attached Senate Bill Report on a Washington bill regarding digital signatures (Exhibit pp. 3-7).

Utah has already enacted a digital signature act based on an early draft of the ABA proposal, and similar legislation is pending in other states. Most importantly, however, in February of this year, Assemblywoman Bowen introduced AB 1577, a California bill based on the ABA draft. As initially introduced, AB 1577 was entitled the "California Digital Signature Act" and set forth *very* detailed provisions establishing a complex system for verifying digital signatures. *See* Exhibit pp. 8-40. Legislative Counsel's Digest of that version of the bill explained that under the bill

> [a] digital signature would be a sequence of bits meeting certain encryption requirements, that would be as valid as if it had been written on paper, except in the case of a digital signature that would make a negotiable instrument payable to bearer, which would be void except to effectuate a funds transfer or a transaction between financial institutions. The bill would also set forth the effect of certain actions taken with respect to digital signatures.

See Exhibit p. 8.

AB 1577 has since been amended and greatly watered down. As amended on June 19, 1995, it consists of but one proposed new section of the Government Code, which would provide that in any transaction in which a public entity is a party, at the option of the parties, a digital signature may be used and would have the same force and effect as a manual signature. The section would set certain requirements for digital signatures, including a requirement that they conform to regulations adopted by the Secretary of State. See Exhibit pp. 41-42. The staff is trying to ascertain the reasons for this substantial change. One reason may be that the ABA has not yet finalized its model legislation.

Other Pending Legislation Relating to Evidentiary Rules for Electronic Data

Senator Calderon has introduced two bills, SB 1034 and SB 926 that would, among other things, amend Evidence Code Section 250, which defines the term "writing." *See* Exhibit pp. 43-49. SB 926 has not been moving forward, but SB 1034 appears well on the way to enactment. It would amend Section 250 to expressly include "data compilations" as "writings." The amendment would thus clarify what the court inferred in *Aguimatang,* that the term "writing" encompasses information stored on computer. As explained in *Aguimatang,* this is important because the business records and official records exceptions to the hearsay rule apply only to "writings" made "at or near" the time of the events

reflected. By expressly providing that a data compilation is a "writing," the amendments would make clear that recording information on computer "at or near" the time of the events reflected is enough to satisfy the hearsay requirements; it is not necessary to produce a hard copy of the information "at or near" the time of the events.

OPTIONS

(1) Drop the Topic (Admissibility of Electronically Recorded Documents and Signatures) from the Commission's Current List of Priorities

What are the Commission's options regarding the topic of admissibility of electronically recorded documents and signatures? One option would be for the Commission to drop the topic from its list of current priorities, while still retaining authority to study "[w]hether the Evidence Code should be revised."

In light of the Commission's limited resources and limited technological expertise, as well as the work being done by others (most notably Assemblywoman Bowen's efforts to implement the work of the ABA Information Security Committee, and Senator Calderon's pending bill changing Evidence Code Section 250's definition of "writing"), this option has some appeal.

On the other hand, however, the work of the ABA Information Security Committee has not focused on evidentiary issues raised by electronic evidence. San Francisco attorney Charles Miller (a member of that committee whose name the staff obtained from Assemblywoman Bowen's office) reports that some members of the committee have done a little looking at evidentiary issues, but those issues have not been, and, at least in the near future, are not going to be the focus of the committee's work on electronic evidence. He would welcome having the Law Revision Commission involved in the area.

(2) Make Piecemeal Changes in the Evidence Code To Accommodate Electronic Data as the Need Appears

Another option would be for the Commission to look into specific evidentiary issues regarding electronic data as the need appears. For example, the Commission could make changes in the best evidence rule along the lines suggested by Mr. Genard. The Commission could also consider broadening Evidence Code Section 1550 to more readily accommodate new types of technology. Compare its very specific language added in 1992 regarding "[a]

nonerasable optical image reproduction," to the broader language in the Washington statute set out below it:

> **Cal. Evid. Code § 1550. Photographic copies made as business records**
>
> A nonerasable optical image reproduction provided that additions, deletions, or changes to the original document are not permitted by the technology, a photostatic, microfilm, microcard, miniature photographic, or other photographic copy or reproduction, or an enlargement thereof, of a writing is as admissible as the writing itself if the copy or reproduction was made and preserved as a part of the records of a business (as defined by Section 1270) in the regular course of that business. The introduction of the copy, reproduction, or enlargment does not preclude admission of the original writing if it is still in existence. A court may require the introduction of a hard copy printout of the document.

> **Wash. Rev. Code Ann. § 5.46.010. Copies of business and public records as evidence**
>
> If any business, institution, member of a profession or calling or any department or agency of government, in the regular course of business or activity has kept or recorded any memorandum, writing, entry, print, representation or combination thereof, of any act, transaction, occurrence or event, and in the regular course of business has caused any or all of the same to be recorded, copied or reproduced by any photographic, photostatic, microfilm, microcard, miniature photographic, optical imaging, ***or other process which accurately reproduces or forms a durable medium for so reproducing the original,*** the original may be destroyed in the regular course of business unless the same is an asset or is representative of title to an asset held in a custodial or fiduciary capacity or unless its preservation is required by law. Such reproduction, when satisfactorily identified, is as admissible in evidence as the original itself in any judicial or administrative proceeding whether the original is in existence or not and an enlargement or facsimile of such reproduction is likewise admissible in evidence if the original reproduction is in existence and available for inspection under direction of court. The introduction of a reproduced record, enlargement or facsimile, does not preclude admission of the original.

[Emph. added.] Changes like this would require relatively little Commission resources, and would improve the Evidence Code to some degree. There is some danger, however, that piecemeal changes like these, coupled with piecemeal

changes instigated by others, may not result in a consistent overall approach to electronic data and other forms of new technology in the Evidence Code.

(3) Undertake a Systematic Review of the Evidence Code and Prepare a Comprehensive Recommendation Adapting the Code to the Increasing Use of Paperless Communications

A further option would be to reexamine the Evidence Code, particularly the portions relating to documentary evidence, in a more comprehensive manner in light of the advent of electronic data and other paperless means of communication. As the original drafter of the Evidence Code and numerous other recommendations relating to evidentiary rules, the Commission is a natural choice for such an effort. Moreover, the virtual explosion in use of electronic means of communication would make such work very timely, and may save trial judges and litigants countless hours and much expense that would otherwise be spent resolving such issues on a case-by-case basis.

The Commission could undertake this type of effort in a number of different ways. One possibility would be to consider each new form of technology (facsimiles, e-mail, digital photographs, computer printouts generated for litigation purposes, other computer printouts, etc.) separately. It may prove challenging, however, to identify which types of technology merit consideration, to account for overlapping categories, and to analyze the evidentiary issues in this manner.

Another possibility would be to consider the issues as the Commission originally considered them in preparing the Evidence Code, by type of evidentiary rule (e.g., hearsay rule). Most of the issues relating to electronic evidence seem to arise in the following areas:

(1) **Authentication of documents.** Given the ease with which a digital signature can be placed on documents, are new safeguards necessary in assessing the authenticity of documents? Even if traditional methods of authentication remain appropriate, should there be new rules, such as a rule affording a presumption of authenticity to a document bearing a digital signature meeting certain encryption requirements? If so, should such rules be set forth in the Evidence Code, or should the Evidence Code merely give an organization such as the Secretary of State or the Judicial Council authority to promulgate such rules? An advantage of the latter approach would be that rules of such an

organization could be changed more quickly and readily than statutes to accommodate rapidly changing technology. Additionally, the task of preparing specific rules for specific types of new technology would then fall to an organization with technological expertise to handle it, rather than to the Commission.

(2) **Best evidence rule.** The best evidence rule applies only to documents, not to other types of evidence. It is already riddled with exceptions. Given the increasing difficulty in differentiating between "documents" and other types of evidence, as well as the ease with which computers and other types of technology can generate duplicates essentially indistinguishable from originals, does the best evidence rule continue to make sense, or does it just result in waste of effort? If it remains useful, should it be modified to account for new forms of technology?

(3) **Business and official records exceptions to the hearsay rule.** As the court recognized in *Lugashi,* courts and commentators have proposed various different approaches for evaluating whether computer records satisfy the business records and official records exceptions to the hearsay rule. There is a lot to be said for the approach adopted in *Lugashi,* — perhaps it should be codified, or perhaps some other approach would be even better.

Perhaps the Commission could consider each of these areas in order, and then prepare a comprehensive recommendation covering all three areas, as well as any additional portions of the Evidence Code that seem to warrant attention in light of the increasingly paperless evidentiary world.

RECOMMENDATION

The staff sees advantages to all three of the options proposed above, but for the reasons expressed above, it leans towards Option #3 (undertaking a systematic review of the Evidence Code and preparing a comprehensive recommendation adapting the Code to the increasing use of paperless communications). There is much to be said for keeping evidentiary rules sufficiently generic to readily accommodate new technology. The Code already follows that approach in many respects, but it has been thirty years since it was enacted and the world of communications has changed dramatically. Revisiting the Code with these

changes in mind, and focusing in particular on authentication, the best evidence rule, and the business records and official records exceptions to the hearsay rule (perhaps in that order), may yield many benefits. Although the Commission lacks technological expertise, it may be possible to find a volunteer consultant to help overcome that problem. Also, if the Commission adopts a generic approach, it may prove unnecessary to do much technologically precise drafting.

Respectfully submitted,

Barbara S. Gaal
Staff Counsel

Law Revision Commission
RECEIVED
MAY - 4 1994
File:

564 Mission Street #609
San Francisco, CA 94105-2918
May 3, 1994

Law Revision Commission
State of California
4000 Middlefield Road #D-2
Palo Alto, CA 94303-4739

Ladies and Gentlemen:

Re: Suggested Amendment to Civil and Evidence Codes Covering "Original" Documents and Signatures

The current attempts to deal with admissibility of photographic and computer-generated copies of documents in the Evidence Code (see Sections 1500.5 and 1550) do not address the question of whether electronically recorded signatures (e.g., signatures directly on a remote computer screen or on a document transmitted via a facsimile (fax) machine) are "originals." Indeed, the language of the current Evidence Code sections is so specific in categorizing methods of creating electronic copies that its failure to specifically include the two examples just mentioned leaves doubt as to whether those sections permit such electronic signatures to be admitted into evidence.

My suggestion is that given the widespread use of fax machines and the coming paperless environment and use of portable computers in business transactions, the Civil Code and Evidence Code be amended to add sections indicating that "written contracts" include contracts where signatures are obtained on computer screens or on faxed documents, that, in such cases, either a printout of such documentation, in the case of the computer screen example, or the fax received is the original document, and that the computer screen version or a printout or a fax document is admissible in evidence. In the use of a faxed

document, the original ink signature of the party to be charged would not be needed as long as the other party has a faxed document showing the signature of the party to be charged. The signature of each party, appearing on the fax, would be the original for the purpose of contract formation and also for the purpose of the best evidence rule. This is a particularly important rule where each contracting party signs and faxes a duplicate original to the other.

Very truly yours,

Gerald H. Genard

Gerald H. Genard

GHG:tln

STATE OF WASHINGTON: DIGITAL SIGNATURES

SENATE BILL REPORT
SB 5969
As of February 28, 1995

Title: An act relating to ensuring security of document transmissions using common carrier, broadcast, and computer technologies.

Brief Description: Attempting to minimize the incidence of forged digital signatures and foster the verification of digital signatures.

Sponsors: Senator Sutherland.

Brief History: Committee Activity: Energy, Telecommunications & Utilities: 2/28/95.

SENATE COMMITTEE ON ENERGY, TELECOMMUNICATIONS & UTILITIES

Staff: David Danner (786-7784)

Background: Digital encryption allows a person to protect a message so that only the intended recipients can read it, and to digitally sign it so that people can verify that it came from the sender. Many digital encryption systems exist or are in development.

Dual key encryption uses two digital codes, or "keys": a secret key and a public key. The user keeps the secret key confidential, and shares the public key to friends, business associates, and others to whom confidential messages are sent. Each key can read a message that has been encrypted by the other. If a person wants to digitally sign a message, he or she may use the secret key to create a signature. The recipient then uses the sender's public key to verify the source of the message.

Private companies, including telecommunications companies, utility companies, banks, law firms, and insurance companies, provide or plan to provide encryption services either as part of their existing services or as a commercial enterprise. In addition, government agencies such as courts or tax offices will have increased need in the course of their own work to protect security of electronic documents.

Unless the integrity of digital transmissions can be assured, on-line services cannot be used for such tasks as court filings, financial transactions, or sensitive personal or business correspondence.

In addition, digital signatures raise several legal questions, such as their validity under the statute of frauds and the liability for damages when the security of an

electronic transmission is violated.

Summary of Bill: Rules are established governing the creation of a key pair. The Department of Licensing (DOL) is directed to license "certification authorities," which are private companies, government agencies, and individuals who certify the integrity of a digitally signed document in a manner that can be readily verified. This provides a threshold level of assurance that a digital signature is legally valid.

Parties may specify in their dealings with each other that their digital signatures are verifiable by a certification authority.

The qualifications for certification authorities are set forth. They must be licensed attorneys, financial institutions, trust companies, insurance and title insurance companies, and state agencies; all must be notaries public. Certification authorities may not employ persons who have been convicted of felonies.

Licensing of certification authorities is limited to licensing only those persons demonstrating financial responsibility by posting surety bonds or letters of credit. Bonds or letters of credit assures that a certification authority is able to pay damages for any errors or omissions.

A certificate issued by a certification authority contains the following information: (1) the name of the subscriber; (2) the public key corresponding to a private key held by the subscriber; (3) a brief description of the algorithms with which the public key is intended to be used; (4) the serial number of the certificate; (5) the date and time on which the certificate is issued and accepted, and the date it expires; (6) the name of the certification authority; (7) the recommended reliance limit for transactions relying on the certificate; and (8) other information which DOL may require.

Certification authorities must be audited annually, and must disclose certain information for inclusion in a DOL database. This information includes relevant information about the authority's regulatory record, its solvency, and financial and legal ability to conduct business.

DOL may investigate the activities of a certification authority for noncompliance, and revoke or suspend its license. DOL may also expressly authorize that persons may obtain punitive damages when a certification authority does not comply with a DOL order resulting in loss to a party that reasonably relied upon the certification authority.

Certification authorities must retain records documenting compliance with these provisions. A certification authority wishing to cease acting as such must provide notice. It must revoke outstanding certificates, and make arrangements with a substitute entity to continue acting on a subscriber's behalf.

A company acting as a certification authority may not conduct business in a way that creates a commercially unreasonable risk of loss to its clients. A certification authority may issue a certificate only after ascertaining critical facts about the subscriber's identity and the dual key numbers. When a certificate is requested by an agent or apparent agent of a subscriber, the certification authority may issue a certificate only after giving the subscriber 10 days' written notice.

A subscriber, by accepting a certificate, warrants that the information contained thereon is true, that the digital signature is valid, and that no unauthorized person has access to the private key. It is the subscriber's duty to exercise reasonable care to keep the private key confidential. The private key is the property of the subscriber, and when the certification authority holds the private key, it acts as a fiduciary to the subscriber.

By issuing a certificate, the licensed certification authority warrants to the subscriber that the certificate contains no information known to be false, and is within the bounds of the certification authority's powers. These warranties may not be limited by contract.

A certification authority must notify subscribers when it becomes aware of any facts that may affect the validity or reliability of an issued certificate. The certification authority must warrant to all who justifiably rely upon a certificate that it complies with all requirements in issuing and publishing the certificate.

A certification authority may temporarily suspend a certificate when it suspects that a private key has been compromised. It may permanently revoke a certificate upon (1) request and payment of a fee by the subscriber, (2) the death of the subscriber, and (3) a determination that the certificates are unreliable, in which case it must compensate the subscriber for any loss, unless the parties' contract states otherwise.

A certification authority must publish notice of a certificate's revocation with the repository named in the certificate, and all other repositories where the certificate may be published. Where a certificate is revoked, a subscriber is no longer bound by warranties he or she makes, and is no longer bound to keep the private key secret. At the same time, the certification authority is no longer bound by its warranties.

Each certificate must bear an expiration date, which must be no later than three years after issuance. When a certificate expires, both the subscriber and the certification authority cease to be bound by their warranties to the other, and the certification authority is discharged of its duties.

A licensed certification authority is not liable for any loss caused by a false or forged digital signature if it complies with all material requirements of the act. In addition, a

certification authority is not liable for failure to comply for more than the amount specified in the certificate as the recommended reliance limit. A certification authority is not liable for punitive damages, except for noncompliance with a DOL order in which DOL expressly authorizes punitive damages.

Notwithstanding any provision contained in a surety bond or letter of credit required under this bill, a person may recover from the surety or letter of credit the full amount of the claim, or, if there is more than one claim during the term of the bond or letter of credit, a ratable share up to a maximum liability equal to the face amount of the bond or letter of credit. Claimants may recover successively on the same guaranty, provided the total liability to all claimants during the term of the bond or letter of credit does not exceed the face amount of the guarantee.

There is a rebuttable legal presumption that a certificate in a recognized repository which is not revoked, suspended or expired is: (1) a valid acknowledgment of a digital signature verified using the public key set forth in the certificate, regardless of whether any words of express acknowledgment appear alongside the digital signature in any document, and (2) affixed with the subscriber's intent to authenticate the message and to be bound by the contents of the message.

If a signature is time-stamped by a repository, the time stamp is prima facie evidence that the time-stamped signature takes effect on the date and time indicated. However, this does not preclude a fact-finder from concluding, based on other evidence, that the date and time of the signature are different than that shown by the time-stamp.

A digitally signed document is as valid as if it is written on paper. However, nothing in this section limits the authority of the Department of Revenue to prescribe the form of tax returns or other documents filed with DOR.

A digital signature is void if it makes a negotiable instrument payable to bearer, except when the signature effectuates a transfer between banks or financial institutions and other non- consumers.

The Department of Licensing must act as a certification authority, and may issue, suspend, or revoke certificates in the manner prescribed for licensed certification authorities. In addition, DOL must maintain an on-line database as a repository for: (1) certificates published in the repository by licensed certification authorities; (2) a list of all licensed certification authorities and their public keys; (3) a list of all certification authorities whose licenses are revoked or suspended, and the grounds for such actions; (4) certification authority disclosure records; (5) notices of suspended or revoked certificates; (6) references to recognized repositories; (7) information required to be kept by a recognized repository; and (8) other data as determined by DOL.

DOL must also maintain a system for date-stamping digital signatures. DOL may promulgate rules with respect to the designing and implementing this chapter, and may, by rule, set appropriate fees.

DOL may recognize a repository maintained by a certification authority if that repository is similar to its own.

A recognized repository is not liable for loss resulting from misrepresentation in a certificate published by a certification authority, or from accurately recording information required to be published by a certification authority, county or court clerk, or DOL. A repository is liable for failing to record publication of a certificate, or a suspension or revocation, only if a commercially reasonable time elapses for processing the publication.

An exemption to the state Open Records Act is created for all records that disclose encryption codes or records jeopardizing the security of an issued certificate.

Appropriation: None.

Fiscal Note: Not requested.

Effective Date: Ninety days after adjournment of session in which bill is passed.

SB 1034 Writings: electronic media.

BILL NUMBER: SB 1034 AMENDED 05/09/95

AMENDED IN SENATE MAY 9, 1995
AMENDED IN SENATE APRIL 27, 1995

INTRODUCED BY Senator Calderon

FEBRUARY 24, 1995

An act to amend Section 2031 of the Code of Civil Procedure, and to amend Section 250 of the Evidence Code, relating to evidence.

LEGISLATIVE COUNSEL'S DIGEST

SB 1034, as amended, Calderon. Evidence: electronic media.

(1) Existing law provides that parties to a civil action may obtain discovery by the inspection of documents, tangible things, or land or other property in the possession, custody, or control of any other party to the action, as specified. Existing law specifies how demanded documents are to be produced to the demanding party. Existing law requires, if necessary, the responding party at the reasonable expense of the demanding party to, through reasonable detection devices, translate any data compilations included in the demand into reasonably usable form.

This bill would revise and recast this later provision to delete the requirement that the translation occur at the reasonable expense of the demanding party and to require the responding party to provide any and all information necessary to understand and utilize the data compilations, as specified. *The bill would authorize the court to allocate between the parties the cost of translation and providing information necessary to understand the data compilations, as specified.* This bill would also provide that, to the extent proprietary information is ordered produced under this provision, the court shall issue a strict protective order, as specified.

(2) Existing provisions of the Evidence Code define "writing" for its purposes to mean handwriting, typewriting, printing, photostating, photographing, and every other means of recording upon any tangible thing any form of communication or representation, as specified.

This bill would specify that a data compilation is included within this definition of "writing."

This bill would also make a legislative finding and declaration that this act is declarative of existing law.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

SECTION 1. The Legislature hereby finds and declares all of the following:

(a) That computerized recordkeeping has replaced less accurate and more burdensome manual recordkeeping systems to the point where businesses and individuals rely primarily, if not exclusively, on computer information in conducting their commercial and personal affairs.

(b) That from the largest corporations to the smallest families, people are using computers to cut costs, improve production, enhance communication, store countless data, and improve capabilities in every aspect of human and technological development.

(c) That computers have become so commonplace that most lawsuits involve discovery of some type of computer-stored information.

(d) That the development of new technologies for using, storing, and transmitting information allows parties to test the rules of disclosure or discovery by using these new technologies as a basis for withholding information otherwise falling within the scope of subdivision (a) of Section 2017 of the Code of Civil Procedure.

(e) That it would be a dangerous development in the law if new techniques for easing the use of information become a hindrance to discovery or disclosure in litigation.

(f) That the principle embodied in California's discovery statutes is that information which is stored, used, or transmitted in new forms, including computer data, should be available through discovery with the same openness as traditional forms.

(g) That case law interpreting applicable provisions of the federal Rules of Civil Procedure relating to computer discovery amply illustrate this point.

(h) That the new developments in computer technology require greater clarity in California's discovery statutes to keep pace with these advances.

SEC. 2. Section 2031 of the Code of Civil Procedure is amended to read:

2031. (a) Any party may obtain discovery within the scope delimited by Section 2017, and subject to the restrictions set forth in Section 2019, by inspecting documents, tangible things, and land or other property that are in the possession, custody, or control of any other party to the action.

(1) A party may demand that any other party produce and permit the party making the demand, or someone acting on that party's behalf, to inspect and to copy a document that is in the possession, custody, or control of the party on whom the demand is made.

(2) A party may demand that any other party produce and permit the party making the demand, or someone acting on that party's behalf, to inspect and to photograph, test, or

sample any tangible things that are in the possession, custody, or control of the party on whom the demand is made.

(3) A party may demand that any other party allow the party making the demand, or someone acting on that party's behalf, to enter on any land or other property that is in the possession, custody, or control of the party on whom the demand is made, and to inspect and to measure, survey, photograph, test, or sample the land or other property, or any designated object or operation on it.

(b) A defendant may make a demand for inspection without leave of court at any time. A plaintiff may make a demand for inspection without leave of court at any time that is 10 days after the service of the summons on, or in unlawful detainer actions within five days after service of the summons on or appearance by, the party to whom the demand is directed, whichever occurs first. However, on motion with or without notice, the court, for good cause shown, may grant leave to a plaintiff to make an inspection demand at an earlier time.

(c) A party demanding an inspection shall number each set of demands consecutively. In the first paragraph immediately below the title of the case, there shall appear the identity of the demanding party, the set number, and the identity of the responding party. Each demand in a set shall be separately set forth, identified by number or letter, and shall do all of the following:

(1) Designate the documents, tangible things, or land or other property to be inspected either by specifically describing each individual item or by reasonably particularizing each category of item.

(2) Specify a reasonable time for the inspection that is at least 30 days after service of the demand, or in unlawful detainer actions at least five days after service of the demand, unless the court for good cause shown has granted leave to specify an earlier date.

(3) Specify a reasonable place for making the inspection, copying, and performing any related activity.

(4) Specify any related activity that is being demanded in addition to an inspection and copying, as well as the manner in which that related activity will be performed, and whether that activity will permanently alter or destroy the item involved.

(d) The party demanding an inspection shall serve a copy of the inspection demand on the party to whom it is directed and on all other parties who have appeared in the action.

(e) When an inspection of documents, tangible things or places has been demanded, the party to whom the demand has been directed, and any other party or affected person or organization, may promptly move for a protective order. This motion shall be accompanied by a declaration stating facts showing a reasonable and good faith attempt at an informal resolution of each issue presented by the motion.

The court, for good cause shown, may make any order that justice requires to protect any

party or other natural person or organization from unwarranted annoyance, embarrassment, or oppression, or undue burden and expense. This protective order may include, but is not limited to, one or more of the following directions:

(1) That all or some of the items or categories of items in the inspection demand need not be produced or made available at all.

(2) That the time specified in subdivision (h) to respond to the set of inspection demands, or to a particular item or category in the set, be extended.

(3) That the place of production be other than that specified in the inspection demand.

(4) That the inspection be made only on specified terms and conditions.

(5) That a trade secret or other confidential research, development, or commercial information not be disclosed, or be disclosed only to specified persons or only in a specified way.

(6) That the items produced be sealed and thereafter opened only on order of the court.

If the motion for a protective order is denied in whole or in part, the court may order that the party to whom the demand was directed provide or permit the discovery against which protection was sought on terms and conditions that are just.

The court shall impose a monetary sanction under Section 2023 against any party, person, or attorney who unsuccessfully makes or opposes a motion for a protective order, unless it finds that the one subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust.

(f) The party to whom an inspection demand has been directed shall respond separately to each item or category of item by a statement that the party will comply with the particular demand for inspection and any related activities, a representation that the party lacks the ability to comply with the demand for inspection of a particular item or category of item, or an objection to the particular demand.

In the first paragraph of the response immediately below the title of the case, there shall appear the identity of the responding party, the set number, and the identity of the demanding party. Each statement of compliance, each representation, and each objection in the response shall bear the same number and be in the same sequence as the corresponding item or category in the demand, but the text of that item or category need not be repeated.

(1) A statement that the party to whom an inspection demand has been directed will comply with the particular demand shall state that the production, inspection, and related activity demanded will be allowed either in whole or in part, and that all documents or things in the demanded category that are in the possession, custody, or control of that party and to which no objection is being made will be included in the production.

Any documents demanded shall either be produced as they are kept in the usual course of

business, or be organized and labeled to correspond with the categories in the demand. If necessary, the responding party shall, through detection devices, translate any data compilations included in the demand into reasonably usable form and produce any and all information necessary to understand and utilize these data compilations including, but not limited to, material relating to the recordholder's computer hardware, custom or proprietary software programs, the computer programming techniques employed in connection with the relevant data, the principles governing the structure of the stored data, and the operation of the data processing system, the underlying data used to compose statistical analyses, the methods used to select, categorize, and evaluate the data, and all of the computer outputs. To the extent proprietary information is ordered produced under this paragraph, the court shall do so through the issuance of a strict protective order restricting the use of this information exclusively to the subject matter of the litigation that is the basis of the order. *The court may, in its discretion, allocate between the parties the expense of translating data compilations and of producing information necessary to understand and utilize data compilations, as justice requires.*

(2) A representation of inability to comply with the particular demand for inspection shall affirm that a diligent search and a reasonable inquiry has been made in an effort to comply with that demand. This statement shall also specify whether the inability to comply is because the particular item or category has never existed, has been destroyed, has been lost, misplaced, or stolen, or has never been, or is no longer, in the possession, custody, or control of the responding party. The statement shall set forth the name and address of any natural person or organization known or believed by that party to have possession, custody, or control of that item or category of item.

(3) If only part of an item or category of item in an inspection demand is objectionable, the response shall contain a statement of compliance, or a representation of inability to comply with respect to the remainder of that item or category. If the responding party objects to the demand for inspection of an item or category of item, the response shall (A) identify with particularity any document, tangible thing, or land falling within any category of item in the demand to which an objection is being made, and (B) set forth clearly the extent of, and the specific ground for, the objection. If an objection is based on a claim of privilege, the particular privilege invoked shall be stated. If an objection is based on a claim that the information sought is protected work product under Section 2018, that claim shall be expressly asserted.

(g) The party to whom the demand for inspection is directed shall sign the response under oath unless the response contains only objections. If that party is a public or private corporation or a partnership or association or governmental agency, one of its officers or agents shall sign the response under oath on behalf of that party. If the officer or agent signing the response on behalf of that party is an attorney acting in that capacity for a party, that party waives any lawyer-client privilege and any protection for work product under Section 2018 during any subsequent discovery from that attorney concerning the identity of the sources of the information contained in the response. The attorney for the responding party shall sign any responses that contain an objection.

(h) Within 20 days after service of an inspection demand, or in unlawful detainer actions within five days of an inspection demand, the party to whom the demand is directed shall

serve the original of the response to it on the party making the demand, and a copy of the response on all other parties who have appeared in the action, unless on motion of the party making the demand the court has shortened the time for response, or unless on motion of the party to whom the demand has been directed, the court has extended the time for response. In unlawful detainer actions, the party to whom the demand is directed shall have at least five days from the date of service of the demand to respond unless on motion of the party making the demand the court has shortened the time for the response.

(i) The party demanding an inspection and the responding party may agree to extend the time for service of a response to a set of inspection demands, or to particular items or categories of items in a set, to a date beyond that provided in subdivision (h). This agreement may be informal, but it shall be confirmed in a writing that specifies the extended date for service of a response. Unless this agreement expressly states otherwise, it is effective to preserve to the responding party the right to respond to any item or category of item in the demand to which the agreement applies in any manner specified in subdivision (f).

(j) The inspection demand and the response to it shall not be filed with the court. The party demanding an inspection shall retain both the original of the inspection demand, with the original proof of service affixed to it, and the original of the sworn response until six months after final disposition of the action. At that time, both originals may be destroyed, unless the court, on motion of any party and for good cause shown, orders that the originals be preserved for a longer period.

(k) If a party to whom an inspection demand has been directed fails to serve a timely response to it, that party waives any objection to the demand, including one based on privilege or on the protection for work product under Section 2018. However, the court, on motion, may relieve that party from this waiver on its determination that (1) the party has subsequently served a response that is in substantial compliance with subdivision (f), and (2) the party's failure to serve a timely response was the result of mistake, inadvertence, or excusable neglect.

The party making the demand may move for an order compelling response to the inspection demand. The court shall impose a monetary sanction under Section 2023 against any party, person, or attorney who unsuccessfully makes or opposes a motion to compel a response to an inspection demand, unless it finds that the one subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust. If a party then fails to obey the order compelling a response, the court may make those orders that are just, including the imposition of an issue sanction, an evidence sanction, or a terminating sanction under Section 2023. In lieu of or in addition to that sanction, the court may impose a monetary sanction under Section 2023.

(l) If the party demanding an inspection, on receipt of a response to an inspection demand, deems that (1) a statement of compliance with the demand is incomplete, (2) a representation of inability to comply is inadequate, incomplete, or evasive, or (3) an objection in the response is without merit or too general, that party may move for an order compelling further response to the demand. This motion (1) shall set forth specific facts showing good cause justifying the discovery sought by the inspection demand, and (2) shall

be accompanied by a declaration stating facts showing a reasonable and good faith attempt at an informal resolution of any issue presented by it.

Unless notice of this motion is given within 45 days of the service of the response, or any supplemental response, or on or before any specific later date to which the demanding party and the responding party have agreed in writing, the demanding party waives any right to compel a further response to the inspection demand.

The court shall impose a monetary sanction under Section 2023 against any party, person, or attorney who unsuccessfully makes or opposes a motion to compel further response to an inspection demand, unless it finds that the one subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust.

If a party fails to obey an order compelling further response, the court may make those orders that are just, including the imposition of an issue sanction, an evidence sanction, or a terminating sanction under Section 2023. In lieu of or in addition to that sanction, the court may impose a monetary sanction under Section 2023.

(m) If a party filing a response to a demand for inspection under subdivision (f) thereafter fails to permit the inspection in accordance with that party's statement of compliance, the party demanding the inspection may move for an order compelling compliance.

The court shall impose a monetary sanction under Section 2023 against any party, person, or attorney who unsuccessfully makes or opposes a motion to compel compliance with an inspection demand, unless it finds that the one subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust.

If a party then fails to obey an order compelling inspection, the court may make those orders that are just, including the imposition of an issue sanction, an evidence sanction, or a terminating sanction under Section 2023. In lieu of or in addition to that sanction, the court may impose a monetary sanction under Section 2023.

SEC. 3. Section 250 of the Evidence Code is amended to read:

250. "Writing" means handwriting, typewriting, printing, photostating, photographing, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, symbols, or data compilations, or combinations thereof.

~~SEC. 2.~~

SEC. 4. The Legislature finds and declares that the provisions of this act are declarative of existing law.