

**PRIVACY ISSUES AND  
THEIR IMPACT UPON THE TRUCKING INDUSTRY**

Jay Barry Harris, Esquire  
Fineman Krekstein & Harris, P.C.  
1608 Walnut Street, 19<sup>th</sup> Floor  
Philadelphia, PA 19103  
215-893-9300

[jharris@finemanlawfirm.com](mailto:jharris@finemanlawfirm.com)

Joel McCarty  
Sr. Vice President, General Counsel  
And Secretary  
Old Dominion Freight Lines, Inc.  
500 Old Dominion Way  
Thomasville, NC 27360  
800-432-6335  
[joel\\_mccarty@odfl.com](mailto:joel_mccarty@odfl.com)

Dale Douglas  
Vice President and General Counsel  
Motor Transport Underwriters, Inc.  
9449 Priority Way  
Indianapolis, IN 46240  
800-809-3660  
[ddouglas@mtuinc.com](mailto:ddouglas@mtuinc.com)

Jay Barry Harris, Esquire, is a Shareholder with Fineman Krekstein & Harris, P.C. His practice focuses upon trucking litigation, employment law, premises liability, product liability, construction law, insurance coverage litigation and professional liability. He is admitted to the Pennsylvania, New Jersey and New York State Bars and is a member of the Pennsylvania, New Jersey and New York Bar Associations, the International Association of Defense Counsel, the Defense Research Institute, the Pennsylvania Defense Institute and the Philadelphia Association of Defense Counsel. Currently, Mr. Harris is the Chair of the DRI Homeowners Law Subcommittee and a Regional Editor for the DRI Trucking Law Committee. Mr. Harris thanks Elyse L. Glazer, Esquire for her assistance in preparing the first part of this article.

Joel B. McCarty, Jr. is Sr. Vice President, General Counsel and Secretary of Old Dominion Freight Line, Inc. in Thomasville, North Carolina, where among other duties, he is responsible for safety, benefits and personnel. He has served as General Counsel since 1987 and previously was Assistant General Counsel for McLean Trucking Company in Winston-Salem, NC after having been in private practice in Houston, Texas. He graduated from the University of Texas in 1962 and is a member of the State Bar of Texas and Transportation Lawyers Association.

Dale S. Douglas is Vice President and General Counsel to Motor Transport Underwriters, Inc. in Indianapolis, Indiana. His practice includes civil litigation, transportation, trucking law and insurance coverage. He is a member of the Allegheny County (Pa.) and Pennsylvania Bar Associations and the Association for Transportation Law, Logistics and Public Policy. He is a past member of the American Bar Association, Motor Carrier and Rail Law Committee and the Risk and Insurance Management Society. Mr. Douglas is also Of Counsel to the Anstandig, McDyer, Burdette & Yurcon, P.C. law firm of Pittsburgh.

In the following article we attempted to provide our readers the legal, practical and insurance issues confronted by today's employers in dealing with employee privacy. The first part, written by Jay Barry Harris, provides an overview of the current state of privacy law. The second part, written by Joel McCarty, provides insights into incorporating the impact of privacy concerns into the everyday workplace. The third part, written by Dale Douglas, addresses insurance issues related to privacy claims. We hope you find the material instructive.

## **EMPLOYEE PRIVACY – AN OVERVIEW**

### **I. INTRODUCTION**

Supreme Court Justices, Samuel D. Warren and Louis D. Brandeis warned of new technology colliding with privacy rights over one hundred years ago. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193,195 (1890) "Technology often outpaces the law" is a complaint heard frequently when discussing employee/employer privacy concerns. The legal system's inherent slowness is intrinsically tied to the problems and concerns facing both employers and employees in today's workplace.

Employee privacy is and will be a dominant issue in the workplace. The tension between the employer's needs and the employee's privacy will continue to be a "flash point." For example, employers are required to initiate internal investigations involving anything from drug screening to email monitoring. These investigations usually spark the debate over employee privacy and often concern highly personal information and/or issues including allegations of discrimination, sexual harassment, wrongful discharge, drug or alcohol abuse and employee violence in the workplace. Although reviewing an employee's personal information is necessary to protect an employer from liability, it is a thin line that separates the employer's investigation and monitoring from an inadvertent exposure to liability.

In today's technological era, it is important that an employer be aware of all the requirements and safeguards it must implement regarding the transmission, storage and dissemination of employee information. An employer must maintain

a system which adequately protects the privacy interest of the employee while still enabling the employer to conduct its business.

The following article will provide a summary of current privacy law and its impact on the concerns and problems facing employers.

## II. PRIVACY LAW/REGULATION/LEGISLATION

### A. Common Law Privacy Torts

The initial theory of individual privacy protection was articulated by Warren and Brandeis in a time when email, fax machines, beepers, cell phones and all the other high technology which makes our world faster, smaller and easier were not even imaginable. These two Supreme Court Justices propounded a flexible, general “right to be let alone” theory of common law privacy. *Supra*, Warren & Brandeis at 193. Initially the difficulty with the privacy theory was its vague and general nature which allowed the right to essentially encompass almost any kind of unwanted attention. However, the right to privacy has evolved into specific causes of actions with firmly established burdens of proof. *Id.*

The common law of privacy has congealed into three distinct torts, often referred to collectively as invasion of privacy: (1) intrusion upon seclusion; (2) appropriation of name or likeness; and (3) public disclosure of private facts. William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 389 (1960). Each tort has the flexibility and potential to cover the new problems created by today’s technological advancements. The critical question is the manner in which the judiciary applies these concepts.

These well-established torts serve as legal guides to addressing current employer-employee disputes. For example, identity theft is associated with the tort of appropriation of name or likeness and e-mail privacy can be linked to the tort of public disclosure of private facts. In the future, the courts may utilize the existing torts of privacy more frequently when dealing with breaches involving today’s technology, but until then much of an employer’s actions, or failures to act, when dealing with the privacy of its employees will be governed by specific legislation. *See, Deal v. Spears*, 980 F.2d 1153, 1158 (8<sup>th</sup> Cir. 1994); *see also, Sanders v. Robert Bosch Corporation*, 38 F.3d 736, 741 (4<sup>th</sup> Cir. 1994); *Ali v. Douglas Cable Communications*, 929 F.Supp. 1362, 1377 (D. Kan. 1996); *Owen v. Morgan Stanley & Co.*, 1997 U.S. Dist. LEXIS 20493 (S.D.N.Y. 1997).

### B. Electronic Communications

The Electronic Communications Privacy Act of 1986 (“ECPA”) arguably limits employer interceptions of employee electronic communications, including e-mail, beeper/pager messages, cell phone calls, and even telephone calls. 18 U.S.C. 2510-2522 (2000). The original purpose of the ECPA was to modernize

the law to address issues created by the explosion of technological advances. The legislative history of the ECPA details Congress's intent to update the Federal Wiretapping Act, originally designed to limit interceptions of telephone communications, to include within the definition of "electronic communication" new technology such as pagers, mobile phones, digital information and e-mail messages.

Few courts have dealt with employee invasion of privacy in the context of the ECPA. The ECPA contains two sections of statutory text relevant to the issue of employee privacy. One prohibits the interception of electronic communications; the other prohibits the unauthorized acquisition of electronic communications in storage. Title I essentially defines an interception as the point in time between when the communication is sent and when it is received, or in the few seconds it takes for an electronic communication to be in transit. 18 U.S.C. 2511 (2000). Title II of the ECPA ("The Stored Communications Act") protects the employee against the unauthorized acquisition of electronic communications in storage. 18 U.S.C. 2701-2711 (2000). Obviously, the ECPA has its most substantial effect on the employer monitoring of employee e-mail, but to some extent may implicate cell phone messages, beepers, Qualcomm messaging and voicemail.

Although it would seem that the ECPA would severely hamper an employer's investigation into the above-mentioned areas, courts and lawyers have had difficulty interpreting and applying the Act's prohibitions. Most case law revolves around the area of monitoring employee telephone use, but recent decisions have addressed the monitoring of e-mail. Fortunately, the ECPA's interpretive difficulties are most often resolved in the favor of the employer. *Deal v. Spears*, 980 F.2d 1153, 1158 (8<sup>th</sup> Cir. 1994); *see also Sanders v. Robert Bosch Corporation*, 38 F.3d 736, 741 (4<sup>th</sup> Cir. 1994). Although Title I prohibits the unauthorized acquisition of a device to intercept an electronic communication such as an e-mail, and Title II prohibits the unauthorized acquisition of a stored e-mail message, the statute contains exceptions which effectively exempt most employers from liability.

The ECPA contains three statutory exceptions to liability that, in effect, immunize employers from the penalties of the Act: The Ordinary Course of Business exception, the Service Provider exception, and the Consent exception. The Ordinary Course of Business exception allows an employer to either purchase an interception device, or utilize one given to the employer from the service provider, to intercept emails, voicemails, pager/beeper messages as long as it is in the ordinary course of business. 18 U.S.C. 2510 (5) (a) (2000). Whether the 'Ordinary Course of Business' applies depends whether the employer has a legitimate legal interest in monitoring the communications.

The Service Provider exception exempts service providers from liability for interceptions or accessing of electronic communication in the workplace.

Finally, the Consent exception allows employers to monitor electronic communications when employees give permission for monitoring. 18 U.S.C. 2511 (2) (d) (2000); 18 U.S.C. 2701 (c) (1)-(2) (2000). Obviously, an employer could require the employee to sign a consent, but even that is not required. Under the ECPA, implied consent is all an employer needs to begin monitoring. However, the emerging case law on implied consent requires actual or “full knowledge or adequate notification” before consent to monitoring can be interpreted as implied. *Ali v. Douglas Cable Communications*, 929 F.Supp. 1362, 1377 (D. Kan. 1996) *see also Deal v. Spears*, 980 F.2d 1153, 1157 (8<sup>th</sup> Cir. 1994) (holding as a matter of law that the employer failed to show implied consent by merely warning employees that phone calls might be monitored). An employee signature on a company policy would constitute “full knowledge or adequate notification” of monitoring, thereby signing away an employee’s right to sue under the ECPA’s consent requirement regardless of whether the employee had actually read the form before signing. The employee’s signature may also bar any common law claims for intrusion into seclusion or violation of privacy rights.

### C. HIPAA

The Health Insurance and Portability and Accountability Act of 1996 (Pub.L.No. 104-191) (“HIPAA”) has privacy implications due to its function to encourage the construction of a national standards for exchange of information among health care providers and insurers. It also regulates the sharing of patient’s medical information by medical providers and health insurance plans. The law provides that Congress or the Department of Health and Human Services (“HHS”) will establish regulations governing security of electronic information maintained by providers and health insurance plans. *The HIPAA Privacy Rule: An Overview of Compliance Initiatives and Requirements*, 70 Defense Counsel J. 127 (2003).

In February of 2003, the HHS published the finalized rules on Health Insurance Reform Security Standards. These rules function to accomplish several goals. First, to simplify the administration of health insurance claims and reduce the associated costs by encouraging the construction of national standards, second, to give patients more control over and access to their medical information, third, to protect individually identifiable health information from real or potential threats of disclosure through the setting and enforcing of standards, and finally, to standardize electronic data interchange for better efficiency. *Id.*

HIPAA requires that providers and insurers notify their patients and clients of their privacy practices. Moreover, HIPAA requires that no information be disclosed except with authorization from the patient or guardian, with the narrow exception of information exchanged between providers or providers and insurers. Even when the information is authorized to be disclosed, it must be the minimum necessary to comply with the request. *Id.*

HIPAA may expose employers to liability for a number of reasons. For example, drug testing involves medical testing/records of an employee being transferred between employer and testing facility or doctor. Potentially, mishandling of this information could expose an employer to liability. Although there is no provision under HIPAA for a private right of action, a disclosure in violation of the Act, which harms a patient/employee, might result in a private cause of action for redress.

### C. The Federal Privacy Act

The Federal Privacy Act of 1974, protects personal information, including an individual's medical records kept by government agencies. This Act ignores the private sector and regulates the handling of personal information like medical records, in only narrow specific instances. For example, an individual's personal information stored by the Veterans Affairs Office would be protected, but the same information stored by their private employer would not be covered by the Act. Since most employer's are outside the governmental context, the Federal Privacy Act is of little help in protecting the privacy of personal information, and offers no benefit/detriment to private employers regarding liability for privacy infringement.

## III. POTENTIAL AREAS FOR EMPLOYER LIABILITY

### A. Employer E-mail Monitoring

E-mail is the new form of communication, fast replacing the telephone and formal correspondence. This new communication phenomenon brings substantial benefits in efficiency, information sharing and productivity but also can cause serious concerns in the context of employee privacy. Employers give almost unbridled e-mail access to their employees today, who utilize e-mail to create a better, more productive and efficient work product. As Americans spend more time at work, personal use of e-mail 'on company time' is becoming commonplace.

Through the ECPA, it is clear that employers will have the opportunity to monitor employee email usage, as well as the content of the email. 18 U.S.C. 2510-2522 (2000). It is important for employers to have this right in order to protect them from potential liability should an employee use e-mail criminally and/or negligently. Monitoring employee web usage and e-mail can assist the employer to take steps against sexual harassment, violence in the workplace, problems with productivity and potential sharing of trade secrets, to name several examples. Micalyn S. Harris, *Is Email Privacy an Oxymoron?: Meeting the Challenge of Formulating a Company Email Policy*, 16 St. John's J.L. Comm. 553, 555.

While employers do have the right to monitor employee web usage and e-mail, certain steps must be taken to make employees aware of this right. *Id.* at 557. The easiest and most fail safe method of limiting an employer's liability is to draft a written policy which requires an employee to acknowledge his or her employer's right to monitor the employee's e-mail. Other than a formal consent waiver, an employer can protect itself by simply publishing a policy which unequivocally and clearly states that the employer is monitoring the employee's web usage. A good practice would require the employee to sign an acknowledgement of receipt of the policy. *Id.*

Although an employer has the right to monitor, it must also be careful to take steps to protect its employee's privacy. Monitoring of employee information may require planning and restructuring to assure that only appropriate people are reviewing the sensitive information. For example allowing individuals to participate in the monitoring who have no supervisory position could amount to a violation of an employee's privacy. *Id.* at 561.

#### 1. Specific Problems/Risks

An employer may be under an ethical obligation to keep certain email communications confidential. For example, those employers who handle their litigation through an in-house claims department may need to restrict access to the e-mails, faxes and telephone calls to and from its attorneys to protect the attorney client privilege doctrine. If any employee empowered to monitor the e-mails is allowed access to those communications, the privilege might be lost. Likewise, many employers are beginning to handle medical benefits for their employees in-house. These employers need to take special precaution with employee medical records and forms or face possible HIPAA violations.

A second risk, that of unauthorized/wrongful disclosure of otherwise privileged/private information may be greater when using e-mail than when using a telephone, a letter in a sealed envelope, or even a fax machine. For example, there is the "oops" effect, when an e-mail is occasionally sent to a group rather than one individual member. Additionally, system administrators have access to e-mail. However, it is not only the sender and receiver's system administrators who have access, but also any intermediate administrator through whose systems the message may pass. Where messages move through third party systems that may or may not be subject to the obligations imposed on commercial providers, obligations of confidentiality are less clear, and will require specific attention inquiry.

#### 2. Exemplary Case Law

In *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107, 2003 U.S. App. LEXIS 24856 (2001), the Third Circuit Court of Appeals ruled that since an employee's emails were stored on Nationwide's system, any search by the

company was authorized by an express exemption in the federal ECPA for e-mail service providers.

Richard Fraser claimed Nationwide had wrongfully terminated him because he filed complaints with the PA attorney general's office regarding Nationwide's allegedly illegal conduct. Nationwide claimed that plaintiff was terminated because he was disloyal, noting that he drafted a letter to two competitors expressing the Insurance Independent Contractor Association's dissatisfaction with Nationwide and seeking to determine whether they would be interested in acquiring the policy holders of the dissatisfied agents.

Nationwide decided to search its main file server, on which all of Fraser's e-mails were saved/lodged, for any e-mail to or from Fraser that showed improper behavior. Nationwide cited its fear, after finding the draft letters, that Fraser might also be revealing company secrets to its competitors as reason for the search.

The Judge found that Title II of the ECPA prohibits "seizures" of stored e-mails but includes an exception for seizures authorized "by the person or entity providing a wire or electronic communication service." Therefore, Nationwide violated the plaintiff's right to privacy.

Similarly, in another privacy action, *Bohach v. City of Reno*, 932 F.Supp. 1232, U.S. Dist. LEXIS 10715 (1996), the court held that the Reno Police Department, could, without violation of Title II of the ECPA, retrieve pager text messages stored on the police department's computer system because the department is the "provider of the service" and "service providers may do as they wish when it comes to accessing communications in electronic storage" on their own system.

## B. Drug Testing

Drug testing is a staple in the American workforce, and is widespread in both private and public employment. Certain industries, including the trucking industry, are required to test their employees for drug use. The collection of a sample for drug testing is simple but inexpensive and implicates important privacy concerns. Three main privacy issues arise: the invasion of privacy inherent in the collection procedure itself, the invasion of privacy based on the substantive test results, and the breach of confidentiality associated with the potential disclosure of the test results. Marion Crain, *Expanded Employee Drug Detection Programs and the Public Good: Big Brother at the Bargaining Table*, 64 N.Y.U.L. Rev. 1286 (1989). Employers who are required by law to test their employees should be concerned with the latter two issues.

Serious liability concerns for employers can be raised by the substantive information revealed through urine testing. Because the tests measure inert

metabolites of substances ingested days or weeks earlier, the test could substantially impact the privacy concerns of the employee. The capacity of drug testing to identify prescription medications may reveal an individual's underlying and private medical condition. George D. Lundenberg, *Mandatory Unindicated Urine Drug Screening: Still Chemical McCarthyism*, 256 JAMA 3003 (1986). For example, an employee testing positive for barbiturates may be taken Phenobarbital under a physician's prescription to help control epilepsy. The drug test results could lead to the discovery of any number of private medical conditions of the employee, and unauthorized disclosures may violate the an employee's right to privacy. Robert B. Sotinsky & Kenneth H. Chase, *The Medical Review Officer*, 32 J. OCCUP. MED. 1003, 1006-07 (1990).

Another privacy concern, and the most common issue, the failure to keep drug test results confidential, despite the possible devastating long-term consequences of a positive result. Because drug tests are often not considered by employers to be medical records, they may be kept in personnel files, which are less confidential and where access is less likely to be controlled. The results are sometimes shared with co-workers, supervisors, managers, prospective employers, health insurers, or government benefit agencies, all potentially having a substantially negative impact on the employee. While excessive or improper disclosures may lead to liability, employers often have a common law privilege to make certain disclosures. See *Gauthier* and *Houston Belt*, *infra*. A Boston Police cadet brought an action for invasion of privacy after a superior officer told other cadets about the cadet's dismissal from the academy for a positive drug test. The Massachusetts Supreme Judicial Court held that the police commissioner had a privilege to disclose the test result to the other cadets because the commissioner had a legitimate interest in deterring drug use by police cadets. *Gauthier v. Police Comm'r*, 557 N.E.2d 1374, 1376 (Mass. 1990).

Alternatively, in *Houston Belt & Terminal Ry v. Wherry*, 548 S.W.2d 743 (Tex. App. 1977), Joe Wherry, a railroad switchman fainted after sustaining a knee injury on the job. In an attempt to establish the cause of the fainting, the company physician ordered diabetes drug tests. The initial drug test showed traces of methadone, but a second test revealed that to be incorrect. Wherry was later discharged for failure to report the accident in a timely manner. During the course of a Department of Labor investigation of the dismissal, the railroad wrote a letter to the Department of Labor stating that Wherry "passed out and fell" and that "traces of methadone" were present in his system. *Id.* at 752. Wherry sued for libel. The Texas Court of Civil Appeals affirmed an award of \$150,000 in compensatory damages and \$50,000 in punitive damages based on this and other statements. The court stated that "the jury was entitled to conclude from the evidence that [employer] made false statements in writing that he was a narcotics user when they knew better." *Id.*

### C. Identity Theft

Identity theft is a growing problem in this country. In response to identity theft problems, employers must take greater care in disseminating private information about its employees. Many employers are required to pass employee personal information between various administrators, supervisors and even inter-office. Employers use electronic communication such as fax, email, telephone or voicemail to disseminate the information. Should an employer fail to take appropriate precautions to insure that only the authorized person have access to the employee's private information, the employer could be exposed to substantial liability. The problem of identity theft is an example of the serious problems arising out of the dissemination of private information to unauthorized people.

In *Sandra Bodah, et. al., v. Lakeville Motor Express Inc.*, 2003 Minn lexis 362 (2003), a fax sent by a defendant employer, a trucking company, to the terminal managers of 16 related or associated freight terminals, which listed the names and social security numbers of 204 employees for purposes of a records check. An employee complained because of a concern of identity theft, and the president of Lakeville sent a letter to all the drivers and dock men explaining that the list was prepared for "insurance renewal purposes" and was "mistakenly sent to other terminals." Additionally, the president instructed the Safety Department to contact the terminal managers and have them destroy or return the lists immediately. The lists were not shared beyond the small group of terminal managers.

The employees filed a tort action against the employer claiming publication of private facts. Under the law in Minnesota, to state a claim for publication of private facts, a plaintiff must demonstrate that one gives publicity to a matter concerning the private life of another if the matter publicized is of a kind that would (a) be highly offensive to a reasonable person; and (b) is not of legitimate concern to the public. The district court dismissed the complaint, stating that the list went to Lakeville employees or their agents and that the immediate follow-up letter by the president "negated any inference that the publication would be disseminated to the public at large." *Id.*

The Appeals Court reversed that decision holding that person's social security number is a private fact and that publication did occur. The Appeals court found that social security numbers are "such a significant identifier that they facilitate access by others to many of our most personal and private records and can enable someone to impersonate us to our embarrassment or financial loss." Despite acknowledging that Mr. Martin acted appropriately, the Appeals Court allowed the suit to continue because it could not be certain that the lists were destroyed. *Id.*

Eventually the Supreme Court of Minnesota overruled the appellate court finding, that publicity required communication to the public at large or to so many

people that the matter would be regarded as substantially certain to become public knowledge. The issuance of the social security numbers to the terminal managers did not constitute publication substantially certain to become public, and the employees merely speculated that the information was still being shared. *Id.*

In *Bodah*, the employer acted quickly to limit access to the private information. Had the employer failed to act quickly and an individual gained access to the information and ultimately ruined an employee's driving or employment record, it is unclear whether *Bodah's* ruling would protect that employer from liability. It is dangerous and all too common that a truck driver's identity is stolen by an individual who will gain employment using the driver's personal information and identity. Therefore, this issue remains a concern for employers who are required to disseminate personal information. Strict rules limiting to access this information is critical to insulating an employer from liability.

#### IV. CONCLUSION

Admittedly, the right to privacy is a relatively new concept in the law, but it is developing quickly and employers must confront it. For the most part, employees know they do not have the same privacy at work as they do at home, but most do not fully understand the scope of an employer's ability to review their personal information. Likewise, employers now possess a myriad of new ways in which to collect useful personal information of employees, but do not fully appreciate the danger of failing to protect that information once it is gathered.

Since the employer is the custodian of the information, the law will continue to impose a duty upon the employer to safeguard it. To meet its obligation, an employer must limit the scope and extent to which employee's personal information is disseminated, and also keep its employees updated with respect to the policies that have been enacted to protect their privacy.

### **EXPANDED EMPLOYEE PRIVACY RIGHTS REDUCING RISKS OF LIABILITY**

#### INTRODUCTION

In today's environment we are often faced with incorporating the effects of new privacy laws, regulations and expanding common law rights into our everyday business operations. It then becomes a real challenge to be certain that our company takes appropriate steps to prevent violations and minimize risks of liability.

This paper will focus on a practical approach to some basic steps involved in examining these issues and then move through the employment process from

hiring to termination, highlighting those areas where a trucking company may be likely to run afoul of the privacy rights of its employees.

Just as we require that our drivers do a pre-trip inspection before they head out on the road we might think of these steps as a “pre-problem inspection” or checklist. This requires you to actually go over each step, talk to those in your company who are responsible for the areas we will highlight to reassure yourself that your company (or your client’s company if you are outside counsel) has taken adequate measures to limit its risks of liability for violations of your employees right of privacy. On the other hand if you should discover shortcomings, take this opportunity to remedy them.

For our purpose we will assume that those in attendance at this seminar will have a general knowledge of the various laws and rulings which deal with the employee privacy rights. They will not be reviewed here except as they will apply to our checklist.

The pre-problem inspection checklist might start with the following four phases:

1. Awareness.

The company needs to be aware of the laws, regulations and common law sources which deal with employee privacy rights. However, we should all bear in mind that it is one thing to have knowledge or awareness of what should or should not be done, it is another to be sure it is being done properly.

2. Policy.

The company should have policies in place which make certain it is in compliance with the laws which protect these rights. These policies should be well thought out and implemented in an attempt to prevent problems and not to react to a crisis.

3. Personnel.

The company must have properly trained personnel responsible for carrying out these policies. A large part of their responsibility will be to understand the significance of handling confidential material and the consequences of failing to safeguard such material.

4. Performance.

The company must make sure that the policies are actually and consistently being carried out or performed. This is a critical stage because it is in this area that most violations will occur and liability imposed.

These steps may be self-evident, but as the saying goes “the devil is in the details.” Each company may have a different methodology or approach to reaching their goal of avoiding liability in this area, but each will likely involve the “three Ps,” policies, personnel and performance. With this in mind we will look at some of the most likely areas of potential vulnerability or liability during the timeline of employment. These will include:

- I. The Hiring Process
    - A. Application
    - B. References and background check.
    - C. Drug and alcohol testing
  - II. Privacy Issues During Employment
    - A. Handling confidential information
    - B. Monitoring (computer and telephone usage)
    - C. Search and surveillance
    - D. Privacy versus safety issues
  - III. Issues upon termination - Information furnished to prospective employers
  - IV. Compulsory Disclosure (Subpoena)
- I. Hiring Process
    - A. Application for Employment.

The first step in the hiring process is the Application for Employment. A checklist should begin with a periodic review of an application to make certain it does not ask for prohibited information such as age, arrest, or medical information. The application may contain certain notices and authorizations for the company to perform background checks, to release information to subsequent employers upon termination and to consent to drug and alcohol testing. However, the Fair Credit Reporting Act requires a separate notice to an applicant. The process of obtaining these authorizations and consents should be done at the earliest time to be sure the company will be able to receive background information on the applicant. If consent or authorization is incorporated into the

application for employment there should be a separate signature space directly under the consent language.

While not being related to privacy issues, an examination of the hiring process also provides an opportunity to review your applicant flow procedures to insure that your company would be able to successfully withstand an OFCCP Affirmative Action Audit.

#### B. References and Background Check

Examine your company's policy regarding background checks. It is generally recognized that it is necessary to do background checks prior to hiring or shortly after hiring a new employee to avoid potential liability for negligent hiring. This should include criminal background checks as well as background checks from previous employers. It is necessary to obtain written consent from the new employee which can be furnished to previous employers. As stated, this consent may be part of the application or on a separate document. Most companies will not furnish information on the applicant unless they have written consent. Even with consent some companies will only give dates of employment and position held. When a previous employer refuses to give information this fact should be noted in the file (rather than have no notation) so that you can demonstrate that your background check policy has been performed as a part of your due diligence. The nuts and bolts of these processes should be reviewed to make sure they are in place and are working in practice using properly trained and knowledgeable personnel.

Many companies use outside companies for background checks and in turn provide information to them. But even in these situations your company should furnish only the information provided for in your policy.

There is some information whose disclosure is mandatory by DOT regulations. Before hiring a driver a company must request drug and alcohol test results from DOT regulated employers who have employed the employee during any period during the two years before the date of the employee's application. Upon inquiry, trucking companies must furnish this information for drivers who leave their employ.

#### C. Drug and Alcohol Tests:

The Department of Transportation mandates pre-employment Drug and Alcohol testing of employees who perform safety-sensitive duties such as drivers, who are required to have a commercial drivers license. DOT regulations also require that such drivers should be tested for drugs and alcohol when involved in an accident where he is issued a citation or where there is a fatality whether or not he is issued a citation. In addition a company which is a government contractor must adopt a Drug Free Workplace policy and may, with consent, test all

employees as a condition of employment. A company may also require an employee to be tested for reasonable cause, random testing and upon sustaining an on the job injury or after a serious vehicular accident.

Other privacy issues may arise in such areas as the collection of urine samples and protecting the confidentiality of the test results. Company policy should address and clearly spell out the procedures for carrying out this test, including designating the person who has authority to request the test; being certain that the laboratory that does the testing is properly NIDA certified, specifying the contact person at the company who can receive the test results and the handling of the paperwork containing the results. While DOT regulations spell out the substances that should be included in the drug test, a non-DOT drug test may test for additional substances that have no relation to job performance. Care should be taken to prevent this additional testing by giving specific instructions to the testing lab. The safest instruction is that only DOT standard testing will be used in all drug tests. The persons handling these matters must be properly trained in the importance of confidentiality and a checklist should include having the person ultimately responsible walk you through these procedures step by step. A “dry run” through the process can verify that only trained personnel are handling this sensitive area and that they are performing in accordance with policy.

## II. Privacy Issues During Employment

### A. Handling confidential information.

Once an applicant is hired the company can obtain a post job offer medical questionnaire. As a part of your checklist you should examine the physical handling of the employee’s file to make certain that separate and distinct files are kept for personnel and medical information. They should be located in different file cabinets, preferably in an area of the office which can be locked so that only those persons with a “need to know” have access. The days of having a row of personnel file cabinets in the middle of an office, with unlimited access, should be gone. These areas should be secure so that confidential paperwork is not in full view of persons who have no reason to know their contents. The medical files would contain the post job offer medical questionnaire, DOT physical in the case of drivers, drug test results, FMLA requests and general medical information such as medical excuses for absenteeism. In companies which self administer health insurance programs or workers compensation matters, medical information dealing with each of these areas may be kept separate from other medical files, again with the preference of having separate, physically secure departments with only the personnel who deal with these matters having access. Obviously, information concerning payroll records and financial benefits such as 401k plans or retirement plans should also be kept in a separate file in separate departments. So, conceivably, one employee might have a personnel file, in the case of a driver the DOT qualification file, medical file, health insurance file and (when

applicable) workers compensation file, payroll file and 401k retirement file, each being handled by different people in different departments in different locations in the office. Some of these functions may be combined under a Human Resources Department, but protected information should still be limited to those with a “need to know.”

The Health Insurance Portability and Accountability Act (HIPPA) and its privacy regulations have also expanded privacy rights for employees with regard to medical information. Many of us have seen changes in practices such as the notice sent out by insurance companies which describe how medical information may be used and even in some pharmacies where protections have been built to provide some degree of privacy to customers. The HIPPA privacy rules became effective in 2000 and were amended in 2002. If your company is self insured and self funded for employee health coverage and is considered a Covered Entity under the Act should be aware of the provisions of HIPPA in order to establish policies which govern your treatment of employee medical information. While HIPPA does not create a new private right to sue for violation of privacy it does provide for civil and criminal penalties for violations.

#### B. Monitoring Issues (Computer and Telephone usage)

You should examine your company’s policy regarding monitoring of computer and telephone usage. If there is no policy how would abuses be handled if they are discovered? Back to our checklist, a company should first be aware that an employee has rights of privacy both at common law (intrusion into seclusion) and by statute, such as Electronic Communication Privacy Act. Your policy should address and define how these rights are balanced against the Company’s legitimate business interests.

In these areas the policy should take into account the employees “expectation of privacy” and should clearly communicate the policy in writing to all employees. For example, some companies have a policy which restricts the employee’s use of the company computer to company business only. This should be communicated to the employee either as a published written policy or a document that the employee signs acknowledging that he is aware of and will abide by such policy and has given consent for the company to monitor his use of the computers. The same holds true for companies who have telemarketing or collection departments. Employees must be made aware of the policy that telephones are for company use and that they will be monitored for compliance. These notices of policy have the effect of taking away an employee’s claim that the company’s monitoring of computers or telephones has invaded an area in which he had an “expectation of privacy”. The notice should clearly state what the employee should expect, e.g. that monitoring their computer usage may include checking to see what he is actually viewing and/or personal time used on the computer. For telephones the notice should state whether monitoring would include personal time on the telephone (for example by checking numbers called)

and/or actually listening to conversations to assure that customers are treated courteously and promptly. The same principle would likely apply to monitoring such electronic devices as cell phones, or the use by some carriers of Qualcomm.

At the same time there should be a legitimate company interest in monitoring e-mails or telephones. Thus, while monitoring customer service calls may require listening to conversations, it may not be appropriate to apply this type of monitoring for the entire office. Your policy should address these issues.

### C. Search and Surveillance

A similar situation arises when there is a question of searching an employee's person, belongings or automobile. The right of the employee to privacy is generally determined on a case-by-case basis with a crucial question being whether or not the employee has a valid expectation of privacy with regard to a specific type of search.

Video surveillance provides another area of potential liability. Because trucking companies are entrusted with goods that are owned by others there is a legitimate interest in having appropriate video surveillance. In addition, since 9/11/01 terrorist threats have increased the need for such surveillance for security purposes. However, just as video surveillance can be helpful it is also subject to abuse as, for example, video cameras which are used to "spy" on employees for reasons not related to legitimate purposes. An examination of policy, personnel and performance is necessary to avoid these privacy violations.

### D. Privacy Issues Versus Safety

There could be times when individual privacy considerations may come into conflict with concern for public safety. These situations place a company in the position of making a choice of potential liability for violating privacy laws or common law rights or violating DOT regulations and the consequences of potential liability for serious injury or death.

This could arise in several different ways, but assume that the company receives information that a driver is being treated for illegal drug use, or that a driver has been injured on the job and in reviewing medical records the self administered workers compensation department or third party administrator learns that the driver has insulin dependent diabetes and is disqualified under DOT regulations. Perhaps a driver turns in a health insurance claim for epilepsy which would disqualify him from driving. What is your company policy regarding such a situation? Do you terminate him or remove him from driver status based upon this information which was obtained in violation of privacy rights or take the risk of letting him drive knowing that he is not qualified under DOT regulations. What is your company's policy regarding a company employee in another department, e.g. health or workers compensation having

knowledge of a driver's disability based upon private medical records. Should they advise the Safety department of the driver's condition? What is your policy regarding disqualification information discovered by a third party health or workers compensation administrator? Again, this is an area where policy should be carefully considered, in advance, to be certain the company would be protected from liability and appropriate personnel are trained to handle these sensitive situations if and when they arise.

### III. Issues Upon Termination – Information furnished to prospective employers.

We have already discussed background and reference checks for new hires. On the other end of the employment timeline, you should examine your company's policy with regard to furnishing information about an employee who has left your company's employ either voluntarily or involuntarily. How much information does your policy allow to be furnished? Of course, without a written consent form from the former employee you should only furnish "name, rank and serial number" information, e.g. dates of employment and job title. Even with consent a company might refuse to furnish any further information. On the other hand we have seen a general trend toward a company furnishing more information if the consent form is broad enough to warrant it. For example, with proper consent, we would furnish information not only giving employment dates and position, but also, if asked, for a driver's vehicle accident record, reason for termination and whether he would be eligible for rehire.

If your company provides reasons for discharge you should be cautious in stating the reason. For example, stating that a former employee was discharged for theft could subject the company to liability for liable or slander unless you had adequate proof of theft such as a confession or conviction; or giving a reason such as "disabled and couldn't work" could give rise to an ADA claim. This step in the process is important and should be entrusted to a person or persons who are trained to understand the significance of the information to be furnished. When your company has multiple facilities or locations your policy must be communicated to managers and supervisors in each location. Many times they are the ones who may be called by a prospective new employer so they should be aware of how your company handles these matters. Most companies require that all references are forwarded to a central location for handling. Your checklist should include drilling down to the details of how this is being handled in your company.

Finally, there is another facet that should be reviewed. If your company is one which only gives minimal information because of a fear that the company might be liable for a privacy violation if you provide any information, consider whether this should change if you have discharged an employee for some type of assault or violence in the workplace. If you fail to reveal this to his next potential employer would your company be liable for damages if your ex-employee was

hired and then committed an assault which resulted in serious injury or death? This would probably vary on a state-by-state basis, but those persons in appropriate management positions should make these types of decisions rather than rely on a clerk in the personnel department.

Finally, you should be certain that your company abides by the DOT policy which requires furnishing positive drug test results to the new employer as discussed previously.

#### IV. Compulsory Disclosure – Subpoenas

The final area it might be helpful to discuss is the matter of a Subpoena for medical records. These situations usually arise when the company receives a subpoena *duces tecum* requesting medical records of an employee or ex-employee who, for example, is alleged to have been injured in an automobile accident. The opposing party wants to discover whether it was a preexisting injury. Of course we are aware that generally speaking such medical records should not be furnished because they are protected under privacy laws. On the other hand we are concerned that if we have such records and fail to respond to the subpoena we could be held in contempt of court and be subject to such sanctions that the court may impose. What is your company's policy with regard to responding to a subpoena for medical records? The usual response may likely be that a subpoena should be honored because it is a court order. A number of years ago most subpoenas were, in fact, issued by the court through its clerk's authorization. But as each state has its own procedures and we are seeing that subpoenas may be sent by attorneys and by third party providers.

Under HIPPA Privacy Rules a Covered Entity may disclose protected health information in response to a court order if it is expressly authorized by the court order. But where the subpoena is received from an attorney or process service company the procedure becomes more difficult. The Covered Entity must not disclose the information unless it receives satisfactory assurance from the party seeking the subpoena that it has made reasonable efforts to notify the employee who is the subject of the subpoena. The purpose here is to afford the employee an opportunity to object to the disclosure or seek a protective order so, for example, the information sought would be furnished to the court "in camera". While HIPPA only applies to Covered Entities, if your company is self insured with regard to health plans it may be treated as a Covered Entity subject to HIPPA rules.

Companies that operate in multiple states should also be aware that some states may have privacy laws that are more protective than any of the Federal statutes. It would be prudent to check with your local counsel in those states to determine what type of response is required to a subpoena for medical records. A process should be established which would insure that these subpoenas are

handled by a person trained to understand the importance of protecting private medical information.

It is apparent that as more and more information becomes available to employers through technology, the privacy rights of employees will be expanded to afford them protection for harmful dissemination of private information. As employers we should take steps to see that a process is in place which keeps pace with these developments.

## **INSURANCE COVERAGE FOR INVASION OF PRIVACY**

As noted above, employers often have conflicting obligations concerning their employees' privacy. There must be a balancing of the employer's business interests with their employees' privacy rights. Even the best prepared employer may find itself in the position of defending an action grounded in privacy, whether arising from common law or a violation of statute or regulation, which is brought by an employee or a group of employees.

If an employer finds itself in the position of defending an employee's claim for invasion of privacy, it becomes very important to look for coverage for both defense and indemnity for the claims asserted. There are several types of insurance contracts that can provide liability coverage for invasion of privacy claims which are brought by employees. Note that the interpretation of coverages and exclusions under an insurance contract is a matter that is determined by applicable State law.

### **I. General Rules of Policy Interpretation**

Insurance contracts are interpreted to effectuate the intent of the insurer and the insured at the time that the policy was issued. As explained in Ostranger & Newman's *Handbook on Insurance Coverage Disputes*, §1.01 (8<sup>th</sup> Ed.), courts look to the language of the whole policy to determine the intent of the parties.

Policies that are worded in plain and unambiguous terms are generally enforced as written, unless they violate public policy. However, where a term or phrase in a policy can be interpreted in more than one way, the policy is ambiguous. Where there is an ambiguity in a particular phrase or term in the policy, the courts first review the entire contract in an attempt to determine the parties' intent. If the parties' intent cannot be determined by reviewing the entirety of the policy, courts will likely next consider extrinsic evidence, such as the parties' correspondence concerning policy terms and conditions, to ascertain intent.

If the parties' intent concerning an ambiguity cannot be determined by either reviewing the contract as a whole or through extrinsic evidence, most courts apply the *contra proferentem* principle, which means that ambiguous terms of a contract are construed against whomever drafted the contract. Since insurers are the drafters of

insurance policies, all such ambiguous terms in policies are interpreted against the insurer.

## II. A Note Concerning Conflicting State Law

As noted above, State law controls in disputes about insurance policy provisions. Accordingly, it may be important to ascertain which State's law might apply to policies which might afford coverage for employees' privacy claims. One who seeks insurance coverage should begin the quest by ascertaining the State law that a court would use to interpret the provisions of the insurance contract. Every State has rules for choice of laws and conflicts of laws. These rules dictate when and how a court must apply the laws of various "interested" States. They are often complex and cumbersome, and must be researched on a case-by-case basis.

Generally, one of the primary factors that courts use when determining which State's law applies to an insurance policy is the State where the policy was "delivered." Policy delivery is usually made by the insurer at the insured's address, as described on the declarations page. For employers with locations and employees in only one State, insurance policies are usually deemed to be delivered to the insured in that State, and that State's law would apply.

On the other hand, multi-state employers have addresses in more than one State. In such instances, most States' courts would view the insured's address on the declarations page as a significant factor concerning policy delivery. Note that the insurer, the insured or both could have reasons for desiring policy delivery in a State other than that identified in the insured's address, may have separately negotiated for policy delivery. Again, issues of conflict of laws and choice of laws are quite specific for each State and are often peculiar to each situation.

## III. Types of Policies which May Afford Coverage

There are several sources that may afford liability coverage to an employer for invasion of privacy claims brought by employees. Note that particular provisions of policies can differ greatly. Many insurers use standardized policy forms and endorsements that are drafted by the Insurance Services Office, Inc. ("ISO"). Some insurers use their own forms and endorsements or modify language of the ISO forms. Yet other insurers issued "manuscript" policies with varying terms and conditions that are often negotiated between the insured and the insurer.

### A. Comprehensive General Liability (CGL) Policies

CGL policies generally provide liability coverage to commercial entities for most exposures. They can be endorsed to include nearly complete liability coverage for specific types of commercial risks, including everything from a barbershop to a widget factory. Insureds who insure their business property and liability exposures in a business owner's package ("BOP") policy usually have CGL coverage as a part of the BOP policy.

The CGL is an important potential source of liability coverage for employees' privacy claims. In general, CGL policies agree to pay, on behalf of an insured, all sums (up to the limit of liability) for which is insured is legally obligated to pay for those "personal injury" and "bodily injury" claims which are covered by the policy. (Please refer to "Bodily Injury v. Personal Injury" discussion below concerning these terms.) The typical CGL policy insuring agreement would likely provide coverage for the insured against employees' privacy claims.

Yet, like all insurance policies, the CGL policy is subject to limitations. The relevant policy limitations are as follow:

- Exclusion for "Bodily injury" to an employee during the course of employment. If the employee's claim against the employer seeks damages for "bodily injury," the CGL will not provide coverage.
- Exclusion for "Intentional Conduct" on the part of the insured. If the insured intended to invade the privacy of the employee and (in most States) further intended to cause the injury to the employee, the CGL will not provide coverage.
- Invasion of privacy claim is not within definition of "Occurrence." CGL policies usually only provide "bodily injury" coverage for an "occurrence," which is generally defined to mean an accident, including repeated exposure to harmful conditions. If the invasion of privacy (or, in most States, the consequence thereof) was not accidental, the CGL would not afford coverage.
- An "Employment Related Practices" endorsement is attached to the GCL. The GCL would generally provide coverage for to the employer for "personal injury" sustained by an employee, unless this endorsement is attached. Note that many, if not most, CGL insurers include an Employment Related Practices exclusion on the policy.

As noted in the introductory materials, employee claims of invasion of privacy can be based in common law or in State or federal statute. These claims can seek remedies for "bodily injury," "personal injury" or both. In short, these claims can take numerous forms, and both the basis of the claim and the type of remedy sought can evolve during the life of the claim. For those reasons, it is essential for the employer to place its CGL carrier on prompt notice of a potential claim for invasion of an employee's privacy.

## B. Commercial Umbrella Coverage

The forms that Umbrella policies can take vary widely among insurers. Generally, Umbrella policies are designed to provide liability coverage above, or in

excess of the limits of, "primary" liability policies, including CGL policies. In other words, Umbrella coverage begins at the point that the limit of liability of another liability is exhausted. In most cases, Umbrella insurers require insureds to maintain "primary" liability coverage, including a CGL policy (or its equivalent.)

An additional feature of Umbrellas is that they may provide coverage that is not provided by the "primary" policy. If an Umbrella policy provides liability coverage to the insured for claims that are not covered by "primary" policies, that coverage is usually provided subject to a deductible or a "self-insured retention." As such, the insured would be required to pay a portion of the claim.

Because the forms for Umbrella policies vary dramatically among insurers, it is essential for insureds to carefully review the policy in order to determine whether coverage might be afforded. Read the insuring agreements to determine the scope of the coverage provided. Then, review the definitions of "bodily injury," "personal injury" and "occurrence." Examine the exclusions, paying particular attention to exclusions that deal with employees and intentional conduct. But always give notice of the claim to the Umbrella carrier.

#### C. Directors and Officers Liability Coverage (D&O)

Another potential type of policy that may afford coverage for employees' invasion of privacy claims is a D&O policy. This type of policy provides broad liability protection for the Board of Directors and the officers of a company for their conduct as members of the board and/or as company officers. Note that the insureds are usually the employer's directors and officers and that many D&O policies do not identify the company as an insured. Most D&O policies do not specifically exclude coverage for employment-related claims, such as invasion of an employee's privacy.

There are, however, some restrictions in D&O policies concerning the availability of coverage. First, as noted above, if the company is not identified as an insured under the D&O policy, only claims asserted against individual directors and officers will be covered. As such, claims asserted against the company (employer) would not be covered.

Second, please note that the policy's coverage is restricted to company directors and officers. If the asserted infringement upon privacy was accomplished by a non-officer or non-director (for instance, by a mid-level manager), a D&O policy would not provide coverage.

The third potential for exclusion of coverage arises from language in most D&O policies that excludes coverage for an action by one insured against another insured. Since officers and directors are the insureds under a D&O policy, it would not provide coverage in the event that an officer and/or a director was the person who brought the claim.

Finally, it should be noted that many D&O policies exclude claims that are grounded in libel or slander, as well as claims which allege emotional distress as damages. If this exclusion is present in the D&O policy, there would be no coverage for a claim asserted by an employee who proves libel or slander, or for the emotional distress damages awarded.

It should be noted that D&O policies can be endorsed to provide coverage for the employer-company as an insured. They can also be endorsed to expand the definition of insured to encompass all employees, to eliminate the exclusions of coverage for claims brought by an insured against another insured and to remove the libel/slander and emotional distress damages exclusions. While these endorsements are available from many D&O insurers, they usually represent a significant premium increase over the basic D&O policy.

There are two other issues associated with D&O policies that employers should note. One of those issues is that D&O policies are "claims-made" types of insurance contracts. Unlike the CGL's occurrence-based coverage (claims are covered when they occur during a policy period), D&O policies respond only to claims which are asserted during the coverage period. The key to obtaining coverage under D&O (and all claims-made coverage) is prompt reporting to the insurer. As well, claims-made policies exclude coverage for known claims that occur prior to the coverage period, unless they are endorsed to provide that coverage. Accordingly, the insurer can escape coverage if the insured knows about a situation that is likely to cause a claim, but fails to report that situation to its D&O insurer, and/or fails to disclose that situation to a new D&O carrier prior to policy issuance.

The other issue associated with D&O coverage is that the limit of the insurer's liability is subject to both a per-claim limit and an aggregate annual limit. Then, if the D&O insurer pays a claim, that payment will reduce the amount available for subsequent claims which are presented under the same coverage period.

As with CGL and Umbrella policies, it is recommended that all claims be promptly reported to D&O insurers. That is particularly true in the instance of D&O (or any claims-made) policies, as coverage keys off of the date of the report of the incident, rather than the date that the event actually happened. However, since there is an aggregate limit of liability which can be depleted by paid claims, it is mandatory that the company's officers and Board of Directors be apprised of the claim.

#### D. Excess Indemnity Contracts (EIC)

This type of coverage is not traditional insurance. It does not pay liability claims "on behalf of" the insured, but rather it pays the insured back (indemnifies) the insured when the insured pays a covered claim. Further, under an EIC, the insurer usually does not have a duty to defend the insured, but shifts responsibility for defense and settlement of claims to the insured. Most EICs have a substantial Self-Insured Retention ("SIR"). The cost of investigating and defending claims is ultimately pro-rated between the

insured and the insurer after all claims have been paid. In most EICs, unless the insurer pays a claim above the insured's SIR, there is no obligation for the insurer to pay any part of defense costs.

One advantage to EIC coverage is that, as to the employer-insured, it is much broader than coverage afforded by the CGL. Generally, EIC coverage reimburses the insured company (employer) for a broad range of liability claims that arise from the insured's "operations." The insured's "operations" are usually described as activities which are necessary to carry on the insured's business. There are comparatively few exclusions in most EIC basic contracts that could preclude coverage for an employee's privacy claim, although some EIC insurers might separately exclude coverage for employment-related practices, including privacy claims.

Another advantage to seeking coverage under an EIC is that most EICs provide coverage for punitive damages, so long as applicable State law does not prohibit insurance for punitive or exemplary damages. This becomes especially important if the conduct of the insured might be considered as egregious, or where there otherwise might be insured punitive exposure for a claim.

Note that most EIC policies exclude coverage for the insured's intentional conduct. As noted in the "intentional conduct" discussion in the CGL section above, the precise definition of intentional conduct is a matter of State law. The EIC insured should be aware, though, that its employees are usually not "insureds," as that term is defined in the contract. An EIC does not generally provide direct coverage for an insured's employee against whom a privacy claim is made, but coverage does extend to the employer-insured for its vicarious responsibility for its employees' conduct. This distinction only becomes a coverage issue for an employee, and then only in the event that the employee's conduct was not within the course and scope of his employment for the insured-employer.

Note also that an insurer's obligation under an EIC does not extend to claims that are less than the SIR. Since the insured bears the cost of investigation and defense of claims and because the EIC insurer does not have an obligation to share those expenses unless it pays a claim, if an employee's privacy claim is successfully defended, or is settled by the insured for an amount which is less than the SIR, the insured will have spent significant sums to conclude the matter. As with any insurance coverage, it is essential to promptly report claims (or potential claims) involving asserted invasions of an employee's privacy.

#### E. Employment Practices Liability (EPL)

As one might expect from the title, this type of coverage provides the most comprehensive form of potential coverage for employees' privacy claims. It is targeted to provide rather broad coverage for most types of employment-related claims, including common-law claims, such as employees' privacy matters.

Like D&O, EPL policies are customarily written as "claims-made" contracts. Most EPL policies cover only "personal injury" claims and exclude coverage for "intentional conduct", "bodily injury" and certain statutory claims, such as claims pursuant to the Americans with Disabilities Act (ADA) and the Workers' Adjustment Retraining Notification Act (WARN).

As with EICs, some EPL policies provide coverage for punitive damages, where State law does not prohibit insurance for this type of damages. Also, employment-related claims often result in an employer being ordered by a court to refrain from (or to commence) some sort of activity, such as refraining from looking at employees' email. This type of court order does not involve direct payment of a plaintiff's claim, and is in the general category of non-monetary relief. Such orders can be for injunctive or declaratory relief, retraining, job reinstatement, etc. Most EPL policies do not provide coverage for a court's award for non-monetary relief.

#### IV. Miscellaneous Matters

##### A. "Bodily Injury" or "Personal Injury"?

When reviewing any policy for potential coverage for employees' privacy claims, it will be necessary to first ascertain what sort of injury was allegedly sustained. Claims for physical injury to a person are usually considered to be "bodily injury" claims, while claims for loss of reputation, emotional distress, etc., are usually regarded as "personal injury" claims. While it is often clear whether a claim is for "bodily injury" or "personal injury," there are claims that might be in a gray area between the two terms. In these instances, it is necessary to ascertain the state of the applicable State's law to determine whether coverage may be afforded under an insurance contract.

##### B. Intentional Conduct or Negligent Conduct?

Again, State law plays a very important role in determining whether a particular claim can be excluded by an insurer by its use of an "intentional conduct" exclusion. Some States look only to the insured's act which gives rise to the claim to determine whether an insurer may exclude the claim as an intentional act. If the original act was intentional, those States would likely permit the insurer to decline coverage. Other States look beyond the original act, including the natural result of the insured's conduct, to determine whether a matter might be excluded. If the insured intended to permissibly infringe on its employees' privacy, but did not intend the result of that infringement, the insurer will not be permitted to decline coverage.

#### V. Conclusion

There are several potential sources of insurance coverage that may respond to an employees' claim for invasion of privacy. Those sources offer varying levels of coverage, but there are both benefits and burdens to each available form.

Whether an employer is contemplating the purchase of coverage, generally reviewing its various insurance programs, or seeking coverage for an actual claim, it is essential to thoroughly review insurance contracts with a basic understanding of applicable State law concerning policy interpretation, damages, and definitions of types of injuries.