

Research



Hewlett-Packard Company  
3000 Hanover Street  
Mail Stop 20BJ  
Palo Alto, CA 94304  
[www.hp.com](http://www.hp.com)

**EVIDENTIARY BENEFITS AND BUSINESS  
IMPLICATIONS OF WRITE-ONCE-READ  
MANY (“WORM”) OPTICAL DISK  
STORAGE FOR RECORDS MANAGEMENT**

*By: Cohasset Associates, Inc.*

**Table of Contents**

Introduction ..... 4

Legality of Electronic Records..... 5

Foundation for Making “Good” Evidence ..... 5

WORM Characteristics ..... 7

Using Evidence with Confidence ..... 8

Inadmissible Hearsay & Business Records Exception ..... 8

Admissibility vs. Credibility..... 10

Chain of Custody ..... 11

Excluded E-Evidence ..... 12

The Challenge of Electronic Records..... 13

Challenges to E-Records ..... 14

Potential Challenges of Electronic Records (Chart) ..... 16

Trial Within a Trial..... 17

Battle of the Experts ..... 18

Costs Associated with a Trial Within a Trial (Chart) ..... 20

Disruption to Employees ..... 20

Losing the Battle ..... 21

Incentive to Attack E-Records ..... 22

Why Retain Records if You Can’t Use Them ..... 23

WORM Use in Regulated and Non-Regulated Environments ..... 24

Defense to Spoliation ..... 25

Table of Contents (cont.)

International Legal Environment.....	26
Conclusion.....	28

## Introduction

Cohasset Associates, Inc. was asked to explore the potential evidentiary benefits of Write Once-Read Many (“WORM”) Optical Disk storage for records management. Accordingly, this white paper explores whether the inherent characteristics of WORM (once records are memorialized in the process of “writing” to optical disk) provide potential benefits to records stored on such media in the context of litigation. As the paper details, the “non-rewriteability”<sup>1</sup> of WORM can make records stored on WORM more resilient as evidence, if and when challenged in a legal dispute.

Initially, it is important to understand that the laws generally allow for the use of electronic records (stored on various types of media) provided that they are trustworthy, authentic, accurate, complete, etc. Although these laws and regulations typically do not mandate the use of specific technologies, document formats and storage mediums, this White Paper explores whether there are, nonetheless, compelling reasons to consider the use of WORM media for records that may be used in any formal proceeding, (audit, investigation or lawsuit).<sup>2</sup>

---

<sup>1</sup> Any record can be altered with enough effort and knowledge of the technology. In that sense, any storage medium is vulnerable to intentional alteration when security and internal controls fail. However, for WORM to be altered, it would take substantial efforts, including in-depth understanding of the technology and unfettered access to special hardware and software. The knowledge, expertise and access necessary to alter records stored on WORM media is generally not possessed by either a company’s Information Technology professionals or technologically sophisticated employees.

<sup>2</sup> There are many “rewriteable” storage mediums that include, but are not limited to, RAID, magnetic tape, hard drive, etc.

Companies retain records for a variety of reasons. Records are used to document the activities of the business whose “life” may outlast the employees who created them. In that sense, records are the “memory” of the business. Records are retained to comply with laws and regulations that mandate records retention. They also are retained to defend the company in the event of an audit, investigation or lawsuit in both regulated and non-regulated industries. To fully understand record value and integrity, one first needs to understand what makes “good” or acceptable evidence.

### **Legality of Electronic Records**

It is important to point out that for most reasons (with fewer exceptions everyday) electronic records are acceptable and on par with their paper counterparts. Federal, state and local laws and regulations specifically allow for the use of records stored electronically. State and Federal Rules of Evidence and Civil Procedure allow “non-original” Records to be admitted into evidence as if they were originals. In fact, recent passage of the Electronic Signatures in National and Global E-Commerce Act at the Federal level and the Uniform Electronic Transactions Act in various states make clear e-records are here to stay and cannot be denied their legal legitimacy.

### **Foundation for Making “Good” Evidence**

In order for a record to be “good” and useable evidence, it must be authentic or genuine—that is it “must be what it purports to be.” It also must be trustworthy, reliable, accurate and complete. Electronic records need to remain trustworthy and reliable during their entire lifecycle- from creation to disposition. The value of a record to the

company in the context of a lawsuit is that it is capable of being relied upon as containing accurate and believable information and that it is authentic. If it satisfies these criteria, it should be allowed into evidence. Failure of a record to be trustworthy in the litigation context provides the basis for a Court to exclude the record in its entirety from consideration. Additionally, any question about record trustworthiness allows an adversary to attack the credibility of its contents, and thereby, potentially minimize its impact.

In order for electronic records to remain trustworthy and accurate throughout their lifecycle, there must be controls in place to prevent intentional and unintentional changes to the record. As articulated by the United States Court of Appeals, 11<sup>th</sup> Circuit, electronic records are admissible if they are “kept pursuant to some routine procedure designed to assure accuracy.”<sup>3</sup>

As will be discussed in greater detail in the sections that follow, one of the biggest challenges to the trustworthiness of electronic records is that they can be generated at any time, by anyone, saying anything. In some cases, meta-data (the data that manages the data) can provide insights into “the when” and “the what” and “by whom.” Additionally, to the extent a record is not capable of being altered after it is stored (or alteration is very difficult, as is the case with WORM) that tends to provide confidence that the record will be trustworthy whenever it is accessed in the future.

---

<sup>3</sup> United States v. Jodi Glasser, 773 F.2d 1553 (11<sup>th</sup> Cir., 1985).

A forged signature on a paper record is relatively easy to detect. In contrast, electronic records are easy to fake because on their surface they all look like an original. An e-record may have been created ten minutes, or ten years ago and, without proof that it is authentic and trustworthy, such a recorded can be easily attacked. After all, what evidentiary benefit is there to the paper printout of the words, "I will buy 3000 Lilies—Signed Dylan, April 17, 2000," if you don't know when it was created and by whom? A printout of such an e-record is easily attacked without more evidence to show that it is accurate and that Dylan entered into it on the date stated. To the extent that any record is not believable to either a judge or jury, it is of little evidentiary value to the company.

### **WORM Characteristics**

Several types of WORM technologies are widely marketed. The two common features with all WORM media is 1) when "writing" or storing records there is a change to the storage medium, and 2) the coding on the WORM disk "communicates" with the hardware during the storing process to prevent alterations to existing records. Thus, the name "Write Once." The WORM functionality was specifically designed to limit "rewriting" once the record had been stored on the WORM media. This is accomplished by the hardware used to "write" to the medium working in concert with the storage medium itself to deny any changes following the initial act of storage.

### **Using Evidence with Confidence**

Companies and government retain records to be able to use them for whatever purpose that they may be needed in the future. Accordingly, records serve to protect rights, resolve disputes and achieve regulatory compliance. However, records lacking trustworthiness may be an issue when used in any formal proceeding such as an audit, investigation or lawsuit. While an attack on record trustworthiness will not occur in every case, there is a need to maximize the likelihood that records are acceptable and useable for whatever purpose, whenever they are needed. If companies go through the trouble of methodically retaining records, they should be confident in their ability to use them to protect or support the company's business activities and legal positions.

### **Inadmissible Hearsay & Business Records Exception**

Companies generally rely upon the Business Records Exception to get records admitted into evidence that may be otherwise excluded due to the Rule Against Hearsay. The Business Records Exception requires that records be created in the ordinary course of business documenting an activity that is usually memorialized in a record, at about the time the event, documented in the record, took place.

Courts have applied the business record exception to the use of computer-generated records. An example is a contract case where one party sought reimbursement for engineering services and the other party, in refusing to pay, contended that due to the destruction of certain potentially relevant electronic business records, "it was impossible to

determine whether the hours claimed actually had been worked and whether certain laboratory tests actually had been performed.” In addressing the electronic records evidentiary issues, the court stated, *“trustworthiness or reliability of the records is guaranteed by the regularity of their preparation and the fact that the records are relied upon in the transaction of business by those who keep them. Admission of such evidence is conditioned upon such proof that the document comes from the proper custodian and that it is a record kept in the ordinary course of business made contemporaneously with the events by persons having a duty to keep a true record...”*<sup>4</sup>

In another case, involving mail fraud, extortion and acceptance of illegal bribes, the government sought to have e-mail messages essential to the case admitted into evidence. The e-mail was successfully attacked as not satisfying the Business Records Exception. In excluding the e-mail, the Court noted, *“the government first sought admission of the E-mail message as a business record exception...to this end they laid the proper foundation that the print out of the E-mail was authentic and accurate, and it was Carey’s routine practice to send such E-mail messages to co-workers in the relevant ‘loop’ immediately following an important phone conversation with a client. This court nevertheless concluded that this foundation was insufficient enough to warrant admission of the E-mail message as a business record.”*<sup>5</sup>

---

<sup>4</sup> Kettler & Scott Inc. v. Earth Technology Companies, Inc. 449 S.E. 2d 782 (Sup. Ct.-VA, 1994)

<sup>5</sup> United States of America v. Mark S. Ferber, 66 F. Supp. 90 (D Ct.- MA, 1997)

In a third case, the plaintiff, suing for discrimination, attacked e-records offered as evidence, asserting that the records were made after-the-fact. The court, in recounting the plaintiff's position, noted that, "*by their very nature insufficiently trustworthy to fall within the hearsay exception contemplated by Rule 803 (6). Brown noted that the documents are not date stamped, are computer printouts rather than business forms, and are not signed.*" <sup>6</sup>

Systematically managing and methodically storing records promotes their use as "business records." To the extent that a litigant can state that they use WORM media, because of its security features which promotes data integrity, such a fact would tend to support their use of their records as "good business evidence."

### **Admissibility vs. Credibility**

When a record is offered as evidence in any formal proceeding, it really undergoes two separate challenges: 1) whether the record should be allowed to be a piece of evidence to be considered in the case (admissibility); and 2) does it deserve to influence or affect the conclusion of the Court (credibility)? In other words, even if a record gets over the initial admissibility hurdle and is considered satisfactory to be allowed into evidence, the credibility of the record's contents can be challenged. For example, how do we know that the electronic record was not altered two weeks after the transaction to say "1000" when the original transaction called for a quantity of "10"? How do we know or, more importantly for this example, how can we prove that the quantity of units in the transaction was not altered or some important delivery terms

---

<sup>6</sup> Brown v. Town of Chapel Hill, 1996 U.S. App. Lexis 4849 (4<sup>th</sup> Cir., 1996)

were not inadvertently deleted? In a legal proceeding, the mere suggestion of alteration may diminish a record's utility as evidence and force the party responsible for the record to then offer evidence regarding the record's trustworthiness.

### **Chain of Custody**

Central to evidentiary trustworthiness and credibility is that the record can be accounted for during its life—sometimes referred to as the Chain of Custody. Records that are out of the control (and practically speaking incapable of being altered) of the person with an interest in changing its content are less likely to be intentionally altered. Such records have greater potential evidentiary benefit because they are less likely to be successfully attacked as fabricated or altered. A record that could be changed at any time, by any person, for any reason is also easier to attack as lacking credibility than a record that is stored at about the time the underlying transaction took place and is retained on a medium designed to minimize intentional or accidental alteration.<sup>7</sup>

In one case, the Court considered excluding electronic records because the testimony “demonstrated a weakness in the security measures” taken by a bank to control access to computer terminals. There is a need to have security procedures in place for all records, including those stored on WORM. The storage of records with a WORM functionality on a medium that promotes record security tends to decrease the likelihood of a legal attack on any specific record's integrity based upon lax record control.

---

<sup>7</sup> Chain of Custody can also be shown by a computerized audit trail, capturing meta-data to show who created it, who edited it, when it was modified, etc. However, use of computerized meta-data to show trustworthiness may be costly and time consuming.

### Excluded E-Evidence

Computer and electronic records are generally admissible with the proper foundation.<sup>8</sup> However, there are many cases where electronic records have been challenged in Courts and the records have been excluded. An example, of the importance of laying the proper foundation is a case where the Court of Appeals overturned a bank fraud conviction because the Court concluded that there was inadequate foundation to allow the electronic records into evidence, upon which the conviction was based.<sup>9</sup> In so doing the Court noted, *“Nothing in the testimony, however, demonstrated that the computer equipment at the data center was standard and that the method of preparation at the data center indicates trustworthiness...there was nothing in [the] testimony which described how the transaction information was entered into and processed through the computer system at the data center which verify the accuracy of the output.”*

In a complex patent infringement case, the Court excluded an e-mail record that was central to the defense of a company because the Court concluded that the record did not have the makings of a good piece of evidence nor was the record “kept in the ordinary course of regularly conducted business”.<sup>10</sup> The Court might have decided this issue differently had the e-mail been “legitimized” by actively managing it in the company’s records management system. How the record was made, if the computer performed as intended, whether the record was

---

<sup>8</sup> United States v. Catraban, 836 F. 2d 453 (9<sup>th</sup> Cir., 1988)

<sup>9</sup> The People of The State Of Illinois v. Arthur Bovio 455 N.E. 2d 829 (Ct. App. –IL, 1983)

<sup>10</sup> Monotype v. International Typeface, 43 F.3d 443 (9<sup>th</sup> Cir., 1994)

trustworthy and if the record was altered are all issues that may have affected this case.

### The Challenge of Electronic Records

Understanding electronic records and the explaining them to a jury can be very challenging. How e-records are created, stored and reproduced is complex and varies depending upon the technology and record at issue. In that context, the less explanation required the better. The objective should be to minimize the issues that may arise and then have simple explanations to any questions that arise (to the extent that they exist).

For example, it is a complex undertaking to explain how records are captured and stored, how they are converted from readable text to a bit map image and then completely reproduced. To the extent that an imaged record is challenged and an explanation is required, there will be time and cost associated with an issue that is only tangentially related to the real substantive issue.

Additionally, the expanding universe of what is considered an electronic record also creates challenges. For example, an electronic record may consist of multiple data streams located in several different systems, which are physically located in different places. Further, there may be meta-data records that are separate records but nonetheless describe when and how the underlying record came into existence, if and when the record was altered or edited and by whom, etc. In a sexual harassment lawsuit, the case hinged upon a computer-generated employee evaluation.<sup>11</sup> When discovery was conducted during the case,

---

<sup>11</sup> Maguire v. Acufex Microsurgical, Inc., 175 F.R.D. 149 (D.Ct.-MA, 1997)

the evaluation was produced albeit missing a key paragraph that had been mysteriously lifted from the final document. Only after the drafter of the original document was deposed and his personal computer searched did it become apparent that another co-worker had altered the original. Without finding the creator and the original located on a separate computer, the fraud would have been successful. Had the original been captured as "the original" on a "non-rewriteable" media, such intentional conduct could have been thwarted.

The complexities that are inherent in e-records prohibit a simple explanation about their creation, transmission, retention and reproduction to a jury who may not be technologically savvy. The less that needs to be explained the better. From a legal practicality perspective, if records cannot be altered once they are stored, there is less of a need to have an "expert" explain meta-data to show that, in this case, the record has remained complete and is authentic and accurate today. If records cannot be inadvertently deleted, no one will have to explain that a disk, for example, remains complete today and prove the same. In this regard, storing records on WORM media offers some real potential benefits.

### **Challenges to E-Records**

An attack on an e-record can be directed at any part of the record lifecycle, including its creation, retention, migration, or reproduction. If the content of a record is harmful, an adversary will seek to exploit weaknesses in the system that managed the record. The less weaknesses in the system, the greater the likelihood of successfully using the record.

From a time perspective, most of a record's lifecycle is spent being "stored". This is also the time when records are most vulnerable to intentional and unintentional changes. To the extent that a party can quickly dispose of any challenges attacking the storage or retention process by stating that a record could not be altered (short of a conspiracy involving technology experts and company insiders) because it was stored on WORM media, such a statement may preempt an expensive and time-consuming inquiry into record trustworthiness. Further, use of WORM media greatly minimizes the possible challenges related to intentional or unintentional changes to the record, whether by a computer virus, disgruntled employee or common mistake.<sup>12</sup>

Clearly, one substantial benefit of WORM media is that once the image or record is memorialized on the medium, there is no simple and practical way to alter the content of the record.<sup>13</sup> WORM "write once" security features greatly diminish the world of possible challenges to record trustworthiness. Unless there is proof that someone with an interest in the outcome of the dispute possessed the technological understanding and had access to all the software and hardware necessary to change a WORM record, a Court would be hesitant to entertain such a time consuming "fishing expedition." In other words, the Court would take "notice" of WORM's built-in security features. Unless someone can show that security was breached, the Court would

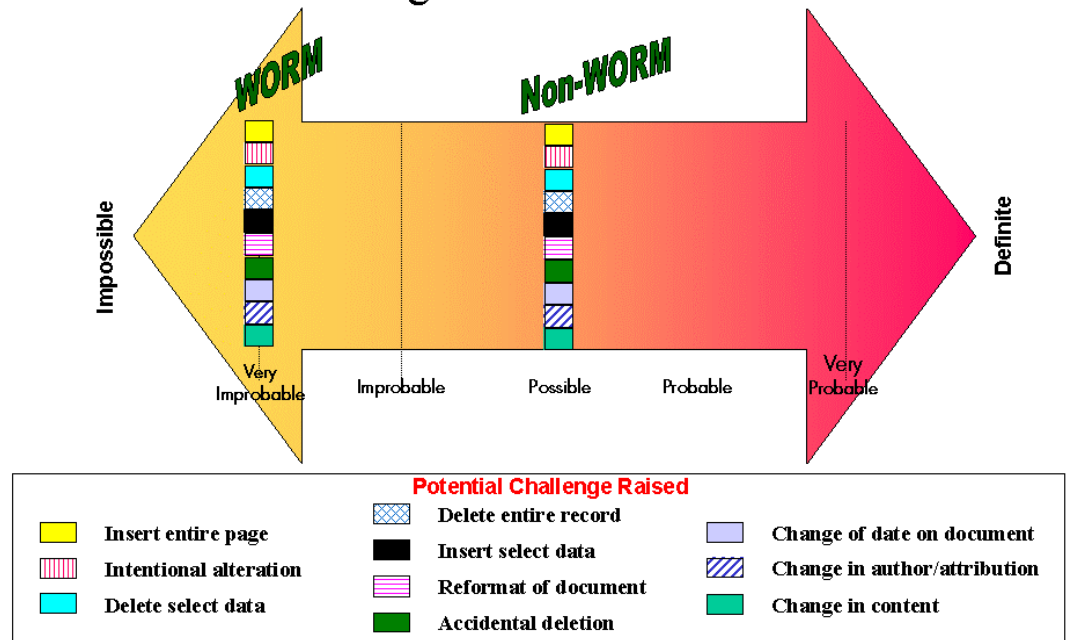
---

<sup>12</sup> A recent survey entitled; "Human Error is Culprit in Data Loss" indicates that "users themselves damage three times more data than do viruses, floods, lightning, earthquakes and hurricanes combined."

<sup>13</sup> That is not to suggest that once stored on WORM, the record will remain permanent forever on its original media. All Electronic Storage Media have a limited useful life. After a specified period of time data needs to be "refreshed" by copying the contents onto new media or risk losing access to or contents of records.

be hard pressed to allow such an inquiry without a very compelling reason. In that sense, the Court may demand more proof of the potential for alteration when the records are stored on WORM before it entertains a closer review of the system that managed the record.

### Likelihood of Losing on Issues Raised About Altering Stored E-Records



A party can challenge any issue at trial, including issues related to WORM. The chart indicates the likelihood of losing on a challenge to e-records at trial and whether or not the results will differ if the record is stored on WORM v. Non-WORM.

### Trial Within a Trial

In the event that litigation arises, companies may need to rely upon their retained records to prove or refute any number of issues. If an adversary contests the veracity of a record by attacking 1) the process by which the record was managed, 2) its content or 3) the reason or timing of its creation, the parties may be forced into a "trial within a trial." A "trial within a trial" diverts attention away from the big issues in the case to smaller side issues. It can be an expensive and time-consuming exercise to attack or substantiate a record that one side wants included and the other side wants excluded from evidence.

For example, the Court may be forced to address when the record was created, whether the record was altered since its creation, whether the record is a recent fabrication or whether the record is complete, etc. To the extent that a company needs to rely on its records as evidence, it needs to be confident that the company will not be challenged to use them that it can rely on them as needed. To the extent that records are challenged, companies need to prevail, but in the process of so doing, they need to minimize the time and expense of defending their records. Clearly, it would be optimal if all the records a company sought to use in a legal proceeding would be unequivocally accepted without any discussion. However, that is not reality today. And in the future, challenges to e-records likely will be done far more frequently than challenges to paper records because there is more "opportunity" to attack e-records. Using a durable storage medium to minimize the possible challenges would provide meaningful added protection.

While, there is no precise guidance regarding the hard costs that would be associated with a “trial within a trial,” there are several significant costs that a party could be forced to pay. The additional costs associated with the admissibility of evidence could include: Expert witness fees, additional lawyers’ fees, deposition costs, travel expenses, etc. Additionally, in certain circumstances, the Court will force the losing party to reimburse the prevailing party for reasonable expenses of the “trial within a trial.” These expenses could be doubly painful.

### **Battle of the Experts**

Where technology is involved, as with e-records, litigants are likely to rely on experts to help them prevail in their dispute. Costs associated with expert witnesses can be quite substantial. While there is little case law that addresses the costs associated with an expert witness used to authenticate or attack electronic records, there is a body of case law that deals with what Courts deem reasonable when one side seeks to be reimbursed for expert witness fees generally. A review of Court cases demonstrates that Courts have found experts’ fees ranging from a few thousand dollars to in excess of \$100,000 to be reasonable.<sup>14</sup>

*In Re: General Instrument Corporation Securities Litigation*, a computer forensics expert was hired to offer testimony regarding the cost and time necessary to produce electronic records. The Court noted that there were more than 60 depositions taken. Additionally, in the sexual harassment case cited earlier, the Court noted that the defendant “*was forced to pay the costs of several depositions, spend significant sums in*

---

<sup>14</sup> Cohasset Associates, Inc. has been hired as an expert in cases where records and electronic records have been at issue. In such cases expert witness fees amounted to tens of thousands of dollars.

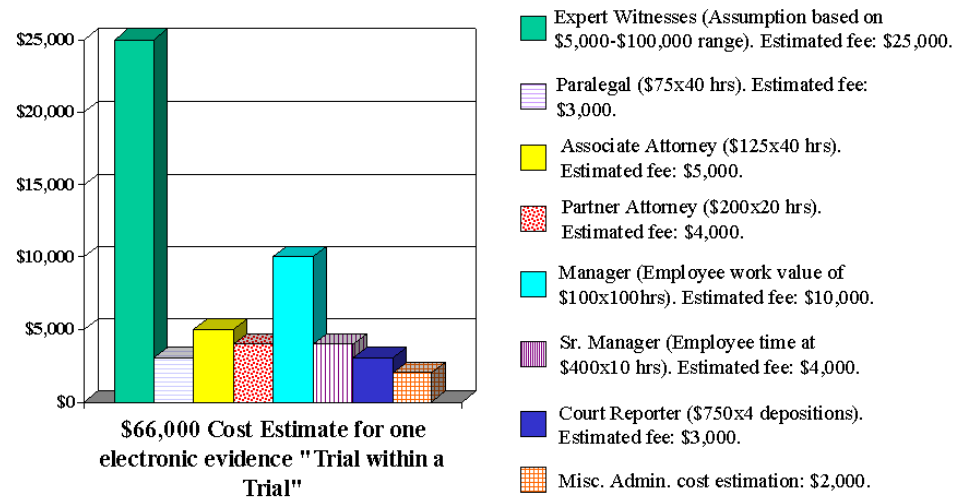
*order to recreate from computer files and backup tapes the original un-edited version of the ... memorandum to determine its history, when it was edited, and on whose computer terminal.”<sup>15</sup> While there is no indication of specific costs in either case, it was likely thousands, if not ten of thousands of dollars or more that were spent, just to be able to use electronic records. (Below is a chart of some of the costs that may be incurred when forced into a “trial within a trial” on the admissibility of electronic records.)*

It is a clear axiom: The more “unknowns” and questions about record integrity and the possibility of alteration, the greater the need to know what happened in the particular situation to ensure that the record at issue is trustworthy. In turn, if experts will be needed to explain how a technology works, whether the record was altered and/or what meta-data is stored to show any and all changes to the record, potentially several experts may be needed. While such fees may need to be figured into the overall cost of using certain technologies, what is clear is that such expert witness fees are only part of the cost equation.

---

<sup>15</sup> See Maguire.

## Costs Associated with a “Trial Within a Trial”



### Disruption to Employees

In addition to the potential need to rely upon expert witnesses in the electronic record authentication process, there also may be a need to get assistance from various employees as well. Employees involved in the original transaction and creation of the records related to the transaction will need to be questioned. Members of the records management staff, technology services and the affected business unit(s) may need to address issues related to company policies, security procedures, system configuration, employee ID standards, meta-data conventions, etc.

Involving employees in the litigation process takes these otherwise productive employees away from normal business activity. They will be required to understand the issues in the case, perform an investigation to determine what happened in this particular matter, prepare for depositions and perhaps testify at trial. Involving several employees for several days each also can equate to a substantial expense.

Additionally, in the typical litigation situation, litigants may seek to depose the senior-most person from the corporation with knowledge of the issues (perhaps in this case the CIO, CTO, CSO and the head of the business unit involved in the dispute). In any event, that requires a member or several members of senior management to take time away from their schedule to deal with a matter, which will likely not contribute anything to the future success of the company.

For each employee deposed in any formal matter or required to testify, a lawyer will be required to work with the employee. That further increases the cost of legal representation. It is conceivable that dozens of "employee days" (including senior management time) may be wasted merely to ensure a Court recognizes and allows the company to use its e-records.

### **Losing the Battle**

The above analysis does not address whether you prevail or not in your quest to be able to use company records. Rather, it addresses what is the possible cost items associated with proving to the Court that records are trustworthy and authentic and deserve Court recognition. On the later point, what happens if the company, through its employees and "hired guns" fails to convince the Court that records should be allowed into evidence? Imagine spending millions on state-of-the-art technology, storing vast quantities of records but not being able to use them to protect company interests? While not an "every case" occurrence, challenges to e-records happen regularly and some e-records do get excluded from evidence. Further, challenges to e-records

will likely be increasingly more frequent than they are with paper records -- because there is more opportunity to challenge e-records.

Losing an attack on a company's e-records has two distinct impacts. First, if you lose, the company is prohibited from using its records in the case in which they were offered. This is no different in the paper world. Second, if you lose, usually it is an attack on the system that retains or manages the record. Once successfully attacked in one case, records stored by the same processes or system can be similarly attacked in other cases in the future. In that sense, losing an attack on e-records can have a profound long-term impact on the utility of records as evidence and comfort with investment in technology that creates, retains and transmits records.

#### **Incentive to Attack E-Records**

Compounding the problem is that if the e-record is really helpful to the company, the adversary has greater incentive to attack the e-record. If the content is unassailable, the adversary will go after the process by which the e-record is managed. In other words, good evidence for one side is a reason to attack the e-record in any manner possible. "Really good" evidence is an invitation to aggressively attack the e-record. Any possible way to call into question the e-record is a way to minimize the e-record's effectiveness as evidence. If the Court and jury know that the record has remained unaltered since creation, such as through the use of WORM media, perhaps the most major avenue of attack is immunized or even eliminated.

### **Why Retain Records if You Can't Use Them**

Given the expense associated with e-records storage and retention, if there was a chance that e-records would be excluded from evidence because of the storage used, there would be ample reason to consider using another storage medium. While WORM is not the only acceptable electronic storage media, the fact remains that once the record is stored on WORM, tampering with a record's content is improbable, nearly impossible and certainly more difficult than with non-WORM media. The reality is that WORM seeks to allow only one "writing" of the record while most other mediums are sold by promoting their "reuse" and "overwrite" capabilities.

Computer systems may be configured to show that records stored on non-WORM media were not altered or that the record remained complete throughout its retention. However, in such circumstances, someone still has to testify about the security procedures in place to show it was not altered in this case. Further, Information Technology (IT) personnel would be called upon to testify about, for example, the meta-data retained by a particular system in order to show that the records remained complete and trustworthy and were not altered during their retention. Accordingly, the company would be forced to explain why its records are trustworthy and should be allowed into evidence (the "trial within a trial").

### WORM Use in Regulated and Non-Regulated Environments

The federal and state governments appear to be hesitant to mandate the use of any specific technology, because 1) it forces one company's product over another; and 2) technology is continuously changing. WORM storage media has been used in virtually all industries since the advent of electronic records management in the early 1980's. The regulators in certain highly regulated industries have required the use of a WORM functionality in the management of certain electronic records under their jurisdiction<sup>16</sup>. For example, companies (brokers/dealer/members) that are regulated by the Securities and Exchange Commission rules and regulations use WORM Optical Disk to comply with relevant e-records laws and regulations.

SEC Regulation (17 CFR 240.17a-4) which deals with e-records and record retention generally mandates that "the electronic storage media must: preserve the records exclusively in a non-rewriteable, non-erasable format." Another of the SEC Regulation Sections indicates "If electronic storage media is used by a member, broker, or dealer it shall comply with the following requirements: ... If employing any electronic storage media other than Optical Disk technology, the member, broker, dealer must notify its designated examining authority at least 90 days prior to employing such storage media."<sup>17</sup>

These two sections read together can be interpreted to mean that WORM Optical Disk is an acceptable medium that satisfies the

---

<sup>16</sup> Three such agencies are the Securities Exchange Commission, the Commodities Futures Trading Commission and the Nuclear Regulatory Commission.

<sup>17</sup> Presumably, the Regulation mandates notice to its regulators to determine if the chosen media is acceptable. While the Regulation does not advance a particular medium it seems to strongly favor Optical Disk, which is "non-rewriteable" and "non-erasable."

regulation and does not require the user to advise their regulators of alternative electronic media use. Many in the securities industry view WORM optical media as the ONLY medium that is “non-rewriteable” and “non-erasable” and, therefore, the only one that is SEC compliant.

The security and “non-rewriteable” technological features may be worth consideration in both regulated and non-regulated industries -- where records may be subject to periodic review, where records need to be organized in a manner to have methodical access and retrieval or where certain records will likely be needed as a business record or evidence. Having comfort that records are trustworthy, because of the way the records are managed and the technology on which these records are stored, provides comfort that the records would be viewed as authentic and trustworthy in a legal proceeding. Records that appear to be targeted in litigation, but are nonetheless hard to manage (like e-mail), also may benefit from being stored on WORM.

### **Defense to Spoliation**

There may be some additional benefit in using WORM media to defend against claims of intentional and mistaken destruction of evidence. Spoliation is nothing more than destruction of evidence. Over time more Courts have been willing to expand the application of spoliation to a wider spectrum of conduct and allow parties the right to sue for destruction of evidence. In fact, Courts in some jurisdictions allow mere mistaken and negligent conduct to form the basis of a claim for destruction of evidence. This trend is particularly problematic because the management of electronic records is complex and prone to mistakes.

The use of WORM would provide a defense to accidental deletion, since the media doesn't allow for records to be mistakenly altered, changed or deleted. The use of the media itself would form a defense. In any event, when a Court looks to companies that have disposed of relevant records in the context of litigation, whether intentionally or negligently, the Court would presumably be influenced by the use of storage technology that seeks to minimize such occurrences whether they happened or not. Use of WORM may help defeat such a claim by showing that 1) destruction was not plausible in the case of intentional conduct, and 2) that deletion is nearly impossible in the case of mistaken or negligent conduct. Finally, no matter what actually happened, the user can always assert, by the use of WORM, that it sought to ensure record integrity and took seriously its responsibility and had made a "good faith" effort to retain its records for litigation. Finally, to the extent that records are stored on WORM disks and all of the company's disks could be accounted for, the assertion that individual records were destroyed would face serious impediments.

### **International Legal Environment**

Without addressing individual jurisdictions, the evidentiary considerations in the other developed countries are similar to the United States. Various countries have been aggressive in their recognition of e-records. Legislatures in countries such as Canada, Australia and Great Britain have all sought to promote the legal acceptance of e-records provided they are trustworthy and authentic.

For example, the Canadian Uniform Electronic Evidence Act states that, " in any legal proceeding, the best evidence rule is satisfied in respect of an electronic record on proof of the integrity of the electronic record system in or by which the data was recorded or preserved."

The Australian Evidence Act abolishes the "original document rules" which "requires the production of the original document in writing." The new law states that one of the acceptable alternative ways to offer evidence includes " *a printout of computer output or a document reproducing the contents of an **optical laser disk***" (emphasis added).

### Conclusion

E-records and the alternative mediums on which they are stored are gaining in acceptance. Where the need to have sound e-records is great, any technology that bolsters trustworthiness, minimizes potential invalidation and maximizes their usefulness for any purpose is worth consideration.

There is a difference between WORM storage media and all other non-WORM media. WORM is specifically designed to ensure that once records are stored, they cannot be "overwritten." Non-WORM storage devices (such as RAID, hard drives, magnetic tape, etc.) are designed to allow or "promote" changes or alterations. While the re-write feature may be good for reusing storage media, it is bad for making trustworthy evidence. This fundamental difference in the nature of the technology makes clear that with the use of WORM: There is less

likelihood of changing the contents of a record once it has been stored on WORM:

- the less chance for alteration, the fewer possible challenges to record integrity;
- the fewer challenges to record trustworthiness, in the litigation context, the faster and cheaper disputes get resolved;
- the smaller the chance of altering a record, the greater the likelihood of trustworthiness and the higher the probability that it would be admissible in a court of law;
- and the more trustworthy the record, the more value it has as evidence.

Information about Hewlett-Packard's optical jukeboxes and HP's WORM media can be found at:  
[www.hp.com/go/optical](http://www.hp.com/go/optical)

This White Paper was prepared for Hewlett-Packard by Cohasset Associates, Inc. It was prepared under the direction of Cohasset's Senior Consultant, Randolph A. Kahn, Esq. (847) 266-0722 or [rkahn76876@aol.com](mailto:rkahn76876@aol.com)