

BUILDING GOOD ELECTRONIC EVIDENCE

NOW THAT E-RECORDS ARE LEGAL,
HERE'S HOW TO MAKE THEM RELIABLE

With the passage of the Electronic Signatures in Global and National Commerce Act, the law is more settled than ever before: e-records are on par with their paper counterparts for most purposes and in most jurisdictions. While legal, however, the kinds of data compilations that companies often use may not necessarily protect their interests or properly document their business or governmental activities. In essence, having an electronic record is quite different from having a complete, trustworthy and authentic electronic record.

The world of e-records is replete with shades of gray. At one end of the spectrum, there are mere "compilations of data" that are not particularly useful. At the other are reliable electronic records that possess all the indicia of acceptable evidence. Simply put, the electronic world creates a variety of records – some good and some bad. As this article explores, merely satisfying the law may not be enough when retaining electronic evidence of e-business transactions.

Merely retaining the content of transactions, without knowing the context for that content, serves as a largely useless record of that exchange. Paper records always have content merged with context: you know from the face of the document what something is and why it came into existence. For example, a purchase order on paper is one physical record. The date of execution, authorized party, subject, and any other contents that reveal its significance, are all clearly and collectively visible.

The electronic world is precisely the opposite. E-records usually consist of multiple packets of data that are rarely stored in one physical location. Quite often in cyberspace, the content is the only part of the record that is retained. That's the equivalent of taking a paper business letter, cutting off the date and salutation and putting it in one file, cutting off the signature and putting it in another file, and placing the body of the letter in yet another file. Separately, the units of those documents are rather useless for record-keeping purposes.

HOW E-TRANSACTIONS WORK

In the typical electronic transaction, the questions (the boxes that the user must fill out) are not physically retained with the answers (the data that the user types in). The answers would be a separate compilation of data and would most likely be stored in a separate physical space from the questions.

The reason for this lack of unity is simple to understand, but difficult to correct. The computing world was structured in a database-centric way to allow the parsing or separating out of information for various types of uses. Technologists were not thinking of building good business evidence. Therefore, the content of a record is almost never connected to the structure or form of the record unless the system is implemented to capture both. Technologists were promoting information functionality, not trustworthy electronic records.

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

In today's online business world, the e-signature used to sign an e-record will likely be in a separate system and most assuredly will be a separate computer file. If you need to prove that a document was executed by a particular person, that individual's mere "signature" may not be enough.

First, a signature, according to electronic signature legislation recently enacted by Congress, may be nothing more than a typed name at the bottom of the document. Second, the name will not be affixed in the traditional sense of the word to the document. Therefore, metadata (data that manages data) is needed to link the questions with the signature. If the metadata has not been retained, proving assent to the terms of an agreement will be all but impossible. If metadata is retained, then if and when the "signer" seeks to repudiate the agreement or legitimately argues that he was the signer, metadata could be used to show the computer from which the "signature" was effectuated.

Put simply, in the electronic world, separate e-files stored in separate computers – perhaps stored in separate physical locations – together make up one record. To have one encapsulated record with the content, context, structure, metadata, e-signature, and logic requires that the record be built. Building the right record for the application is in part a technology decision, in part a legal decision, and in part a business decision.

INHERENT PROBLEMS WITH E-RECORDS

To further confound the process, the applications, formats or computer languages that have become popular in the electronic age do not possess the ability to retain and structure records in a trustworthy way. For example, HTML (Hyper Text Markup Language) may be good for retaining content but is not very helpful in retaining the template (what people saw).

Needless to say, what people see online has become more important than ever. According to the new privacy regulation for the securities industry, for example, notice of a brokerage's privacy policy must be "clear and conspicuous." It is wholly inadequate to discard or lose the precise privacy information that the customer reviewed. Such issues as retention of the form of the record that the customer viewed – and proving that the form at issue was the form in use when the transaction was completed – becomes central to prevailing in a dispute. Changes to forms, fonts, colors, and software (unless backward compatible) can and will affect the look, size and appearance. Being able to deliver the precise record that was viewed and used has great utility not only with regard to SEC compliance (and compliance with other similar new regulations) but also lessens confusion and increases trust in the transaction effectuated.

ACCEPTABLE EVIDENCE

Even if the new generation of e-record and e-signature laws has been generous in not mandating the precise record to be retained, the fact remains that incomplete, untrustworthy records will be excluded from evidence or otherwise attacked as lacking integrity.

Certain regulations have been somewhat helpful to guide companies in building the right evidence to satisfy their regulatory environment. For example, the FDA electronic record/electronic signature rule advises that, when using an e-signature, metadata must be captured "linking" the signature to the record. To comply with FDA policies, a signature that isn't logically and/or physically linked to the underlying record fails to comply with the agency's rule. So, the applicable rules should be consulted to ensure that the e-records under construction will satisfy the relevant regulator.

WHERE LAW & TECHNOLOGY MEET



CONSULTING INC.

157 LEONARD WOOD NORTH • HIGHLAND PARK IL • 60035
 PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM

USING ACCEPTABLE E-SIGNATURES

The technologically-neutral brand of laws that has evolved allows the use of any type of e-signature, provided that it evinces the users' intent to be bound by the alternative to the manual "wet signature." While that is good because businesses are free to use whatever type of technology they deem necessary under the circumstances, the fact remains that not all e-signatures are created equally. For example, "xxx" at the bottom of e-mail could be sufficient to satisfy the language of the federal law on electronic signatures (commonly known as E-Sign). However, it provides little verification of the signer's true identity. Truly anyone could use or "forge" such a signature. Authenticity in that case would clearly be an open question.

Similarly, a typed name at the bottom of the page would seem to satisfy E-Sign, but the same concerns around authenticity and trustworthiness would persist.

Some types of e-signatures, however, can better confirm that the signer is who he/she claims to be, thereby minimizing concerns about repudiation, contracting with minors, etc. Biometric signatures – unique physical attributes like eye scans, fingerprints, or voice scans – would satisfy E-sign and provide much greater comfort in the identity and integrity of the relations. Similarly use of Digital Signatures (asymmetric cryptography or encryption sometimes referred to as Public Key Infrastructure or "PKI") allows information to be sent in an encrypted form and secured during transmission, and also allows parties to "sign" a contract with the use of a "private key." Assuming there are controls in place regarding the issuance of the Digital Certificates, use of the key pairs, and access controls, a recipient of a document signed with a Digital Signature can have greater comfort that the "signature" is authentic and that the user cannot easily repudiate the transaction.

THE PROPER SAFEGUARDS

This discussion makes clear that all electronic signatures are not equal in their inherent security, or their ability to address issues of authenticity, trustworthiness, and repudiation. Utilizing electronic signatures will require controls and procedures to ensure that e-signatures are used properly and with authorization.

For example, if companies use ID and passwords in place of a handwritten signature on paper to allow employees to change the type of investment or beneficiary on their retirement plan, then controls around access to employees' identification and passwords will be critical to prove that the authorized employee – and not another person with access to the system – effectuated the change. Additionally, metadata will be crucial to show the computer or telephone number where the change originated. Such ancillary information, if captured, can provide great support and evidence for the event. Failing to have the metadata makes authentication difficult, and may undermine the transaction by forcing a party to rely on a "signature" that can be easily challenged.

When making decisions regarding the type of electronic signature utilized, companies should consider the need to rely on it in the future and the ability to prove identity and authenticity as well as to preempt issues that may arise regarding the veracity of the signature or true identity of the "signer." In that regard, there is a need to understand the relative merits of the various kinds of e-signatures to be able to make the right choice for the application at issue.

WHERE LAW & TECHNOLOGY MEET



CONSULTING INC.

157 LEONARD WOOD NORTH • HIGHLAND PARK IL • 60035
 PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM

So here we are in a world that allows business to happen with the use of a telephone line and computer. Business and government function in an anonymous electronic fashion, where information free-flows around the globe and where business partners can be introduced on a third party exchange in cyberspace. The parties never meet and remain faceless to each other throughout their relationship. In such a world there is a profound need to have good evidence available to document business events.

There are a whole host of internal business process (HR functions, Sales Information, e-filing with regulators, etc.) that are now conducted electronically. For each of those transactions, the objective should be to build the same kind of evidence that was relied upon in the paper world. If you need good records in the paper environment, then build them in the electronic world.

Technological solutions will continue to be offered to help bridge the trust gap that currently exists when doing electronic business. As companies and consumers grow comfortable doing business solely within an electronic environment, the size and value of transactions will increase. As the size and risk of transactions goes up, so too will the need to have trustworthy records memorializing the events and activities. While the law has allowed us to make choices, companies can ill afford to make bad decisions.

The task of building good e-evidence has to move quickly up companies' priority lists. Failing to retain acceptable and trustworthy electronic business records will have devastating consequences. Companies will spend enormous resources to store e-data that may not be useable or legally sound.

***This Report was Downloaded from <http://www.KahnConsultingInc.com>
A version of this report originally appeared in *Digital Discovery & E-Evidence*.
For more information email: info@KahnConsultingInc.com
© 2002 Kahn Consulting Inc.***

WHERE LAW & TECHNOLOGY MEET



CONSULTING INC.

157 LEONARD WOOD NORTH • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM