ZETLIN & DE CHIARA LLP
COUNSELORS AT LAW

Current Legal and Business Developments Affecting the Design, Construction and Real Estate Industries

Quarterly Review

INSIDE THIS ISSUE

2006 · Volume 11 · Number 2

Privacy in the Workplace: Is There Any Such Thing?

By Robert L. Honig, Esq.

The computer age has transformed the workplace from a dynamic across-the-office verbal exchange of information into a fragmented labyrinth of isolated workers typing furiously on their keyboards. For many employees, the telephone has unceremoniously been rendered obsolete by electronic mail; the majority of their communications now originate from their computers. Indeed, many of the computer savvy use electronic files to store virtually all of the important information in their lives, information used for both business and personal purposes. "Secret" passwords are the key to every document or piece of information that has any meaning. Along with a reliance upon updated software, these technophiles seem to have developed a misguided sense of security about the information they enter into their electronic files. The concept of "employee privacy" is one that most companies have faced in one form or another in the last several years. While much has been made of selecting a password that prohibits others from perusing the most confidential information, employers and employees, with their legal representatives in tow, are continually exploring and redefining the legal rights and obligations governing such confidentiality. The same issues have also surfaced with respect to telephones and other means of communication. This article will focus on some of these legal issues.

The Password to Danger

Perhaps the most widely used computer software is that of electronic mail (e-mail). Millions of workers use e-mail as their primary form of communication both in business and with friends. Most, however, erroneously believe that their e-mail accounts are confidential and not subject to review by their employers. These employees are sorely mistaken. In addressing these issues, the courts have been quick to support an employer's right to monitor and review all of its employees' e-mail communications. In Garrity v. John Hancock Mutual Life Insurance Company, 2002 WL 974676 (D. Mass. 2002), for example, the United States District Court for the District of Massachusetts found that the defendant/employer's legitimate business interest in protecting its employees from harassment in the workplace trumped any of the plaintiffs' privacy interests in maintaining the confidentiality of their e-mail transmissions.

Continued on pg. 6

Federal E-Discovery Rules Proposed

By Burt P. Natkins, Esq.

As electronically-stored information has become an increasingly important source of evidence for litigants, its discovery has concomitantly grown more time-consuming, logistically burdensome, and costly. Recognizing this ever-expanding problem, the Judicial Conference of the United States, the administrative arm of the federal courts, has now recommended that the Federal Rules of Civil Procedure ("FRCP") be modified to specifically govern the discovery of electronically-stored information within the federal trial court system. These proposed rules will likely take effect on December 1, 2006, if, as largely expected, the United States Supreme Court approves them and Congress does not subsequently disapprove them.

Continued on pg. 2

Recent Legal Updates

1. A New York appeals court affirmed that coverage is excluded for the total loss of a home due to mold contamination and that the insurer is entitled to recoup extra living expenses advanced to the homeowner. Mary Elizabeth Hritz, et al. v. Donald A. Saco, et al., No. 6180-6180A, 6180B, 6180C, N.Y. Sup., App. Div., 1st Dept.; 2005 N.Y. App. Div. LEXIS 5698 (2005).

2. A wind deductible did not apply to an insured's claim for damages caused by rain where the rain entered the insured premises by way of wind-caused openings because the damages were indirectly and not directly caused by wind. Turner Construction Co. v. ACE Property & Casualty Co., No. 04-6641, 2nd Cir. (Oct. 2005).

Federal E-Discovery Rules Proposed

Continued from pg. 1

The discovery of electronically-stored information raises markedly different issues from the conventional discovery of paper records. Easily generated and stored, digital documents are characterized by the enormity of their volume when compared to hard-copy documents. Furthermore, computers, unlike paper, are dynamic – merely turning a computer on or off can change the information it stores. Another exceedingly important difference is that electronically-stored information, unlike words on paper, may be incomprehensible when separated from the system that created it.

> *"The proposed amendment states that, absent exceptional circumstances, sanctions may not be imposed if electronically-stored information sought in discovery has been lost as a result of the routine operation of an electronic information system."*

These differences and others were the underpinning for the Judicial Conference when it recommended the adoption of the e-discovery amendments to the FRCP. Indeed, the amendments are necessarily far-reaching in scope, modifying several provisions of the FRCP, including Rules 16, 26, 33, 34, 37 and 45, and Form 35. A few illustrations of their broad nature follow.

Under FRCP 26(f), parties must confer in the very early stages of a litigation to consider the basis of their claims and defenses and the possibilities for a prompt settlement; to make arrangement for the disclosure of documents; and to develop a proposed discovery plan. The proposed e-discovery amendments would require this conference to include a discussion of issues particularly relevant to the disclosure or discovery of electronically-stored information.

The topics to be discussed include the form of producing electronically-stored information. This distinctive and recurring problem in electronic discovery results from the fact that, unlike paper, electronically-stored information may exist and be produced in a number of different forms. The parties are also required to discuss preservation, newly important because of the dynamic character of electronic information. Finally, the parties are directed to discuss whether they can agree on approaches to asserting claims of privilege or work-product protection after inadvertent production in discovery.

FRCP 26(b)(2) clarifies the obligations of the responding party when providing electronically-stored information not easily accessible, an increasingly disputed aspect. Under the amendment, the responding party need not produce electronically-stored information if it is not reasonably accessible because of undue burden or cost. However, the amendment requires the responding party to identify the sources of potentially responsive information it has not searched or produced due to the costs and burdens of accessing the information. If the requesting party, in turn, moves for the production of such information, the responding party has the burden to show that the information is not reasonably accessible. Even if the responding party makes a showing, the court may still order discovery for good cause and may impose appropriate terms and conditions (sharing of costs, for example).

The proposed amendments modify FRCP 37(f) to respond to another distinctive feature of computer systems – the recycling, overriding, and alteration of electronically-stored information. While paper documents are typically destroyed as the result of a conscious, affirmative effort, computer systems lose, alter or destroy information as part of their routine operations, making the risk of losing information significantly greater than with paper. The proposed amendment, therefore, provides limited protection against sanctions under the rules for a party's failure to provide electronically-stored information and discovery.

The proposed amendment states that, absent exceptional circumstances, sanctions may not be imposed if electronically-stored information sought in discovery has been lost as a result of the routine operation of an electronic information system, as long as that operation is in good faith. However, the proposed amendment does not provide a shield for a party that intentionally destroys specific information because of its relationship to litigation, or for a party that allows such information to be destroyed in order to make it unavailable in discovery by exploiting the routine operation of an information system.

The recommended amendments are extensive and attempt to address in a balanced fashion the ever-increasing problems associated with e-discovery. The true effectiveness of these amendments, however, will only be known after they take effect and have been implemented over a reasonable period of time. ■

In January, partner **Carol J. Patterson** co-chaired *Expecting the Unexpected: Anticipating and Managing Key Risks to Successful Projects*. She was instrumental in developing this program for the American Bar Association's Forum on the Construction Industry.

Tech-Protect — New Areas to Safeguard Your A&E Firm

By Dana Brown, RPLU
Beazley Group

Advanced technology enables the building industry to provide cheaper, faster and better construction. The possibilities appear endless – designing and constructing bridge deck slabs and roof structures with inexpensive plastics and corrugated materials, evaluating lighting aesthetics in simulated environments for accurate foot-candle reading, creating virtual building models incorporating entire mechanical, electrical and structural details, etc.

But advanced technology has also created innovative ways to be sued. While cost-overruns and delay claims are, unfortunately, the norm, the many different computer-aided design (CAD) application programs have made it imperative to know how to integrate them into a project. Also, design team members must communicate with each other regarding CAD documents to avoid misinterpretations and costly results.

The Soldier Field renovation project in Chicago is perhaps one of the more famous failed integrated technology snafus. With a budget soaring beyond $50 million, one of the more costly issues was the failed supply chain coordination of structural components, despite using 3D modeling by the fabricators.

To add insult to injury, many found the final architectural and structural "feat" a failure – a ruin of a once famous landmark. Litigation continues in an effort to remove the site from the National Historic Landmark register. According to *Chicago Tribune* architectural critic, Blair Kamin, the project was an "invasion of the lakefront. Despite the intimate interior of the finished Soldier Field, the bulbous and outlandish design defiles Chicago's brightest jewel." (*Chicago Tribune*, September 21, 2003).

As widely as technology is expanding, unexplored liability issues are also springing up. Protection from legal actions arising out of internet liability, cybercrimes and e-business interruptions has become paramount to the survival of one's firm. Other emerging areas of business liability include technology based services, technology products, computer network security, multimedia and advertising.

> *"Design team members must communicate with each other regarding CAD documents to avoid misinterpretations and costly results."*

Technology Based Services

Technology based services are defined as:

- computer and electronic technology data processing
- internet services
- data and application hosting
- computer systems analysis
- technology consulting and training
- software programming, installation, integration and support

Claims alleging negligent acts, errors or omissions and breach of contract in rendering or a failing to render these services have already arisen in many courts.

Technology Products

Product liability claims now cover new technologies, specifically the failure of technology products to perform the function or serve the purpose intended.

CASE STUDY

The Wall Street Journal, February 27, 2001: Nike Warns 3rd-Quarter Earnings Will Miss Estimates by at Least 28%.

Nike announced problems with its supply chain computer management system which resulted in missed earning expectations — their fiscal 3rd quarter sales were revised nearly $100 million lower than anticipated. It seems that some inventory problems from software systems provided by i2 Technologies created duplicate orders in some cases and no orders in others. Several class action lawsuits were filed against i2 related to the drop in its stock following Nike's announcements. Nike's own stock lost $2.6 billion in market value following the earnings warning.

Computer Network Security

The failure to provide or manage computer systems security can result in cyber liability claims. These cover issues such as:

- the inability of a client or other project team member, who is authorized to do so, to gain access to computer systems or technology based services;
- the failure to prevent unauthorized access to computer systems that results in the theft, destruction, deletion or corruption of electronic data;
- the failure to prevent transmission of malicious code from computer systems (viruses) to another party causing business interruption losses

CASE STUDY

A disgruntled employee of a major consulting firm downloaded malicious code onto the networks of the firm, its clients and vendors. The code launched confidential information into the public domain and destroyed some critical corporate applications, resulting in more than $10,000,000 in third party claims.

Continued on pg. 8

Agreements Regarding the Transfer of Electronic Documents

By Tara B. Mulrooney, Esq.

New risks and management issues are emerging in connection with the electronic transfer of design documents. As an accommodation to the owner and to make the exchange of documents faster and more efficient, architects will often agree to furnish their documents to the owner, for use by the contractors, in electronic format. This electronic transfer of documents raises liability issues and increases the need for protection whenever design professionals share the intellectual property they create for projects. The American Institute of Architects (the "AIA") addresses this issue in its Standard Form Agreement between owner and Architect, B141.[1] Specifically, Section 1.3.2.4 of B141 advises that the owner and architect should set forth the specific conditions governing the exchange of electronic documents by a separate written agreement.[2]

This article provides an overview of the issues and potential liabilities that can arise when drafting an agreement to protect architects and other design professionals. In particular, the following issues should be considered and addressed: (1) indemnification for liabilities arising from the use of the electronic documents furnished by the architect; (2) preventing the inadvertent increase in the architect's responsibilities, specifically with respect to shop drawings; (3) ensuring the architect maintains ownership of the electronic documents transferred; (4) confirming that hard copies of the documents are given precedence over the electronic documents; (5) releasing the architect from any liabilities resulting from inconsistencies between the hard copies and the electronic versions of the documents; (6) prohibiting the alteration and modification of the electronic documents exchanged; (7) addressing durability and data integrity issues associated with documents in electronic form; (8) restricting the owner's and/or contractor's rights to use the architect's documents other than for a stated, limited purpose; (9) ensuring that the electronic documents are not products so that there are no warranties of any kind in such electronic documents; and (10) requiring the owner and/or contractor to waive all claims resulting from the failure to comply with the agreement and providing for injunctive relief in the case of a breach of the agreement.

An agreement concerning the transfer of documents by the architect in electronic form should reflect the understanding of the parties that the electronic documents are to be used solely for the intended purposes set forth in the agreement and only for informational and reference purposes. One critical provision to any such agreement is an indemnification provision pursuant to which the recipients of the electronic documents, the owner and contractors, agree to indemnify and hold harmless the architect from all actions, claims and liabilities arising from or related to the use of the electronic documents by the owner and those to whom the owners provides such documents, including contractors and consultants.

It is important to reiterate the responsibilities of the respective parties, specifically the contractor to whom the owner will be furnishing these documents, in the agreement so that the architect is not held liable for the content of documents which are not its responsibility. The agreement should contain a provision that the furnishing by the architect of the electronic documents does not relieve the contractor and its subcontractors from being solely responsible for assuring the accuracy of all information contained in any shop drawings. Moreover, the agreement should explicitly state that it remains the responsibility of the contractor or its subcontractors, as appropriate, to obtain, verify and coordinate all required information necessary to produce accurate and complete shop drawings. This provision is especially critical if the parties set up a project website for the exchange of documents. In such case there is a danger that the architect could be held responsible for the entire content of the website.[3]

Every agreement controlling an architect's transfer of electronic documents should include a provision addressing the ownership of the documents.[4] The provision should specify that all drawings, specifications and other documents of any kind prepared by the architect, whether hard copies or in electronic form, are instruments of the architect's services. Further, it should clearly state that the architect and its sub-consultants retain all common law, statutory and other reserved rights, including copyright.

Since one cannot be certain of how electronic information might read under a different system, how intended or unintended changes beyond the architect's control may be introduced to electronic documents and how electronic information may change over time, it is critical that architects protect themselves by including a provision specifically stating that hard copies take precedence over the electronic documents.[5] The provision should specify that electronic documents do not replace or supplement the paper copies of the drawings and specifications which are, and remain, the contract documents for the particular project to which the agreement relates. Further, it should state that if any differences exist between printed drawings, specifications or other documents and the electronic documents, the information contained in the printed documents shall be presumed to be correct and take precedence over the electronic documents.

To further protect itself in regard to this issue, the architect should get a release from the owner and/or contractor with respect to their use of the electronic documents. The agreement should include a provision whereby the owner and contractor agree to accept full responsibility for their use of the electronic documents and, to the fullest extent permitted by law, release the architect, its sub-consultants and their respective partners, principals, employees, agents, successors and assigns from all claims, actions, liabilities, debts, controversies, damages and expenses arising from or relating to any errors, inaccu-

racies or differences between the architect's filed hard copies and the electronic documents. The owner should be required to compare the electronic format to the hard copy to confirm accuracy and release the architect prior to its use of the electronic versions of such documents.

Unlike written copies that clearly reflect any changes made, computer data can be modified and bear no evidence of the modification.[6] For this reason, it is critical not only to have a provision like the release discussed above, but also to include a provision prohibiting modifications or alterations to the architect's documents. Thus, the agreement must clearly state that the owner, and those with whom it shares the information, including contractors and consultants, agree not to add to, modify or alter in any way the electronic documents.

"Unique to electronic information are concerns regarding the integrity and durability of the documents over time, and how information will be read if converted."

Two issues which are unique to electronic information are concerns regarding the integrity and durability of the documents over time, as well as how information will be read if it is converted to a different system. Any agreement regarding the transfer of electronic documents should address the issues of potential deterioration and conversion of information in electronic form. The agreement should specify that it is understood by the owner and those it hires, such as contractors and consultants, that the media in which electronic documents are transmitted can deteriorate over time and under various conditions and that it could be converted to other formats. It should state that the architect is not responsible for such deterioration or for any conversion of the format.

One of the most critical provisions of this type of agreement is one which protects against unauthorized use and inappropriate reuse of the electronic documents. First, a provision addressing this issue should clearly set forth the intended and limited purpose for which the documents are being transferred. It should explicitly state that the documents were prepared for use in connection with a specific project. Second, the transfer agreement should specify that any reuse of the architect's documents, or use for any reason outside the specified purpose, without the express written consent of the architect will be at the client's sole risk.[7] Finally, the provision should state that the client shall indemnify and hold harmless the architect for all claims and losses arising from any unauthorized use of the electronic documents.[8]

Another special protection that should be incorporated into a transfer agreement is a protection against the electronic documents being construed as a product. It is important to stress that the electronic documents are instruments of the architect's services and not products. The potential for electronic documents to be reused could allow for the documents to be considered as products generated by the architect, as opposed to instruments of the architect's services. The danger with this is, if the electronic documents are considered products, it could lead to product liability exposure for the architect. Therefore, disclaimer language should be added to the agreement "to prevent the possibility of the application of product warranties or guaranties, such as warranties of fitness for use and merchantability."[9] A provision should be included stating the parties' agreement that the electronic documents are not products and that the parties expressly agree that there are no warranties of any kind, express or implied, in the electronic documents or in the media in which they are contained.

Finally, there should be a provision pursuant to which the architect, and those with whom its shares the electronic documents, waive all claims and liabilities against the architect resulting in any way from the owner's failure to comply with the agreement. Since a violation of the provisions of the agreement may cause irreparable damage or injury to the architect, this provision should also expressly state that in the event of a breach of the obligations described in the agreement, the architect is entitled to an injunction restraining any further violation of the agreement, in addition to all other available remedies under law or equity.

In conclusion, although providing documents in electronic form is a more efficient and practical means for the exchange of documents between architects, owners, contractors and consultants, it also exposes architects to ad-ditional, and often unexpected, liabilities, such as those discussed above. For this reason, it is critical that architects enter into an agreement controlling
the transfer of documents which incorporates the provisions discussed in this article prior to providing documents in electronic form.

---

[1] AIA Document B141-1997, Subparagraph 1.3.2.4.

[2] Id.

[3] See XL Design Professionals, Architects Loss Prevention Library, "Collaborating in Cyberspace," www.sldp.com/architects/cyberspace/hmtl (2004).

[4] See American Institute of Architects, "Transfer of Electronic Documents and Electronic Information" www.aia.org/pm_a_transferdocs (2005).

[5] Id; see also Victor O. Schinnerer & Company, Management Advisory, "Electronic Information Transfer Issues," www.schinnerer.com/risk_mgmt/designfirms/manadvis.hmtl (2002).

[6] CRisk Consultants in Risk Management, "Wired: Electronic Transfer of Design Information," www.crisk.com/articles/sgms_wire.html (2001).

[7] American Institute of Architects, "Transfer of Electronic Documents and Electronic Information," www.aia.org/pm_a_transferdocs http://www.aia.org/pm_a_transferdocs (2005).

[8] Id.

[9] Id; see also Victor O. Schinnerer & Company, Management Advisory, "Electronic Information Transfer Issues," www.schinnerer.com/risk_mgmt/design-firms/manadvis.hmtl (2002).

If you would like to receive our newsletter and other bulletins via email, please forward your e-address to smaher@zdlaw.com.

Continued from pg. 1

In Garrity, the defendant terminated the plaintiff for violating the defendant's e-mail policy by transmitting e-mails that were obscene, profane, sexually-oriented or otherwise prohibited. When the plaintiff sued the defendant for wrongful termination, the defendant moved for summary judgment as a matter of law.

Upholding the defendant's motion, the District Court rejected plaintiff's claim that the defendant led him to believe that his e-mails would be kept private by virtue of his use of a personal password and private e-mail folders. The Garrity court referenced the case of McLaren v. Microsoft Corp., 1999 WL 339015 (Texas Ct. App. 1999) in which the Texas Court of Appeals addressed a similar situation and held that:

> According to [plaintiff], his practice was to store his e-mail messages in "personal folders." Even so, any e-mail messages stored in [plaintiff's] personal folders were first transmitted over the network and were at some point accessible by a third party. Given these circumstances, we cannot conclude that [plaintiff], even by creating a personal password, manifested and [defendant] recognized a reasonable expectation of privacy in the contents of the e-mail messages such that [defendant] was precluded from reviewing the messages.[1]

Employing the same rationale as the District Court in McLaren, the Garrity court also emphasized the employer's right to take affirmative steps to "maintain a workplace free of harassment and to investigate and take prompt and effective remedial action when potentially harassing conduct is discovered."[2]

Similarly, in Autoli ASP, Inc. v. Dep't of Workforce Services, 29 P.3d 7, 12-13 (Utah Ct. App. 2001), the Appellate Court found that the e-mail transmission of sexually explicit and offensive material including jokes, pictures, and videos, exposes the employer to sexual harassment and sex discrimination lawsuits.

Therefore, wrote the court in Autoli, once the defendant received a complaint about the plaintiff's sexually explicit e-mails, it was required by law to commence an investigation. It is not difficult to see that these courts have taken great pains to protect employers' rights to monitor the email and computer usage of its employees, even when the employee makes use of a private password.

Other courts have reached a similar conclusion about an employer's right to monitor its employees' e-mail transmissions. In Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996), for example, the defendant/employer maintained an e-mail system in order to facilitate internal communications among its employees. The defendant repeatedly assured its employees, including the plaintiff, that all e-mail communications would remain confidential and would not be monitored. The employer further advised its employees that e-mail communications would not be intercepted and used by defendant against its employees as grounds either for termination or reprimand.

> *"The courts have been quick to support an employer's right to monitor and review all of its employees' e-mail communication."*

The defendant notified the plaintiff that it was terminating his employment for transmitting what it deemed to be inappropriate and unprofessional comments over defendant's e-mail system. The e-mails set forth threats to "kill the backstabbing bastards" and referred to the company holiday party as the "Jim Jones Kool-Aid affair." The plaintiff then sued his employer for wrongful termination based on its purportedly improper review of his stored e-mails. The court, however, rejected the plaintiff's claim for wrongful termination and upheld the employer's right to search its employees' e-mail files.

In determining whether an alleged invasion of privacy is substantial and highly offensive to a reasonable person, the Smyth court chose to adopt a test which balanced the employee's privacy interest against the employer's interest in maintaining a drug-free workplace. Unlike urinalysis and personal property searches, the court found no reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system, even though the employer assured the employee that such communications would not be intercepted by management.

The Smyth court determined that once plaintiff communicated the alleged unprofessional comments to a second person over an e-mail system utilized by the entire company, any reasonable expectation of privacy was lost. Conversely, the court did not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy. In short, the Smyth court explained that the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system *outweighed* any privacy interest the employee may have had in those comments. Not surprisingly, Smyth has become one of the leading cases championing the rights of an employer to search its employees' e-mail files.

Many other courts, both federal and state, have relied on the balancing test utilized in Smyth to measure an employee's expectation of privacy in his computer files and e-mail. In general, courts will now typically consider four factors:

1) Does the corporation maintain a policy banning personal or other objectionable use?
2) Does the company monitor the use of the employee's computer or e-mail?
3) Do third parties have a right of access to the computer or e-mails?
4) Did the corporation notify the employee, or was the employee aware of the use and monitoring policies?[3]

These factors should serve as a guideline

for the evaluation of employees' right to privacy in their electronic files.

An Effective E-mail Policy

As you can see, the workplace is littered with landmines for the unprepared e-mail user or provider. As an employee, you should be fully familiar with your company's e-mail and computer policies, including any reservation of your firm's right to review stored e-mails for any legitimate business purpose. As an employer, it is important to have an express written policy clearly delineating your employee's rights, or lack thereof as the case may be, with respect to the firm's e-mail or internet system.

The e-mail policy should provide ample notice to employees that their e-mails will be reviewed by appropriate personnel and disclosed to third parties as the employer deems necessary. The policy should also:

1) contain a statement that all employees waive any right to privacy in e-mail messages and consent to such monitoring and disclosure;
2) explain that employees should treat e-mail messages like shared paper files, with the expectation that anything in them will be available for review by authorized representatives of the corporation; and
3) reserve the company's right to disclose e-mail messages to law enforcement officials or to other third parties without notice to either the sender or the recipient of the message.

A proactive e-mail policy should employ language similar to the following:

> The purpose of ABC Corp.'s electronic information systems, including telephone, voice and electronic mail ("e-mail"), all computer equipment, software and the local and wide-area networks, is to facilitate transmittal of business-related information. Accordingly, firm computers and electronic information systems should be used exclusively for matters of concern to the firm's operations, and not for communications of a personal, private or non-business nature.

The more specific the language, the more protection your computer privacy policy will afford. For example, the following language can be used to address issues involving private passwords:

> To achieve compliance with this policy, all computer files and electronic information, including e-mail and voice mail, are subject to review by firm management at any time. Even though you use a password and may be able to classify files or messages as "personal and confidential" or "private," such files and messages remain subject to inspection and review. The firm is capable of viewing the passwords of computers and is able at all times to access computer files and the messages each user sends and receives on the electronic information systems.

"Technological advances utilized by employers to monitor their work force have also resulted in a variety of novel statutes aimed at curbing potential abuses."

Your attorney can assist with the modification of your firm's employee handbook to include similar protective language.

Telephone Monitoring

Technology has also reared its ugly head with respect to an employer's ability to monitor its employees' telephone calls.

Given the freedom that the courts have provided employers to monitor their internal e-mail and internet systems, many employers have begun to assume that they have equal or greater rights with respect to their employees' telephones. Some of these employers, however, have found themselves on the wrong end of recent court decisions. The way the law stands now in most jurisdictions, employers may monitor their employees' calls with clients or customers for reasons of quality control. Intercepting communications is not actionable under Federal, New York or New Jersey law if the person intercepting is a party to the communication, or acts with the consent of a party to the communication. In some states, the law actually requires the employer to inform its employee that the conversation is being recorded or monitored by either putting a beep tone on the line or playing a recorded message. Not every business is aware of this requirement, however, so calls may still be monitored without a warning, albeit at the peril of both the employer and the employee.

As stated above, Federal law, which regulates phone calls with persons across state lines, does not prohibit unannounced monitoring for purely business-related calls. An important exception is made for personal calls. Pursuant to some recent Federal court decisions, when an employer realizes a call is personal, he or she must immediately cease monitoring.[4] When employees are told not to make personal calls from specified business phones, however, the employee takes the risk that calls on those phones may be monitored.

Technological advances utilized by employers to monitor their work force have also resulted in a variety of novel statutes aimed at curbing potential abuses. One such statute, the New York State General Business Law, makes it a felony for the owner or manager of any premises to knowingly permit a "two-way mirror or other viewing device" to be installed or maintained "for the purpose of surreptitiously observing the interior of any fitting room, restroom, toilet, bathroom, washroom, or shower." Although enacted as a consumer protection measure, the statute could encompass cameras or other mechanical viewing devices that might be used to surreptitiously observe employees in the workplace.

Conclusion

Like it or not, e-mail and other computer technologies are here to stay. With

Continued on pg. 8

Tech–Protect

Continued from pg. 3

Multimedia and Advertising

One of the nation's largest health insurers inadvertently sent e-mail messages to 19 members containing confidential medical and personal information of 858 other members. Although the company immediately took steps to correct the problem, it received several lawsuits alleging invasion of privacy.

This is an example of how breach of contract and negligence actions can be applied to the multimedia and advertising arena. Claims can allege one or more of the following acts committed in the course of a firm's performance of its services:

- defamation, libel, slander, product disparagement, trade libel, infliction of emotional distress or harm to reputation
- invasion of privacy
- misappropriation of trade secrets or ideas
- plagiarism, piracy or misappropriation of ideas under implied contract
- infringement of copyright, trade dress ("total image" copyright) or domain
- negligence regarding the content of media communication (including harm caused through any reliance or failure to rely upon such content)

CASE STUDY

A company created its web site by framing the content of other media companies within their site. By doing so, the service created the illusion that the content was all their own.

Several media firms sued the company for copyright and trademark infringement on the basis that the firm was a "parasitic" site that republished the news and editorial content in order to attract users.

In many ways, technology has made the industry more efficient, but unexplored territory does contain unknown dangers. Most professional liability (errors and omissions) and general liability policies provided to design professionals do not cover the liability exposures noted above, thereby leaving firms unprotected. The upside is that the insurance industry is developing coverage vehicles that address these issues. Beazley USA, in particular, has developed a new policy form designed to "fill" in some of the current gaps to provide basic coverage for professional liability, technology-based services, technology products, computer network security and multimedia and advertising. ■

Privacy in the Workplace

Continued from pg. 7

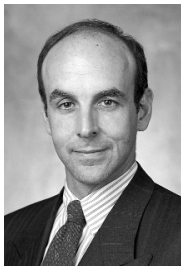
these advances come a myriad of new legal issues regarding appropriate use and confidentiality. Recent court decisions have begun to lay the groundwork for employers to formulate effective confidentiality policies. Firm management must review their employment policy handbooks to ensure that they have protected themselves from claims that they have violated some expectation of their employees' privacy. Those who fail to do so may find themselves as a defendant in a burgeoning new area of litigation. ■

[1] See McLaren v. Microsoft Corp., 1999 WL 339015 (Texas Ct. App. 1999).

[2] Id.

[3] In re Asia Global Crossing Ltd., 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

[4] For example, see Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983).



Partner **Michael S. Zetlin** was recently named to the American Arbitration Association's Roster of Arbitrators and Mediators. As an AAA neutral, he will provide alternative resolution and conflict management services upon request to those involved in construction disputes. For more information, please contact Mr. Zetlin or visit www.adr.org.

Promotions

The Firm congratulates

Burt P. Natkins
on his promotion to Principal

Lina G. Telese
on her promotion to Principal

Jenifer B. Minsky
on her promotion to Associate Principal

New Jersey office move

We are pleased to announce the relocation and expansion of our New Jersey office.

80 Bloomfield Avenue
Caldwell, NJ 07006

Tel: 973.364.9900
Fax: 973.364.9901

2006 · Volume 11 · Number 2
Quarterly Newsletter Publication from Zetlin & De Chiara LLP
Counselors at Law

801 Second Avenue
New York, New York 10017
212.682.6800
Fax 212.682.6861

www.zdlaw.com

80 Bloomfield Avenue
Caldwell, New Jersey 07006
973.364.9900
Fax 973.364.9901

900 Merchants Concourse
Westbury, New York 11590
516.832.1000
Fax 516.832.2555

Six Landmark Square
Stamford, Connecticut 06905
203.359.5733
Fax 203.359.5858