

# RESPONDING TO THE NEW LEGAL LANDSCAPE CREATED BY TECHNOLOGY

As we near the millennium, computer technology is presenting companies with unprecedented business opportunities and also potentially significant risks. In hopes of expanding business and improving efficiency, companies are committing tremendous human and financial resources to the application of new technology. One of the primary objectives of this commitment to technology is to improve the interrelations of two key corporate assets, people and information – and thereby achieve new levels of productivity.

The application of so much new technology is predicated on an ever-expanding digitization of society. The resulting digital economy and the associated changes in how information is managed and communicated will, in turn, have a profound effect on corporate liability and risks – both what they are, as well as how they are addressed. All too many law departments view these potential liabilities and risks in much too distant or narrow context. For example, many view the Year 2000 problem (Y2K) as at least under control, if not resolved. Technically, that is increasingly true, but from a legal perspective, we are just beginning to address the issue as the first filed Y2K case, *Produce Palace v. TEC-American and All-American Cash Register*, (#97-3330 Macomb Co. Cir., MI 1997), has recently been settled.

Many do not view e-mail as an important component of their corporate memory, and as if they are not records that document business activity. And for the minority that do, most describe the process of how they manage their e-mail as “chaos”. Yet, e-mail is one of the more important and potentially damaging sources of evidence in recent litigation.

Many view the internet and their website in the popular, but limited context of an incredible interactive library rather than a communication vehicle in which the company should move cautiously due to the significant risks. Most have given little or no consideration to the extraordinary new legal risks associated with the long-term storage of digital information. In an era of incredibly rapid change in both computer hardware and software, will your company be able to retrieve what you need when you want it? Consider the consequences of technology impinging on your ability to respond to discovery, which the revised Federal Rules of Civil Procedure require your company to produce in greater quantity and in less time.

As the following case law highlights indicate, there is an acute need for corporate counsel to guide the corporation through this new risk frontier by assisting in the management of technology and managing the employees’ use and misuse of the technology.

---

## MANAGING THE MEDIUM

---

Every large corporation, almost without exception, has embraced the idea that improving lines of communication both within and outside the corporation allows companies to work more efficiently, reach customers more directly, and deliver products less expensively. However, the company needs to manage and establish clear policies to minimize risk related to the explosive use of internets and intranets by employees and customers.

WHERE LAW & TECHNOLOGY MEET

**KAHN**  
CONSULTING INC.

For example, in the case of *Comedy III Productions v. Class Publications*, 1996 LEXIS 5710 (S.D. NY 1996), the court found both the corporation and its president liable for copyright infringement based upon the offering for sale of a product (the rights to which were owned by another company) the corporation advertised on its website. Therefore, because liability can attach not only the business but also to its principals, a thorough review of all website activity should be undertaken regularly to limit exposure not only to the corporation but its management as well.

Similarly, there is a line of decisions which hold website owners responsible for the actions of independent third parties on their website. In one example, *Playboy Enterprises, Inc. v. George Frena, et al.*, 839 F. Supp. 1552 (M.D. Fla. 1993), the court held the website owner liable for copyright violations for failing to purge its website of legally protected material placed there by an independent third party without the copyright owner's permission. Therefore, if the company website allows attachment of articles or pictures to the site by employees or outsiders, then at a minimum, the site should include a written prohibition regarding attachment of any work without permission from its author or owner. Concurrently, the company should review the website to rid it of all questionable content, attachments or postings.

Because services or products offered for sale or advertised on the internet may satisfy personal jurisdiction requirements and force an unsuspecting defendant into a court far from home, the corporation should be clear about the purpose of the website and understand the potential effect of the site's content. This is particularly significant in the Internet context, where the corporate website and its content may potentially be viewed anywhere in the world. This issue was addressed in *Inset Systems, Inc. v. Instructions Set*, 937 F. Supp. 161 (D. Conn. 1996), where the court held that personal jurisdiction was established by a mere website advertisement. Therefore, corporate lawyers should review the material on a company's website to determine the legal impact the content may have. They should also ensure that the website will require a buyer to agree to choice of law before consummating any electronic transaction.

---

#### TECHNOLOGY MEETS TORT

---

When and how to digitize company records, and how long they should be kept, are questions of great import for lawyers, records management personnel and technology staff. As companies become increasingly reliant on electronic records and information, potential pitfalls must be recognized and addressed. Simply put, while the paradigm shift from a paper to a digital environment creates operational efficiencies, so too does it create difficulties which the lawyers are uniquely qualified to rectify.

For example, if an electronic message replaces a paper version, then the records management program must address the record not by the medium in which it is created or the system through which it passes but rather by the content of the message. In other words, if the record has business content and significance, it must become part of the large body of company records on a topic. Failure to retain electronic records, including e-mail transmissions, for the same period as the paper memoranda on a topic undermines the overall legitimacy of the records program and can subject the company to claims for spoliation.

In *Applied Telematics v. Sprint*, 1996 LEXIS 14053 (E.D. Pa. 1996), the court found that Sprint had destroyed records when they re-used computer storage tapes containing otherwise potentially relevant discoverable data. While some have interpreted the case as attacking the short retention period for the system containing the information at issue, others have concluded that the court allowed the claim for spoliation against Sprint because the company failed to have procedures in place to preserve relevant records and information for litigation.

To obviate risks similar to the one addressed in *Applied Telematics*, corporate counsel should:

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

- 1) Ensure that the company document retention schedules are not media-dependent, and
- 2) Ensure that procedures are in place for both paper and electronic records which suspend destruction schedules for all potentially relevant records when the corporation is faced with litigation or governmental audit or investigation.

Another technology issue ripe for the application of the expanding definition of spoliation is in the context of technology obsolescence. While originally the definition of spoliation did not expand beyond willful destruction of records, more recently courts have been far more liberal, allowing claims for what once was considered merely negligent conduct. For example, in *Kozlowski v. Sears*, 73 F.R.D. 73 (D. Mass. 1976), a spoliation case, the court noted that a record-keeping system which conceals rather than discloses information, or makes it unduly difficult to identify or locate records was the “functional equivalent of destroying records”. As corporations implement new technology, change operating systems, and use new storage media, they must also develop plans to ensure the company will retain access to the old records. Without regularly migrating information to currently accessible technology, over time vast quantities of information may be trapped on old computers or storage devices. This situation could potentially give rise to the next generation of claims for spoliation, especially in light of the approach taken in the *Kozlowski* case.

Given the fact that it is within the law department’s purview to protect corporate interests and comply with orders of courts and discovery obligations, the lawyers need to ensure that technology personnel understand the legal issues and have a plan in place to allow access to corporate records for as long as retention schedules dictate, sometimes with short response times.

---

#### CONTROLLING RISK WITH PROCEDURES

---

Companies rely more and more on optical storage and imaging systems, which can create and store records without an “original” being created until the record is retrieved and printed to paper. This reliance requires confidence that such records will be useable and acceptable to government agencies and/or courts. That is to say that the various complexities, both technological and evidentiary, unearthed by the use of optical disk storage must be understood before plans are implemented to rely on such a system for official company records. While the laws regarding the acceptability of “good” optically stored records are commonplace, the existence of such laws does not mean that such records will be allowed into evidence if and when needed. In other words, while courts and government agencies seem to be more comfortable with records stored on optical media generally, admissibility of specific records will depend on integrity.

For example, in 1997 both the IRS and SEC issued positions on the use of optical disk storage. Those positions make clear that for optically stored records to be acceptable, they must be created on imaging systems which have procedures and policies in place to ensure record accuracy, integrity and completeness. This has very little to do with hardware, which is assumed to be adequate, but rather that certain procedural protections and policies are in place to ensure record trustworthiness. Under both the SEC and the IRS positions, the use of optically stored electronic records will depend on whether there are reviews of image quality, accuracy, completeness and indexing, among other things. All of these elements lend credibility to the process by which records are stored and make them “good evidence”. While attacks on record completeness and integrity are not common in the litigation context, if an optically stored record is successfully attacked by creating doubt about whether the imaging system captures “all of the record” (a complex discussion involving the underlying technology which is beyond the scope of this article), all records captured on the same system are thereafter vulnerable to attack. Policies and procedures should be drafted which address the various issues of record integrity and the system must be periodically reviewed and audited to make sure that it is “making” good records.

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

---

## CONTROLLING LIABILITY THROUGH POLICIES

---

By now, you have heard about the numerous high-profile discrimination lawsuits based either in whole or in part on inappropriate e-mail messages sent through the company network. The liability and negative public relations exposure exacted when a company fails to stop the transmittal of inappropriate jokes or images have cost many business millions of dollars. In order to rectify this problem, policies must be drafted and strictly enforced to limit use of all electronic mail to business purposes only, with specific prohibitions on certain content. Thereafter, the system should be audited for compliance and all violations of the policy should be uniformly punished.

While the aforementioned suggestions are seemingly an easy solution to a daunting problem, corporations may be reluctant to take the prescribed actions. Such reluctance may be due to concerns regarding the legal authority to monitor employee electronic communications or the belief that current corporate policy suggests that employee communications will be private and the e-mail system can be used for non-business purposes.

However, there is support in recent court decisions for implementing the more aggressive policies which raise eyebrows in the short run but may benefit the corporation substantially in the long run. For example, *Smythe v. Pillsbury*, 914 F. Supp. 97 (E.D. Pa. 1996), is a case in which a former employee sued his former employer for invasion of privacy; after Smythe's e-mail was intercepted and he was fired, he sued. Despite a company policy which stated that all e-mail communications would remain confidential and privileged and could not be intercepted and used against the employees as grounds for termination, the court refused to recognize the contractual invasion of privacy claim. The court stated, "we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding the assurances that such communication would not be intercepted by management."

Further, another related concern stemming from the auditing and reviewing of employee's e-mail messages is that such conduct may violate the Electronic Communication Privacy Act (ECPA). This concern can be allayed somewhat by the exclusion in the statute for accessing electronic communications "in the ordinary course of business", and recent case law. In *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996), the court made clear that the Electronic Communications Privacy Act did not apply to the employer because simply reviewing what their system stored was not "interception" within the meaning of the statute.

---

## CONCLUSION

---

While the foregoing illustrates only a few representative legal issues facing corporations which arise out of technological change, they are all very real. In fact, in advising our clients in the past several months, we have seen each one of these and many other technological/legal issues. In each instance, we assembled a multi-disciplinary team that included lawyers and personnel specializing in technology, information systems, and records to address the problems and propose solutions. It has been our experience that such an integrated approach is necessary to successfully guide companies through the obstacles of digitization while simultaneously reducing corporate exposure to liability. It is critical that corporate counsel understand the risks, assist in limiting liability and ease the disruption caused by technological innovations to move the corporation forward without the uncontrolled backlash of failing to anticipate problems when applying technology to new business problems.

***This Report was Downloaded from <http://www.KahnConsultingInc.com>. A version of this Report originally appeared in The Corporate Counselor. Original authors were Randolph A.Kahn and Robert F. Williams. For more information email: [info@KahnConsultingInc.com](mailto:info@KahnConsultingInc.com). © 2002 Kahn Consulting Inc.***