ARTICLE:

BRANDEIS BRIEF IN THE CASE OF *IN RE WILLIAM FRENCH ANDERSON*

A Brandeis Brief is a brief to a court that combines evidence, testimony and arguments in relation to a matter, together with legal argument. The Brandeis Brief is named after Louis D. Brandeis, who was asked by Florence Kelley and Josephine Goldmark in 1907 to compile statistics from medical and sociological journals and list citations to the articles in representing the state of Oregon in the case of *Muller v. Oregon,* 208 US 412 in the United States Supreme Court, involving the constitutionality of limiting hours for female laundry workers. This document was of utmost significance in the case, and was the first brief submitted to the Supreme Court that relied primarily on extra-legal data to prove an argument.[1]

The Brandeis Brief set out below in full was prepared by George L. Paul, who circulated it to all of those listed at the end of the Brief for their comments. Mr Paul was retained as Co-Counsel in a Writ of Habeas Corpus proceeding in California. The client was the subject of a covert operation that involved the use of a recording device, that had as one of its capabilities the recording to a WORM drive. It was the policy of the Sherriffs Department that this authenticity protocol be used. WORM drives are not perfect, but arguably they are better than nothing.

The recording was intentionally made without the use of the authenticity protocol, and was instrumental in the conviction of a crime. The client's position is that the recording was edited and his lawyers have marshalled substantial evidence to that effect. His original lawyer did not object to the admission of the recording into evidence. The client now wants a new trial, on the basis that his lawyer did not protect his rights. The original lawyer did nothing relating to the authenticity of recording.

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA
SECOND APPELLATE DISTRICT, DIVISION THREE

In re WILLIAM FRENCH ANDERSON, Petitioner, On Habeas Corpus.	Court of Appeal No. B232746; Los Angeles County Super. Ct. No. BA255257

AMENDED APPLICATION TO FILE AMICUS BRIEF REGARDING DIGITAL AUTHENTICATION

Thomas G. Stolpman, SBN: 69640
STOLPMAN, KRISSMAN, ELBER & SILVER, LLP
111 W. Ocean Blvd., Suite 1900
Long Beach, CA 90802
Telephone: (562) 435-8300
Facsimile: (562) 435-8304
stolpman@skes-law.com

Attorney for Amici Curiae

1 *For more detail about the concept, see Noga Morag-Levine, ' Facts, Formalism, and the Brandeis Brief: The Making of a Myth' , 2013 U. Ill. L. Rev. 59.*

TOPICAL INDEX[2]

AMENDED APPLICATION TO FILE AMICUS BRIEF REGARDING DIGITAL AUTHENTICATION

STATEMENT OF INTEREST OF AMICI

AUTHENTICATION OF DIGITAL EVIDENCE IN THE 21ST CENTURY

A. The Qualitative Difference Between Digital and Physical Evidence.

B. The Authenticity Issues Regarding Digital Evidence.

C. The Unavailability of An "Original" of a Digital Record.

D. Theoretical Solutions to Digital Authentication Issues.

E. Practical Solutions to Digital Authentication Issues.

1. Physical protection of the digital data.
2. Widespread dissemination of the digital data.
3. Creation of an uneditable first copy as the reference.
4. Integrity, Identity and Time Attributes As Established by Advanced Information Security Techniques.

CONCLUSION

TABLE OF AUTHORITIES

STATUTES CITED

Cal. Evidence Code section 255

California Rules of Court, Rule 8.200

Federal Rules of Evidence, Rule 1001

TREATISES

George L. Paul, *The Authenticity Crisis in Real Evidence,* first published in Scientific Evidence Review, Monograph No. 5, (ABA, 2001), and then subsequently in Law Practice Today, 2006, available at http://www.abanet.org/ lmp/ lpt/articles/tch03065.shtml

George L. Paul, *Foundations of Digital Evidence* (ABA publishing, 2008)

Stephen Mason, "Digital Evidence in Five Nations," Appendix D to George L. Paul, *Foundations of Digital Evidence* (ABA publishing, 2008)

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA SECOND APPELLATE DISTRICT, DIVISION THREE

In re WILLIAM FRENCH ANDERSON, Petitioner, On Habeas Corpus.	Court of Appeal No. B232746; Los Angeles County Super. Ct. No. BA255257

AMENDED APPLICATION TO FILE AMICUS BRIEF REGARDING DIGITAL AUTHENTICATION

STATEMENT OF INTEREST OF AMICI

The *amici curiae* submitting this brief are experts who specialize in the authentication of digital information, and who have experience in the evidentiary use of digital media in legal proceedings. Our experience and qualifications are summarized in the concluding section of the brief. We believe that the accompanying brief will assist the Court in deciding this matter because there is a general lack of recognition in the rules of evidence and case law regarding the qualitative difference between traditional evidentiary writings that are tangible, three-dimensional, and free-standing, e.g., an affidavit with an original signature and notary seal, vs. digital writings that cannot exist outside a host medium such as a

2 *Editors note: the original pagination cannot be retained for the purposes of publishing this document in the Review, so page references have been removed for the convenience of the reader.*

computer or electronic data storage unit. This qualitative difference has major implications not well-recognized in the rules of evidence or case law as to reliable means of authenticating digital writings.

Amici curiae therefore apply for permission to file the accompanying brief to assist the Court in reaching an informed and reliable resolution of the pending issues regarding the authentication of the digital recording at issue here. In compliance with Rule 8.200(c)(3)(A), California Rules of Court, *amicus curiae* George Paul states that petitioner William French Anderson paid him fees for coordinating communications among the other amici, and for preparing and editing the brief. In compliance with Rule 8.200(c)(5), amici curiae state that they do not support either party.

AUTHENTICATION OF DIGITAL EVIDENCE IN THE 21ST CENTURY

A. The Qualitative Difference Between Digital and Physical Evidence.

Traditional writings had a physical and tangible existence, subject of course to the deterioration inevitable with the passage of time, e.g., ink fades, parchment crumbles, etc. However, it was always at least theoretically possible to detect extrinsic and intentional changes to the original writing. Detection was not guaranteed, and forgers have been challenging the integrity of the legal system for centuries. The legal system responded with rules regarding the authentication of proposed writings, and frequently relied on specialists such as questioned document examiners to inspect the writing for indicia of alteration.

In contrast, digital records do not depend on the alteration of physical matter, and therefore the inspection of an item of digital data is not a reliable or even a logical method for testing authenticity. In an inspection one can only view the information in its current state as contained in its host medium. The digital record consists of an arrangement of a finite number of 1s and 0s,[3] and not untold molecules bound together in a three-dimensional space. In most instances, the medium host in which digital writings are offered as evidence is not the original host in which the digital writing was created.

One of the most important but least understood things about digital writings is that they can be altered without any ability to ***test*** for change by an inspection of the record itself. This is a stark difference from traditional physical writings in which traces of change could be detected from indicia in the document under inspection. Writing can be smeared or smudged, and that smear or smudge appears on the record because it is an artifact of three-dimensional matter that carries the information. A page can be torn out of a document, and be found to be missing upon inspection. One can sense a cut-and-paste job in a photograph. Magnetic clips can be heard in taped sound recordings, where the physical medium was altered.

In our digital age, software has generally evolved to facilitate undetectable or seamless editing of informational records. This is one of its main advantages in a business or legal context. The advantage of a word processor over a typewriter was the ability to easily modify the previous text, and yet leave no indication of that modification. The old information was lost—on purpose—and the new information was saved in an information object, often called a "file."

Information was thus undetectably changed in the record as a result of the processing of information. The new arrangement of information was saved as the record. There was not, however, necessarily a record about a critical, second set of information: information about the changes that were made. The history of what has been changed may or may not have been recorded. The ability to record such a history is dependent on the abilities of the program and whether that function has been enabled by the user. Or, there may be an incomplete record of the history of any changes. Or, there may be no record of changes. Furthermore, whatever record there is can subsequently be destroyed. And in addition, there are tools that enable individuals to edit certain records about the properties of files, making the process of testing authenticity even more difficult.

Nearly every application in use today is designed to modify existing content in such a way that a modification would not be detectable unless a history of the change was being recorded. Thus, this seamless editing function is endemic. It occurs with most business software such as word-processing applications, e-mail, spreadsheets, and graphics programs. But one also has the ability to seamlessly edit photos. Even a newbie user of Adobe Photoshop can make a dirty glass disappear off the table, or change the time on a clock, for example.

Seamless editing can occur in sound records, as well.

3 *This could be hundreds of thousands, or millions, or even more bits. But in all instances, it is only a successive order of 1s and 0s, not their unique arrangement in three-dimensional space that is involved. In all events the system involved can easily replicate the successive order exactly, identically, and in reliable succession.*

Words in a recorded conversation can be rearranged digitally, without any indication there has been a change. Transitions, formerly quite discontinuous, can be smoothed out by computer processing in sound editing tools. So, too, can digital video be edited, as any viewer of modern commercial advertisements can attest.

B. The Authenticity Issues Regarding Digital Evidence.

Almost everything that can be digitized can be modified, leaving no indication it has been changed. There may be no information in the file about the change. Who changed it? When? How was it changed? What was the information before it was changed?

Critically, it is most often impossible to answer these questions. There is simply not enough information available to allow a test for answers. The information about the torn-out page in the book of account, the smudge that appeared with the pencil, or the presence of white-out that appeared with the pen—the information about the change—is missing in the digital realm.

Accordingly, profound authenticity issues pervade all spheres of modern society, including legal systems.[4] Our tried-and-true inspection paradigm, which was written into the law of evidence long ago, fails us with regard to digital records. No matter how carefully one studies things, one may only be able to discern the most recent version of a digital file, not its makeup seventeen versions ago, much less its original composition. There is now a panoply of products designed to erase any vestiges of the past history of files—to annihilate their metadata, and any vestigial changes or comments. Law firms frequently use these on, for example, Word® files before they are sent outside the law office. This way, opposing firms can only know the current information in the file, the information of the present, and not discover the thinking of their opponents by looking at various other views that might be available.

This endemic inability to test digital information about previous states—a combination of seamless editing with the fact that digital evidence consists of pure information objects, not complex three-dimensional artifacts—is referred to here as ***untestability***. This characteristic of untestability gives rise to the need for countervailing authentication requirements to maintain the integrity of the legal system. All participants in the system deserve a system in which the authenticity of records can be tested. Otherwise we are adrift.

C. The Unavailability of An "Original" of a Digital Record.

The venerable best evidence rule appears to provide a simple solution to authentication of digital writings, i.e., a requirement that the original electronic file be produced. Unfortunately, that is virtually unattainable because the "original" record cannot exist independently of the machinery on which it was created. A lawyer who drafts a contract on a word processor, hits "Save", and names the document has created the original. However, that pristine original file cannot be maintained in its original form unless the computer on which it was saved is taken out of service and stored for future evidentiary use. And even then, there would need to exist testable evidence the digital file was not edited before preservation of the device. Similarly, a recording device that captures a conversation has the original digital audio data, but that data cannot be maintained in its original form without taking the recorder out of service and preserving it with the digital data for future reference. That procedure is manifestly impractical, as the recording device could only be used once. Instead, what happens now is the original digital data is electronically removed from its initial resting place, re-processed through a computer program, and presented in a different host medium. At that point, there no longer exists a data set that can be identified as the original.[5]

The printout is an original of what was printed out, not necessarily an exact copy of the original digital information. Thus, the definition is almost meaningless. The drafters of Rule 1001(d) of the Federal Rules of Evidence gave no thought to the fact that digital files are pure information, and live apart from the world of artifacts, and that such information can be undetectably edited on networks without any ability to test for changes.

4 *George L. Paul, The Authenticity Crisis in Real Evidence, first published in Scientific Evidence Review, Monograph No. 5, (ABA 2001), and then subsequently in Law Practice Today, 2006, available at http://www.abanet.org/lmp/lpt/articles/tch03065.shtml.*

5 *The legal system has generally responded to this technological reality by relaxing the best evidence rule to the point that it is no help in resolving authentication issues. The drafters of the Federal Rules of Evidence in the early 1970s could not have foreseen the technological developments of the 1980's and beyond. Indeed, in defining "original" in Rule 1001(3), the drafters declared that anything that was printed off a computer was an original so long as the printouts accurately reflect the data currently in the computer. F.R. Ev. 1001(d) currently reads, "For electronically stored information, 'original' means any print-out – or other output readable by sight—if it accurately reflects the information". Even if an electronic file had been edited numerous times over several years, as long as a printout is accurate of what is currently stored in the computer's memory, the printout is an "original" for purposes of Rule 1001(d). This eviscerates the traditional meaning of the term "original".*

Thus, the concept of "original" under the Federal Rules of Evidence and the evidence codes of most jurisdictions[6] has been reduced to triviality regarding digital information.

D. Theoretical Solutions to Digital Authentication Issues.

A reliable test for authenticating a digital record requires a comparison of the proffered digital record with a trustworthy standard. This requires creation of a digital equivalent of an "original": the will carefully sealed in a vault, with a record of access, or a notarized deed kept in a county recorder's office. The information object against which we compare the questioned object is called the *reference*.

The reference is simply the object we agreed to trust as being authentic as compared with any other object. It is the object we choose as the standard of comparison when we do our act of comparing. Because digital information is no longer tied to physical artifacts, we must arrive at our notions of reference differently.

Accordingly, the concept of reference now looms large in the world of evidence. Indeed, it is the closest proxy or surrogate to an "original" in the physical world. The reference is the set of pure information, of which there might be a billion copies, that has been declared by an entity as the authentic information. A reference therefore has an identity associated with it; the identity that declares it as authoritative, and, as we will see, the identity that protects it and defends its immutability. These are most often but not always the same identity. A reference contains the information that is the reference information (the official content), and an implied promise the information will not change through time. A reference by its very nature contains a promised attribute of immutability.

In the world of physical records of information, there was clearly an act of declaring a reference: the signing of the original. The immutability of the artifact gave protections against change to the information. Such immutability "services" were accepted, and not overly pondered. The act of declaring, by an actor or participant, was clearly what was in mind, and we therefore have the important concept of "signature" in the law. Often there were notaries involved, and sometimes other physical mechanisms, such as wax or other "seals." In the digital world, we must now be self-conscious about declaring what will hence forward be used as references in future tests of authenticity.

E. Practical Solutions to Digital Authentication Issues.

Here are four possible solutions to establishing a reference for authentication of digital records.

1. Physical protection of the digital data.

First, one could use the old-fashioned way to protect references: physically secure them, typically by locking them up. One could use a vault to protect a record of digital information. One could use a super-secure computer system to store reference information. More generally, this objective can be achieved by using a trusted third party, whose role is to protect a digital record. Indeed, there are now services springing up that provide this function. This method works to the extent that the reference data submitted to the digital safe-keeper is trustworthy.

2. Widespread dissemination of the digital data.

A second approach takes a diametrically different tack. Instead of locking up information to prevent manipulation, one could spread the information far and wide, which does not prevent change but which might guarantee that change could be easily discovered through the act of comparison with the widely distributed information. One could, for example, publish either the reference information or the "hash"[7] of a reference in a newspaper of wide circulation. This would ensure there were numerous physical repositories of the reference or its hash existing on a certain date. The chance that such newspapers could all be gathered up, reprinted, and then substituted, all over the United States without their owners' knowledge, is mathematically almost zero percent. One can trust the digital information object existed on a certain date if one found widely distributed

6 *Cal. Evidence Code section 255 is virtually identical to the Federal Rule – "'Original' means the writing itself or any counterpart intended to have the same effect by a person executing or issuing it … 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'".*

7 *A "hash" is the result of a one-way transformation of a digital file, by means of a mathematical algorithm, which results in a unique, but much smaller, digital file. In a way these can be conceived as a "digital fingerprint." There are several such algorithms in use today, and they are the subject of repeated tests and discussions. Appropriate hash algorithms have several attributes. Importantly, they are one-way, irreversible transformations. With a good hash algorithm, it is mathematically infinitesimally unlikely for one to deduce the content of the original file. Thus, the fingerprint is a secret fingerprint to those that have been distributed the hash file. Among other attributes, hashes are useful because the transformed file is extremely small. Accordingly, hash algorithms, and hashes, are useful in comparing digital files to test whether they are perfectly identical. If the files differ by only one bit, when hashed, the two files will render fundamentally and unpredictably different results.*

newspapers with its hash published on that date.

3. Creation of an uneditable first copy as the reference.

The third approach is to require the party who creates the digital data to immediately make an un-editable digital memorialization of the contents of that file. One could store the record in read-only format on media, commonly known as "WORM" or "write once, read many" format. This is a "preventing change" solution, not a "discovering change" solution. Many solutions do exactly that. Many believe this is in fact the simplest and most straightforward method for an individual or entity that seeks to preserve digital records for litigation use. This is also the procedure recommended by the manufacturer of the recording device used by the Los Angeles County Sheriffs in this case. See Exhibit E, Habeas Corpus Petition. This procedure is technologically simple, and requires no third party involvement. It does require that the individual or entity follow a clear protocol that minimizes the possibility of alteration.[8]

4. Integrity, Identity and Time Attributes As Established by Advanced Information Security Techniques.

There are technologies, which involve various types of encryption and other algorithms, that have become important in the last few years and which address concerns involving the authenticity of digital information. Indeed, as illustrated in Stephen Mason's case study, "Digital Evidence in Five Nations," found as Appendix D to George L. Paul, *Foundations of Digital Evidence* (ABA publishing 2008), this methodology has been incorporated into many of the civil law jurisdictions in Europe and elsewhere. Such techniques are used as a way to authenticate digital records by testing various "attributes" of digital information -- including the *identity* of the creator or "signer" of a file, a continued *integrity* through time (meaning testable knowledge a file has not changed in unauthorized or unknowable fashion), and even a trusted method of determining the relevant *time* associated with of a reference. Such methods can be used, if implemented properly (the details of which are beyond the scope of this brief), to confirm who declared the reference or who protected it as inviolate; and to provide a check of integrity on any purported information object that is compared to the reference as identical. Just like locking information up in a safe with trusted guardians protecting it, this mathematical and business process solution can solve the issue about both how to protect the reference as immutable and to test its "signer," or the entity that declared it as a reference. In some implementations, the "time" of the creation of the reference can also be recorded as trusted data, with technologies explained in Chapter 5 of *Foundations of Digital Evidence*. Such more advanced, mathematically and business method solutions can be used to reveal the existence of any unauthorized tampering between the time the reference is protected and the time the purported digital information is tested against the reference.

CONCLUSION

We urge the Court to consider these aspects of digital records in adjudicating the issues presented here, and, for the benefit of the bench and bar, promulgate appropriate standards for the authentication of digital writings.

DATED:

Respectfully submitted,

_____

THOMAS G. STOLPMAN
STOLPMAN, KRISSMAN,
ELBER & SILVER, LLP
Attorney for *Amici Curiae*

8 This method makes the reference immutable, but cannot conclusively preclude the creation of an altered reference by those in control of computer environment variables.

QUALIFICATIONS AND EXPERIENCE OF AMICI CURIAE

Conor R. Crowley, Esq., CIPP/US/E, *has more than a decade of experience advising corporate and law firm clients on e-discovery readiness and responsiveness, information governance and data privacy. Mr. Crowley has served as both a testifying expert and a court-appointed special master on e-discovery issues. Mr. Crowley is the incoming Chair of The Sedona Conference Working Group on Best Practices for Electronic Document Retention and Production in addition to being the Editor-in-Chief of The Sedona Conference Commentary on Proportionality in E-Discovery, and Senior Editor of a number of The Sedona Conference' s publications including The Sedona Conference Commentary on Legal Holds and The Sedona Principles (Second Edition): Best Practices Recommendations & Principles for Addressing Electronic Document Production.*

Lisa Grant, Esq., CISSP, CIPP *has been in the data security industry since 1997 and a Certified Information Systems Security Professional since 2001. As an attorney and IT security professional, she has worked for internet security leaders IBM, VeriSign and PwC where she spent over a decade consulting to Fortune 500 companies about appropriate information security practices commensurate to the risk. She currently serves as Executive Director/ Trainer at SecurPrivacy, Inc., and teaches as an Adjunct Professor in Mercy College' s Cyber Security program. Ms. Grant currently co-chairs the National Strategy for Trusted Identities in Cyberspace, Legal and Contract Committee and teaches Internet Safety to Parents and Children through her non-profit organization, SecurPrivacy.org. Having held various roles in the industry from ethical hacker to in-house counsel, Lisa has a wealth of education and experience with regard to data security and law which includes, but is not limited to, hands-on technical experience securing an enterprise by configuring firewalls, public key infrastructures, routers and intrusion detection systems. Ms. Grant graduated from Pace University School of Law in 2009 and is admitted to practice in the State of New York. She has an undergraduate degree in Biology and is currently pursuing practice before the USPTO. Ms. Grant is married to Mr. John DeGraffenreidt and resides in New Rochelle, New York.*

Sherry Harris *is Senior E-Discovery Advisor at the Crowley Law Office. She is a Charter Member and Steering Committee Member, The Sedona Conference Working Group on Electronic Document Production and Retention, and active participant in many special project groups. Member, The Sedona Conference RFP+ User Group. Editor, The Sedona Conference Glossary For E-Discovery and Digital Information Management. Co-Editor, The Sedona Conference RFP+ Group, Navigating the Vendor Proposal Process: Best Practices for the Selection of Electronic Discovery Vendors, 2nd Edition. Member, Georgetown University Law School E-Discovery Advisory Board and Georgetown Law Practice Support Training Program Planning Committee. Founder and organizer of B-Discovery Richmond, VA, Chapter - January 2011 to present. She specializes in E-Discovery Project Management - over 30 years experience in complex litigation, with expertise in preservation, collection, culling, processing, review, integration of automation and use of automated discovery applications in complex litigation and investigations, while living within (or below) budget. Experienced and well versed in corporate records management, legal hold requirements, preservation issues, and electronic discovery.*

Kelly "K.J." Kuchta, CPP, CFE *is an Information Security and Computer Forensics Consultant with over 16 years of experience in computer, physical and operational security issues. Mr. Kuchta has 18 years of experience in the Banking, Insurance and Financial Services Industry, and has presented numerous times nationally, and has written many papers. During this time, his responsibilities included managing Fraud Investigations (including computer-related incidents), Physical Security Reviews, Risk Management Operations and E-Commerce initiatives. He has conducted or managed in excess of 5,000 investigations in his career. KJ has been credited for introducing many groundbreaking ideas and concepts in the areas of risk management and investigations.*

Mark E. Lassiter *is an AV Rated attorney with 29 years of practice in the areas of Alternative Dispute Resolution ("ADR"), business, real estate and construction law with a focus in commercial litigation and dispute resolution. He is a member of the State Bar of Arizona' s Business, Real Estate, Construction and ADR Sections and a member of the State Bar of Arizona' s Technology Committee, where he Chairs its Cloud Computing and Law Practice Management Subcommittee. Mr. Lassiter is currently enrolled in a Masters in Administration - (Legal) Project Management at Northern Arizona University and working on a Cloud Based Legal Project Management platform, which will allow his law firm clients to view the ' real time' status of the documents and activities in their cases ' 24/7' from their i-Pads, mobile phones or computers. An expert in computer aided evidence presentation and case management matters, he is a frequent speaker at Bar*

Associations and in Continuing Legal Education ("CLE") programs and has given presentations in 24 major U.S. cities, including programs sponsored by the Seventh, Eighth and Ninth Circuit Judicial Conferences, the National Institute for Trial Advocacy ("NITA"), the State Bars of Arizona and New Mexico, the Federal Bar Association, the American Arbitration Association and other groups.

***Stephen Mason** is a barrister at the Bar of England & Wales and an Associate Research Fellow at the Institute of Advanced Legal Studies. He is general editor of **Electronic Evidence** (3rd edn, LexisNexis Butterworths, 2012) and **International Electronic Evidence** (British Institute of International and Comparative Law, 2008); he is also the author of **Electronic Signatures in Law** (3rd edn, Cambridge University Press, 2012) and **Electronic Banking: Protecting Your Rights** (PP Publishing, 2012); and is the founder, general editor and publisher of the international journal **Digital Evidence and Electronic Signature Law Review**, which has become an international focal point for researchers in the area.*

***George L. Paul** is Senior Partner at the Phoenix office of Lewis and Roca, LLP, and graduate of Yale Law School. He has written numerous articles about the authenticity of digital records, including The Authenticity Crisis In Real Evidence, and two books, one of which is **Foundations of Digital Evidence** (ABA Publishing 2008). He testified before the Civil Rules Advisory Committee in its consideration of the 2006 E-Discovery Rules of Civil Procedure; before the Federal Evidence Advisory Committee in its consideration of Fed. R. Evid. 502; drafted the Arizona Supreme Court' s version of Arizona' E-discovery Rules of Civil Procedure; co-founded the Arizona Bar Association' s Section of Internet and Technology Law; and is currently Co-Chair of the American Bar Association' s Electronic Discovery and Digital Evidence. He lectures frequently about evidence, ethics, and trial tactics. Other significant publications are Information Inflation: Can the Legal System Adapt?, and Transformation, to be published in the 2013 Winter Edition of the ABA' s Sci-Tech Lawyer.*

***Kimberly Baldwin-Stried Reich, MBA, MJ, PBCI, RHIA, CPHQ, FAHIMA** – is a credentialed health information, quality, and compliance professional with over 25 years experience in a variety of healthcare settings. She is a national speaker and author on the topics of health information operations, e-discovery and healthcare compliance. Since 2006, she has been an active member of the Health Level Seven (HL-7) Working Group responsible for review and development of the Records Management and Evidentiary Support (RM-ES) profile for the design and development of the functional profile for Electronic Health Record (EHR) systems. She has also been an active member and contributor in AHIMA task forces and working groups related to electronic discovery. Kim is a member of The Sedona Conference® Working Group I on Best Practices for Electronic Document Retention and Production, the Public Health Data Standards Consortium (PHDSC), the American Medical Informatics Association (AMIA), the National Association for Healthcare Quality (NAHQ), the Health Information Management Systems Society (HIMSS), the American Society for Healthcare Risk Management (ASHRM), and the Association of Certified Electronic Discovery Specialists (ACEDS). She is the lead author on the AHIMA publication, **"E-Discovery and Electronic Records."** (AHIMA Press, 2012) In 2011 Kim was awarded the AHIMA e-HIM® Triumph Award in recognition of those individuals, groups, or organizations who have made important advancements in areas related to electronic health information and digital evidence. (e-HIM®).*

***Timothy Reiniger** is an attorney currently serving as Director of the Digital Services Group of FutureLaw, LLC, in Richmond, Virginia. He specializes in digital document and personal identity strategy and policy development and information assurance protocols. He is a nationally recognized expert on the notary office and information policy, testifying on these topics before the U.S. House Judiciary Committee, the California House and Senate Judiciary Committees, the Florida Senate Judiciary Committee, and the Hague Conference on Private International Law. As an author, Tim has contributed a chapter on electronic notarization to "Foundations of Digital Evidence," authored by George Paul and published by the American Bar Association. He is a member of the ABA' s E-Discovery and Digital Evidence Committee and is licensed to practice in California, New Hampshire and the District of Columbia.*

***John W. Simek.** John W. Simek is the Vice President of Sensei Enterprises, Inc. He is an EnCase Certified Examiner (EnCE) and a nationally known testifying expert in the area of digital forensics. Mr. Simek holds a degree in engineering from the United States Merchant Marine Academy and an MBA in finance from Saint Joseph' s University. After forming Sensei, he ended his 20+ year affiliation with Mobil Oil Corporation, where he served as a senior technologist designing and troubleshooting Mobil' s networks throughout the*

western hemisphere. Mr. Simek has in-depth experience with network troubleshooting, hardware and software implementations, systems integration, and logistical and financial expertise in a wide range of computer engineering designs and solutions. He has an extensive knowledge of multi-protocol environments and a diverse range of networking technologies. He is the co-author of numerous books published by the ABA and co-host of the Legal Talk Network podcast series "Digital Detectives." In addition to his EnCase Certification (EnCE), Mr. Simek is a Certified Handheld Examiner, Certified Novell Engineer, Microsoft Certified Professional + Internet, Microsoft Certified Systems Engineer, NT Certified Independent Professional, and a Certified Internetwork Professional. He is also a member of the High Tech Crime Network and of the International Information Systems Forensics Association as well as the American Bar Association. John has also been a member of the Planning Board for the American Bar Association' s TECHSHOW and a past member of the Boyd-Graves Conference Subcommittee on Electronic Evidence.

***Steven Teppler** is a nationally known expert on trusted time stamping and other areas involving digital authenticity issues. Teppler chairs Kirk•Pinkerton PA' s electronic discovery and information governance practice. Steven' s litigation practice focuses on electronic discovery, including production, preservation, spoliation issues. His experience includes Federal and state court litigation matters both against and on behalf of Fortune 500 companies as well as probate and family law disputes where electronic discovery is critically implicated. He has practiced law since 1981, is admitted to the bars of New York, the District of Columbia, Florida, and Illinois and advises private and public sector clients about risk, liability, and compliance issues unique to information governance (i.e., from instantiation through management, preservation and disposition). Steven is an adjunct professor at Ave Maria Law School, teaching electronic discovery, and also lectures nationwide on evolving theories of information governance and electronic discovery. Mr. Teppler is also a member of the Florida Bar' s Business Law Section eDiscovery Subcommittee, and is a co-drafter of the 2012 electronic discovery amendments to the Florida Rules of Civil Procedure.*

***Kenneth J. Withers** is an attorney currently serving as the Director of Judicial Education at The Sedona Conference®, a non-profit, non-partisan educational and research foundation dedicated to the just and reasoned development of the law in the areas of complex litigation, antitrust, and intellectual property, headquartered in Phoenix, AZ. He previously was Research Associate and Senior Education Attorney at the Federal Judicial Center in Washington, DC; Education Director at the Social Law Library in Boston, MA; and ten years in private practice. He specializes in the application of technology to civil litigation, particularly discovery and trial practice. Among his published articles are "Computer-Based Discovery in Federal Civil Litigation," 2000 Federal Courts Law Review 2; "Self-Deleting E-mail: A Self-Delusion?" Discovery Edge, Fall 2000; "Computer-Based Disclosure and Discovery in Civil Litigation," 2001 Journal of Information, Law & Technology, Issue 1 (which received the British Irish Legal Education Technology Association, Lord Lloyd of Kilgerran Prize for Best Postgraduate Essay in Information Technology and Law); "Two Tiers and a Safe Harbor: Federal Rulemakers Grapple With Electronic Discovery," The Federal Lawyer, September 2004; "They' ve Moved the Two Tiers and Filled in the Safe Harbor," The Federal Lawyer, November 2005; "Ephemeral Data and the Duty to Preserve Discoverable Electronically Stored Information," 37 U. Balt. L. R. 349 (2008); and "Living Daily with Weekley Homes," Texas State Bar Advocate, Vol. 51 (Summer 2010), 23. He has also contributed to several well-known Federal Judicial Center publications, including the Manual for Complex Litigation, Fourth Edition (2004), Effective Use of Courtroom Technology (2001), and the Civil Litigation Management Manual (2001). The opinion he expresses by endorsing this brief is solely his own and does not necessarily reflect opinions of The Sedona Conference®, its members, or sponsors.*

***Stephen Wu** is a Silicon Valley partner in the law firm Cooke Kobrick & Wu LLP. He advises clients concerning e-discovery, electronic records retention, digital evidence, and legal matters relating to information assurance, data security, privacy, and secure electronic commerce. His litigation practice focuses on information technology, intellectual property and business cases. Mr. Wu served as the 2010-2011 Chair of the American Bar Association Section of Science and Technology Law and is a member of the Section' s E-Discovery and Digital Evidence Committee. In addition, from 2001 to 2004, he was Co-Chair of the Section' s Information Security Committee. Mr. Wu is also a member of the ABA Standing Committee on Technology and Information Systems. He is a 1988 graduate of Harvard Law School and, before starting his private practice, was the second in-house attorney at VeriSign, Inc. At VeriSign, he was in charge of the company' s worldwide security and legal policies and practices governing its digital certification information*

security services. Mr. Wu authored or co-authored five books on information security, and writes the eDiscovery, Digital Evidence and Cybersecurity Law blog for RSA Conference, the industry-leading continuing educational forum for information assurance and data protection.

DECLARATION OF SERVICE

RE: People v. William French Anderson
Court of Appeal No. B232746
Los Angeles County Super. Ct. No. BA255257

I, John Holdsworth, am over the age of 18 years, am not a party to the within entitled cause, and maintain my business address at 111 W. Ocean Blvd., Suite 1900, Long Beach, CA 90802. I served the attached:

AMENDED APPLICATION TO FILE AMICUS BRIEF REGARDING DIGITAL AUTHENTICATION

on the following individuals/entities by placing a true and correct copy of the document in a sealed envelope with postage thereon fully prepared, in the United States mail at Long Beach, California, addressed as follows:

Attorney General
300 S. Spring Street
Los Angeles, CA 90013

I declare under penalty of perjury that service was effected on January 2, 2013, at Long Beach, CA, and that this declaration was executed on January 2, 2013, at Long Beach, CA.

_____
John Holdsworth

