

# Law Practice TODAY

## The "Authenticity Crisis" In Real Evidence

*by George L. Paul*

March 2006

### INTRODUCTION

Authenticity, in the broad sense of the word, is fundamental to litigation. It acts as a dynamic -- as the conceptual glue holding together the pieces of a case. As part of its most basic function, therefore, a jury constantly assesses authenticity. Once falsehood is detected, or truth perceived as misrepresented, a party's case unravels. Indeed, tribunals could not serve their function without an ability to assess whether proffered assertions are what they "purport to be."

Each type and piece of evidence must therefore be subject to a test for authenticity. The testimony of witnesses is a familiar example. Such evidence is examined for bias, for interest and for the human capacity to exaggerate or mislead, among other things. Cross-examination, including the comparison of testimony with records of various types, is the chief tool by which we probe witnesses, whose genuineness or authenticity is usually called "credibility."

### Real Evidence and "Informational Records"

But witnesses, and their assertions, constitute only one type of evidence. Another category, anciently but misleadingly labeled, is "real evidence." This can be a three-dimensional object, such as a weapon or a piece of art. It can also be, and is far more commonly an "informational record," a message or record containing language, numbers or other portable information. Such records -- examples of which are memos, contracts and e-mails -- are created millions if not billions of times daily, and are involved in practically every dispute. The photograph is a specialized subset of this type of evidence, being both informational and representational. Sound recordings are also informational records.

Informational records are thus key components of our culture, and play a special role in disputes. Whether a given informational record is authentic is already quite often an important issue in litigation. Given society's increasing reliance on records, however, such issues undoubtedly will only increase in importance with time.

## THE CHALLENGE TO OUR SYSTEM OF FOUNDATIONS

Few lawyers are discussing the fact that digital technology has fundamentally changed the world of real evidence, particularly regarding authentication of informational records. Digitization of records is skyrocketing. It is increasingly easy for a record to enter the digital world, and many records are now digital *ab initio*. The cost of storage is dropping monthly, thus catalyzing government and companies to switch from files of bulky paper, to files in computer memory.

Equally if not more important, however, is the fact that the cost of *manipulating* such records has also become extremely low. Many tens of millions of people possess software, such as "word processing" programs, which permit the seamless manipulation of informational records. It is simple to alter a record while keeping an appearance of authenticity. Given such trends, it is time to ask how we test for or even recognize the existence of an *authentic* informational record that exists in digital format.

### Our Analog Rules of Evidence

As background, it is important to remember that the Federal Rules of Evidence were enacted in 1975. At that time, informational records were made with analog technology, and were likely to be "faithful" as a result. For example, traditional photography left a record imprint on a delicate emulsion of film. Sound recordings were stored as imprints on magnetic tape. Papers were written or signed by hand, and mechanical devices like typewriters were used for other communications. Even duplication technologies -- such as carbon paper and copier machines-- utilized analog technology. Traditionally, the storage of informational records did not facilitate seamless editing; much less allow editing by tools specifically designed for such a purpose.

Because of the relative immutability of the storage media, analog informational records have long been perceived as relatively dependable. Analog technology makes alteration expensive, a process requiring both skill and intent. If alteration happens, it is usually detectable.

As a result of these facts juries became accustomed to assuming that informational records, such as a photograph, are the “real thing.” If a witness departs from the information represented in a photograph, she was assumed to be unreliable, or worse, intentionally deceptive. The analog photographic record, although not guaranteed to be accurate, was enormously convincing.

## **Authenticity Requirements for Photographs, Recordings and Writings**

Because of the assumptions relating to analog informational records, under the current rules only a few quick and sketchy foundational questions are required to allow writings, photographs and tape recordings to come into evidence as “authentic” -- as being what they “purport to be.” It is up to the cross-examiner, usually without extrinsic evidence concerning the record, to test or attack the authenticity of such evidence.

The foundation required for authentication of a photograph is a good example of our traditional reliance on the technological underpinnings of analog information records. The requirement to admit a photograph into evidence is a mere conclusion by a witness that it “accurately represents the scene depicted.” The photographer is not called to the stand. Nor is anyone who handled the image. Nor is there evidence required of the first image in the chain -- the one created by the information existing at the time of the historical event.<sup>1</sup> All that is necessary is for someone – not necessarily someone present when the photograph was taken – to declare that a photograph is accurate.<sup>2</sup> Most often this happens *years* after the event.

The same implicit assumptions about technology exist in the foundational requirement for sound recordings. The U.S. Courts of Appeals for the 2d, 5 th, 7 th, 9 th, 10 th, 11 th and District of Columbia circuits have flexible approaches to authentication. Similar to the photograph, a party seeking to admit sound evidence need only show that the recording is an accurate reproduction of sound that was *previously heard by a witness*.<sup>3</sup> Once again, proof of the authentic information in the original recording is almost never required.

It is therefore no surprise that the foundation to authenticate an informational record such as a multi-page contract is the conclusion of a witness that the document is accurate. Our authentication scheme does not genuinely inquire into the likelihood that a human being can remember all details of a multi-page contract. Instead, the system relies heavily on the societal assumption that a change in the information represented is (1) unlikely and (2) capable of detection.

## **The Fallacies in Our Current System**

These assumptions are simply fallacious when applied to digital records. And the disconnect between evidentiary assumption and technological fact is growing ever wider. Just a few years ago, a \$30,000 “drum scanner” was necessary for the high-quality digitization of a 35mm negative. Now one can buy a scanner for \$400. Just 10 years ago, digital cameras were esoteric devices costing many thousands of dollars. Suddenly they are everywhere, inexpensive, and of high quality.

Technology has thus fundamentally changed the way informational records are handled by Society. No longer is an image necessarily stored on the molecules of a film emulsion, or as handwriting or printing on paper. In photography, digital technology allows images to be represented as “pixels” in a digital file. Pixels can be made so small that they are functionally invisible. In addition, images can be transferred from the digital domain onto traditional film. Indeed, it is not necessarily possible, by looking at the record alone, to know whether something was ever digitized in the first instance. A history of the “evolution” of the image is necessary to test its authenticity. The same is true for business records that are digitized, and then printed out onto paper. They can be edited before printing, by a “word processor,” or other image editing software.

## **The Ease of Manipulation**

Indeed, the critical difference between digital and analog representations of reality is that once evidence enters the digital domain, it passes out of the world of three dimensional objects with unique atoms (which are relatively difficult to manipulate), and into the world of stored

information, which at its basic level, is nothing but bits of binary code. As such, digital information is subject to far easier manipulation than is analog information. Editing software exists for almost all types of digital information, whether it be business records (word processing), photographs (image editing software), or sound (digital audio workstations).

To give an example of this challenge, Adobe PhotoShop is already licensed to many millions of users, probably many tens of millions worldwide. With such a program, a computer operator can do a myriad of operations to affect a digital photographic file. Images of people can, with a high degree of sophistication, be seamlessly inserted into novel backgrounds. Objects can be removed from scenes. The task is not particularly difficult and only one person need be involved.

But fantastic changes are probably not the greatest challenge presented by digital photographs. Subtle changes, such as apparent lightness or darkness, or hue, can be changed with an easy click. With documents, a zero can be easily added to an invoice on a business record. Once again, given the ease of change, chance suggests dictates that a certain changes may happen accidentally.

In short, because of digital technology's ability to chop up records into tiny information fragments, manipulate such information at will, and then reassemble everything, society possesses a power not really contemplated when the authentication rules were adopted in the 1970s. In fact, the new informational record paradigm is now pervasive.

## **Non-Assurance of Detection**

The final straw is whether manipulation or change of stored digital records necessarily is apparent from *ex post facto* examination. Ability to detect manipulation of records is a critical aspect of the foundational underpinnings of the current authenticity scheme. The Rules seem to assume that, like good cross-examination of testifying witnesses, expert testing of a document, photograph, or sound recording will in most cases reveal any lack of authenticity. Before, there were magnetic discontinuities if someone altered a sound recording. A cut and paste job on a picture left artifacts. And a forgery was usually detectable. Imposters -- and attempts to pass records as something other than what they purport to be -- left tell tale clues and an opponent could be expected to discover "phoniness."

But because of digitization, examination of a record no longer necessarily reveals manipulation. Although skill remains a factor, there is nothing in digital manipulation of a document or photograph, *per se*, that leaves behind the traces of change inherent in traditional media. Such absence of intrinsic “artifacts of change” is a fundamental characteristic of the new information storage paradigm.

Clearly, therefore, a record of information is a precious thing for a culture and is indispensable for its legal system. Because we now record and edit information in a far purer form than previously, the assumption that evidence of change will be available is no longer valid.

## **EVOLVING THE NEW PARADIGM**

The current state of affairs with digital informational records is chaotic. The bottom line is that if presented with a file that has been previously digitized, there is simply no way to know, without extrinsic evidence, whether it has been subtly or radically altered, or instead is what it purports to be. Indeed, elaborate discovery would be necessary to test any hypothesis, and would need to trace the history of the file from inception. Usually such evidence is not preserved.

Jean Borda, European Coordinator for DIG 35 (“Digital Imaging Group”), a 70 member international consortium of imaging companies, proclaims that because of such issues, “photographs, as evidence of reality, are dead.”

As long as there is merely a digital file, which can be printed at any time, it is an elaborate process indeed to determine if and to what extent a business record has been changed since inception. Discovery of the media involved, and examination by experts, are both necessary to test authenticity of the record. This is an expensive “electronic detective” process. And, if a dispute is litigated years later as so often is the case, the hard drives in question may not even be available.

For all these reasons, in the absence of new authenticity regime, proving or testing the authenticity of business records will be extraordinarily expensive, and in many cases, simply impossible.

## New "Foundational Logic" Is Required

There is already at least one way to address these concerns. One solution is to deliberately implement a protocol that "freezes" a digital file at the relevant time, and then allow parties to test the frozen contents of that file. The solution requires parties to create records with future authenticity concerns in mind -- or be left by default with the expensive electronic detective process described above. Without a historical life raft, one is left awash in a sea of bubbling information.

## Public Key Infrastructure

One solution to these authenticity concerns is to employ the same technology which facilitates "secure" electronic commerce. The solution, allowing transmission of digitally coded information with an assurance of provable authenticity, is called Public Key Infrastructure, or "PKI." PKI is not new, and it is beyond the scope of this article to fully describe the technology. Its logic will be discussed as it relates to an evidentiary authenticity solution for informational records.

PKI employs an algorithm (mathematical formula) using two different but mathematically related "keys," one for creating a "digital signature," or encrypting data, and another for verifying a digital signature, or decrypting data. Computer equipment and software for utilizing such different key pairs is often termed an "asymmetric cryptosystem."

The complimentary keys of an asymmetric cryptosystem for PKI are termed the private key, known only to the holder, and the public key, which is ordinarily more widely known. Although the two keys of a pair are mathematically related, it is computationally infeasible to derive the private key from knowledge of the public key. The keys are issued by a trusted third party, called a certification authority ("CA"), which has as a business objective the knowledge of the correct identity of the subscriber to a key pair.

A critical methodology employed by PKI is the "hash function," which is an algorithm that starts with an informational record, and creates from it a digital "fingerprint" in the form of a "hash value" of a fixed length. The hash result is usually much smaller than the informational record, but

nevertheless unique to it. Critically, *any change* to the message always produces a *different hash result* when the same hash function is used. Thus, the hash result can be utilized as a “test” of whether even one bit of information in a record has been altered. This is the key to the new evidentiary scheme: which have a built-in, logical test for authenticity.

To explain the capability of PKI and its digital signature from another angle, a “digital signature” identifies the signed message, typically with far greater certainty and precision than a paper signature. Verification by reference to the public key reveals any tampering, since the comparison of the hash results (the one made at signing and the other made at verifying) shows whether the message is the same as when signed. This verification can be done at any time after someone sends a digitally signed message – upon receipt; a year later; or at trial.

Thus, a key aspect to a new evidentiary scheme is to conceptualize that sending a digitally signed message is a capability far broader than simply communicating by e-mail. The authenticity test, allowed by the hash function, allows any electronic informational record to be stored in a provable, frozen state. Invoices, letters, contracts, photos, and indeed any informational record that can be digitized can be subject to this mathematical test, which is dependent on logic. The technology has been tested and verified by the National Institute of Standards and Testing (“NIST”).<sup>4</sup>

## THE EVOLVING STATUTORY SCHEME

Certainly no action has been taken by Congress to change the Federal Rules of Evidence to address the recent wave of digitization. There is no new federal foundational system.

### New State Statutes

However, states are enacting solutions in the form of statutory evidentiary presumptions. The groundbreaker was the Utah Digital Signature Law, enacted in 1995 and reflecting early drafts of the Digital Signature Guidelines published by the American Bar Association’s Section of Science and Technology.<sup>5</sup> The Utah law provided presumptions that a properly verified digital signature is presumed to be the digital signature of a subscriber listed in that certificate. *See* Digital Signature Guidelines, 5.6(2)(1996) and Utah Code Ann. § 46-3-406(3)(1995).

With variations, the evidentiary presumption in favor of the validity of a digital signature has been followed by digital signature legislation in Washington, Wash. Rev. Code § 19.34.350(3)(A); Illinois, 5 Ill. Comp. Stat. 175 (10-120(b); Minnesota, Minn. Stat. § 325(K). 24, subd. 1(C)(1); Singapore, Singapore Electronic Transaction Act, § 18(2)(A) (1998) ([Http: //www.cca.gov.sg/eta/part5.html](http://www.cca.gov.sg/eta/part5.html)) and the UNCITRAL Model Law on Electronic Signatures. UNCITRAL, Art. 6 (3) U. N. Doc., A/Cn. 9/483, Report of the Working Group on Electronic Commerce, 37 th Sess. (October 5, 2000), A/Cn. 9/Wg. IV/WP. 88 ¶¶ 117-118, draft guide to enactment of the model law on electronic signatures, UNCITRAL 34 th U.N. Doc. Sess., (January 30, 2001). So long as certain foundational facts were proved (such as proper utilization of a PKI technology), *rebuttable* presumptions regarding authenticity have been provided by statute.

## **“E-SIGN” and Technology Neutrality**

On June 30, 2000, Congress enacted the Electronic Signatures in Global and National Commerce Act (“E-SIGN”), effective October 1, 2000, governing transactions in or effecting interstate commerce. 15 U.S.C. § 7001 et seq. (enacted June 30, 2000 effective October 1, 2000).

Section 101 of E-SIGN provides a general rule of validity to all electronic signatures used in interstate commerce. Importantly, Section 102 of E-SIGN prohibits the adoption of conflicting state laws to the extent they “accord greater status or legal effect to the implementation or application of a specific technology” relating to electronic signatures or records. Currently, there is a dispute as to whether § 102 of E-SIGN broadly preempts the state digital signature laws discussed above, and nullifies evidentiary presumptions about how informational record evidence is treated in courts. The emerging authenticity regime has suffered accordingly.

## **The Arizona Model: Security Procedures and Evidentiary Presumptions**

The Uniform Electronic Transactions Act, published by National Conference of Commissioners on Uniform State Laws (“NCCUSL”) avoided the “technological neutrality” issue caused by the later enacted E-SIGN. UETA does not provide any evidentiary presumptions of authenticity. For this reason, although UETA legitimizes electronic transactions and what it calls “electronic

signatures,” it does not provide for authentication certainty, or evidentiary presumptions necessary for future authenticity litigation.

A solution that is both technology neutral, and which provides evidentiary presumptions, does exist. The Arizona Electronic Transactions Act, A.R.S. § 44-7001 is an example of both worlds. The statute is modeled primarily after UETA. But the Arizona Act also includes an entire segment, Article 2, not contained in UETA. This is “Secure Electronic Records and Signatures.” The Arizona Act also defines a concept known as a “secure electronic signature.” *See* A.R.S. § 44-7031. It defines a “security procedure,” which is a process and logic allowing proof of authenticity, as defined above.

After application of a security procedure, a signature or record is deemed to be “secure” if it can be demonstrated that an electronic signature, at the time the signature made, was (1) unique to the person using it; (2) capable of verification; (3) under the sole control of person using it; and (4) linked to the electronic record through which it relates in such a manner that if the record were changed, the electronic signature would be invalidated.

“Secure” electronic records are optional in Arizona. Critically, the statute provides rebuttable evidentiary presumptions that a secure electronic record has not been altered. In the absence of a secure electronic record, there are no evidentiary presumptions regarding authenticity.

For these reasons, while remaining technology neutral, Arizona allows choice of a technology that will solve the authenticity problems posed by digital informational records. The utilization of a security procedure, with PKI as an example of such a procedure, forms the basis of such a rebuttable evidentiary presumption.

## **THE PECULIAR PROBLEM OF PHOTOGRAPHS**

Photographs present a somewhat peculiar problem as “informational” real evidence. They can be digitized and manipulated in the digital domain. As discussed above, software such as Adobe™ PhotoShop makes the manipulation of digital images easy, thus calling into question many aspects of image authenticity.

The concerns discussed here motivated at least one manufacturer, Kodak, to develop a forensic camera that permits the authentication of digital images. Kodak developed a "picture authentication module" for its digital DC 280 Camera, which allows digital photographic files to be tested for authenticity.<sup>6</sup>

Perhaps not coincidentally, Kodak™ chose to incorporate a digital signature standard, in effect a specialized application of PKI, into its product. The digital signature technique used in the Kodak™ DC 280 is identically the digital standard of the Digital Signature Guidelines endorsed by NIST.

Kodak's system has three components: 1) authentication "firmware" on the camera; 2) authentication software on a personal computer; and 3) a simple public key management system to enable a trusted third party or third party proxy to verify authentication images.

Briefly, a unique key pair is stored on each individual camera, with the private key confined to the camera from the start. Following the logic of digital signatures (which can be applied to any digital record, as this camera invention shows), the authentication process "signs" captured jpeg files. Each image is jpeg-compressed by the standard camera firmware. A secure hash algorithm is run on the data, generating an image digest. The digest and camera's public key are input to the digital signature algorithm, which produces the digital signature for the image. The image file is written to the camera memory card, the digital signature and the camera's public key are written to the image file's authentication tag, and the process is complete. Such a process is repeated for every image captured.

If an image is altered since it was created, it will not pass an authentication test carried out by the authentication software, which utilizes a hash algorithm.

These facts about the Kodak™ camera are discussed not so much to give details of a digital photographic authenticity solution, but to point out that PKI technology can be used not only to authenticate files such as traditional business records, but anytime there is a digital file.

## CONCLUSION

The digitization of information marks a “societal sea change.” Our modern legal system evolved recently, but nevertheless, since its inception it has based its tests for authenticity on an age-old paradigm of analog informational records.

Now, more purely stored and easily manipulated information is pervasive in our society’s informational records. All these records -- used to document communications, transactions and the appearance of reality – must be capable of “authenticity testing.” Otherwise, Tribunals will be unable to provide their most basic function.

Accordingly, courts must become aware of the demise of the old authenticity paradigm, simultaneously acknowledging incipient solutions for authentication which are possibly superior to the old regime.

---

<sup>1</sup> Jack B. Weinstein & Margaret A. Berger, Weinstein’s Federal Evidence, § 901.02{3} (Joseph M. McLaughlin, ed., Matthew Bender, 2d ed. 1999).

<sup>2</sup> See U.S. v. Mojica, 746 F.2d 242, 244-245 (5 th Cir. 1984).

<sup>3</sup> Weinstein & Berger, supra n. 1, at § 901.07{3a}. See U.S. v. Biggins, 551 F.2d 64, 67 (5 th Cir. 1977); U.S. v. Lance, 853 F.2d 1177, 1181-1182 (5 th Cir. 1988).

<sup>4</sup> U.S. Department of Commerce, National Institute of Standards and Technology FIPS PUB 186-1, <http://www.itl.nist.gov/fipspubs/by-num.htm>.

<sup>5</sup> [http://www.abanet.org/scitech/ec/isc/digital\\_signature.html](http://www.abanet.org/scitech/ec/isc/digital_signature.html).

<sup>6</sup> The discussion of Kodak’s technology is taken from a “whitepaper” on its website, “Understanding and Integrating KODAK Picture Authentication Cameras.”

[Back to Top](#)

---

**George Paul** is a partner in the Business Litigation Section of Lewis and Roca LLP in Phoenix, AZ. Paul is Chair of the firm's E-Discovery and Data Management Group. He recently coauthored a book for the American Bar Association, *The Discovery Revolution: E-Discovery Amendments to the Federal Rules of Civil Procedure*, which was released in December of 2005.

In addition, Paul has written numerous articles on the subject of electronic records; has chaired several CLE and American Bar Association panels on the topic, and is a frequent national lecturer on the topic of E-Discovery.

He is currently active in the ABA's [Section of Science and Technology](#) (former Council Member), the [ABA Litigation Section of Litigation](#), and the [Law Practice Management Section](#), where he will be speaking at [ABA TECHSHOW 2006](#). Paul is founder and past Chair of the Arizona State Bar's Section of Internet, E-Commerce & Technology Law.

[Current Issue](#) | [Article Archives](#) | [Subscribe](#) | [Advertise](#) | [Contribute](#) | [RSS/XML](#) | [Feedback](#)

© 2003-2006 American Bar Association -- [Copyright Statement](#) | [Privacy Statement](#)