Privacy in the Workplace and Conducting an Internal Investigation ©

By Randy Howry
HowryBreen L.L.P., Austin TX

Introduction

Privacy in the workplace and conducting internal investigations related to employment law and practices are areas that have become increasingly complex since the use of electronic devices and communication has become so pervasive in the workplace. The objective of this paper is to address issues related to privacy and internal investigations in the workplace, offering practical information for business owners, managers, human resource professional, in-house counsel and legal advisors.

I. Privacy in the Workplace: The Developing Law and Practical Applications

To protect businesses and companies from unwanted employment litigation, employers need to be very familiar with various laws governing the workplace in many areas of employer/employee relations. These laws include federal statutes such as: Civil Rights Act of 1964 and Title VII; Age Discrimination in Employment Act of 1967; Americans with Disabilities Act of 1990; Immigration Reform and Control Act of 1986; and the Civil Rights Act of 1866. Applicable state statues in Texas that also are important include: Texas Commission on Human Rights Act of 1983 and the Texas Workers' Compensation Act .

A. Screening Job Applicants: Reference Checks, Credit Checks, Drug Testing

Screening job applicants thoroughly, though fairly, is the best course of action for an employer for a variety of reasons. However, keep in mind that federal law prohibits an employer from discriminating against any person on the basis of sex, age, race, national origin, or religion. In addition, employers cannot ask personal questions during job interviews such as: medical or disabling conditions an employee may have; marital status; whether or not the person has children, or plans to; religious beliefs (unless it is a religious-based organization); age; sexual orientation; where the job applicant was born; and if the job applicant has ever been arrested.

While screening job applicants, diligent documentation of hiring processes, including background information and work history, is an important practice to protect companies from negligent hiring claims. It is acceptable to ask a job applicant to submit official records such as transcripts, certificates and licenses. However, it is not permissible, according to the EEOC (Equal Employment Opportunity Commission), to inquire about a job applicant's arrests or problems with the law, unless the job to be performed requires by law that information to be disclosed. If an EEOC claim is filed, the employer must be prepared to show how the criminal record was relevant to the job in question.

Extensive detail is provided in this paper in the second part on the benefits of conducting thorough investigations of job applicants, rather than current employees, as a method of screening to protect the workplace from unwanted problems.

Reference Checks – ideally all applicants should sign a waiver and release of liability when they leave a job so that a new employer can contact the previous employer for a reference. When an employer is contacted about a previous employee, the employer should be very careful to be factual, in good faith and non-inflammatory. Case in point: *Frank B. Hall Company v. Buck, 678 S.W.2d 612 (Tex. App-Houston [14th Dist.]1984*. A terminated employee suspected that his previous employer was bad mouthing him so he paid a private investigator to pose as a new employer who recorded the defaming comments of the man's

previous boss. A jury agreed that the defamation was unwarranted and damaging and awarded the terminated employee $2 million in total damages.

On the employer side, in 1999 the Texas Legislature enacted into law H.B. 341 (Texas Labor Code Chapter 103) which deals with defamation liability and the release of information about a job applicant from one employer to another. The law offers protections against defamation lawsuits, as long as the employer can prove they did not knowingly report false information.

Credit Checks - Credit checks have long been disliked by the EEOC claiming they encourage unnecessary discrimination against job applicants. While a rising number of employers are running credit checks on potential employees, finding increased amounts of debt owed on mortgages, credit cards and student loans, many lawmakers are trying to change this practice given the uncertain economic times and how that negatively impacts a job applicant's chances of finding work. Texas is one of five states in the U.S. that is currently trying to curb the practice of credit checks for screening job applicants, unless they can prove there is a direct connection to a person's bad credit and their ability to perform the job.

Refer to Section II of this paper – Conducting a lawful internal investigation – for extensive details offered about the Federal Credit Reporting Act.

Drug/Alcohol Testing –
While Texas law contains no general provision for drug/alcohol testing, most employers favor testing job applicants as opposed to current or incumbent employees. Reasons for this include: it is more legally defensible to test job applicants over current employees; there is no employee/employer relationship or issues of job performance; employers generally have the right to make a workplace "drug-free"; job-applicant testing as opposed to employee drug testing is less likely to result in union-filed grievances.

In addition, job denial for applicants is not nearly as complicated as employee dismissals from the standpoint of severance pay, pensions, unemployment benefits, etc.; job applicant testing won't impact employee morale the way employee testing would; job applicant drug testing sends a strong message to the new employee about the employer's desire for a drug-free workplace; and job applicant testing is more cost effective because it keeps drug users out of the employer's workplace which can drain resources when drug abuse problems arise.

If an employer decides to implement a drug/alcohol testing practice of current employees, it is very important to complete certain steps before implementing the practice:
Create a policy for your workplace; have employees sign the policy as acknowledgement and compliance; state clearly in policy which employees will be tested; policy must include discipline procedures for employees who test positive; include a search procedure in the workplace policy; state in the policy the steps that will be taken toward termination if an employee refuses a search or to take the test; a positive drug test should always be confirmed with a (gas chromatography/mass spectrometry) GC/MS method which is required by the Texas Workforce Commission in order for an employer to avoid an unemployment insurance claim; confidentiality is key; and employers need to make sure that employees being tested sign a consent, not only to the test, but also for any lab results to be shared with their employer and the Texas Workforce Commission.

A final note is that drug tests are not included in the definition of what is considered a "medical examination" by the Americans with Disabilities Act (ADA), and thus may be given at any time an employer deems necessary, assuming the employer has implemented the right protocols.

<u>B. Evaluating Performance and investigating misconduct: surveillance of calls and emails, searches of workplace and polygraph tests.</u>
The two main federal laws that pertain to workplace privacy issues are the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA). The ECPA was passed in 1986 to protect electronic communications that are configured to be private, such as email and electronic bulletin boards. The predecessor to this Act was the federal Wiretap Act. The SCA was enacted because the dynamics of the

Internet presented a host of potential privacy breaches not protected by the Fourth Amendment. The SCA makes it a crime to access without authorization any electronic communication while it is in electronic storage. The ECPA protects the interception of electronic communication while the SCA protects the access to stored electronic communication. These two statutes offer both criminal and civil prosecution to which no one is immune – business owner, employee, employer, contractor, shareholder, etc.

Offering these two federal laws as background, the question is how does all this trickle down to the day-to-day functions in any given workplace setting. On the issue of privacy of employee email and other forms of electronic communication (pagers, cell-phone [texting and phone calls], laptops, desktop computers, etc), the most important issue is that employers make sure that company policy on this vast subject is clearly understood by all employees. As long as an employer has clearly defined the limitations on usage of office property for personal use and can prove that the policy has been clearly publicized to all staff, an employee claiming an invasion of privacy in this area will not have much of a case.

Most employment law cases in this area have sided with the employer as long as an electronics communications and devices policy is in place, and there is no proven unlawful activity by the employer such as harassment or coercion. Issues become more complicated is in the areas of how employees are interacting with online websites, blogs and bulletin boards and what of that is personal and what is connected to their work. Any comments that are considered defamation of character of an individual, regardless of how true an employee or employer may believe them to be, is against the law.

A new area that has generated conflict between employee and employer is the use of location monitoring, either GPS (global positioning system) or RFID (radio frequency identification). Most reported cases involved placing the location monitoring device in the employees' work vehicle without them knowing. The lawsuits have claimed discrimination and mistreatment, but no direct claims about the devices themselves. However, at present, federal law does not address the use of location monitoring in the employment context. It is important to note that while federal law has not caught up with the technology, labor unions have and are pushing state legislatures to offer more protection to employees. Bottom line, once again, is proper disclosure in employee policy, by letting employees know that location monitors may be in use and having them consent to that knowledge, an employer is protected.

Otis Elevator Co. V. Local 1, International Union of Elevator Constructors, 2005 WL 2385849 (S.D.N.Y. 2005) offers an applicable case study. Otis Elevator's installation of GPS devices in company vehicles unleashed a labor dispute between the union and affected member workers versus the company. The union claimed that the devices created a "Big Brother" type monitoring situation and invasion of privacy. Otis countered that the information gained from the tracking devices would allow them to dispatch employees more efficiently and track vehicle mileage. The district court affirmed an arbitration in favor of Otis, allowing the company to keep the monitoring devices in their vehicles as long as they could continue to prove that the information collected from the devices was used to improve business practices.

Another case example is *Elgin v. St. Louis Coca-Cola Bottling Co*., 2005 WL 3050633 (E.D.Mo. 2005). Leon Elgin, an African American, sued his employer under state law for race discrimination and for the tort of intrusion on seclusion. He complained that his employer had secretly installed a GPS device in his company vehicle as part of an investigation into cash shortages in vending machines in the company's assigned areas. The employer also had installed the tracking devices in the vehicles of Caucasian workers. The district court granted a summary judgment to the employer stating, "use of the tracking device on defendant's company car, even though it was assigned to the plaintiff, does not constitute a substantial intrusion upon plaintiff's seclusion, as it revealed no more than highly public information as to the van's location. Especially because the van was the property of defendant, defendant's use of the tracking device on its own vehicle does not rise to the level of being highly offensive to a reasonable person." (2005 WL 3050633 * 4)

Use of Polygraphs and Privacy Issues –
In 1988 the debate between employee privacy versus the need for workplace protection came to a defining moment with the passage of the Employee Polygraph Protection Act. The passage of this act was the

government's effort to strike a balance between employer's rights and employees' privacy. The Employee Polygraph Protection Act (EPPA) prohibits most private-sector employers from requiring job applicants or current employees to take polygraph tests (aka lie detector tests). Under this legislation, the routine use of polygraph tests is permitted only in organizations that produce and distribute controlled substances, and those whose work involves them in national defense, security services, nuclear power, some elements of the transportation industry, or certain involvements with currency, commodities or proprietary information. Detailed information concerning specific exemptions can be obtained through the United States Department of Labor (DOL), the enforcement arm for the EPPA, at www.dol.gov.

Workplace Searches –
The justification and ultimately legality of workplace searches boil down to two opposing sides – the employer's need to protect the workplace and how much information employees were offered about the possibility of workplace searches versus respecting the privacy rights of the employee.

The outcome of these cases depends on the judge's view of the worker's misconduct and the employer's methods for getting to the bottom of things. Because there are no legal guarantees in this area of law, you would be well advised to talk to a lawyer before conducting any type of search. Keep in mind the following: Search only if necessary; Verify first, if possible; If you plan to search, have a policy; Don't conduct random searches; Never search an employee's body; Restrooms and changing rooms are generally off limits; Consider the worker's privacy expectations; and Don't hold employees against their will.

C. Privacy Issues in formal complaint procedures and litigation
In addition to the cases mentioned above, the case below reinforces the complexities employers and employees face in today's workplace.

Michael A. Smyth v. The Pillsbury Company, C.A. NO. 95-5712, U.S. District Court for the Eastern District of Pennsylvania
Michael Smyth was a regional operations manager with the Pillsbury Company. Pillsbury assured its employees that its email system was proprietary and protected and would not be used against employees. Smyth sent some unprofessional comments via his Pillsbury email account from home to his supervisor, assuming it was protected. The emails were intercepted and he was terminated. Smyth filed suit claiming an invasion of privacy. The court found that an employer can terminate an employee for any reason it deems necessary, unless that reason goes against public policy. The court further found that once an email is sent, Smyth lost any reasonable expectation of privacy. Finally, the court noted that Pillsbury interest in preventing inappropriate or illegal activity over its email system was more important than Smyth's privacy of email communication.

II. How to Lawfully Conduct an Internal Investigation

While many forms of electronic communication and transmission have made our workplaces more productive and efficient, they also have ushered in a new generation of issues related to corporate governance and compliance. Whether an internal investigation is initiated due to an employee whistleblower, a concerned manager or executive, or receipt of a lawsuit, employers must navigate carefully and strategically to avoid a host of issues.
When an extensive Internal Investigation is needed, often the ideal solution is to create a team of investigators that include in-house counsel, a human resource staffer(s) and an outside attorney or professional investigator. The team approach offers the essential element of corroboration should the complaining employee, the accused or a witness change his or her earlier statement or testimony.

Guidelines for conducting an internal investigation include: Decide what the objective and goal of the investigation will be; identify the potential disadvantages of conducting the investigation; select the appropriate investigator or team of investigators; identify potential witnesses; collect all documents that can be used in the defense (employee policies, communications, notes, expense reports and receipts, prior

complaints, etc.); outline investigation questions; secure all electronic data in storage and communications; and conduct periodic assessment of the investigation proceedings.

A. Employer Obligations: privacy, confidentiality, privilege

Wise company owners and business executives should always be in touch with the delicate balance between corporate responsibility and employee rights if there is a concern that a criminal act has happened or is ongoing in their workplace. While recent signals from Congress, the Justice Department and federal regulators warn of an increase in enforcement of federal criminal statutes in the employment context, violation of employee rights continue to be a favorite verdict of juries.

B. Electronic surveillance and email files

Monitoring of employee electronic communication is an obvious priority in an internal investigation, but if an employer has not attempted to get consent from employees to do so, then the employer has no right. This is in accordance with the Electronics Communications Privacy Act (ECPA). Several courts have suggested that an employer simply needs to notify employees that their communications may be monitored, and if the employees continue to use the electronic communication after receiving the notice, then that is their implied consent to the notice. See *Griffith v. Milwaukee*, 74 F.3d 824 (7th Cir. 1996). The ideal scenario is that employers prepare a written consent that employees sign which affirms that employer monitoring may take place only for legitimate business purposes.

An interesting example of workplace privacy via email is a recent case of first impression. A New Jersey judge held that an employee's e-mail to her lawyer sent by use of a company computer isn't a protected attorney-client communication, and the company's lawyers did no wrong in retrieving the message. Superior Court Judge Estela De La Cruz's decision, in *Stengart v. Loving Care Agency*, BER-L-858-08, turned
on the fact that an employee handbook, distributed to staff and made available on the company servers, warned that e-mail and voice-mail messages "are considered part of the company's business and client records" and "are not to be considered private or personal to any employee." The judge also found that the company lawyers did not obtain the e-mail in a clandestine or sneaky way but through "routine imaging and recovery" after litigation began, to comply with court rules for preserving discovery.

C. The Effect of the Fair Credit Reporting Act

The Federal Credit Reporting Act (FCRA) is the federal law that governs pre-employment screenings, primarily background checks that are prepared by a third party. Third party professional investigators include credit bureaus, screening companies and private investigators. The background reports could include criminal and civil court records, driving records, past employment, education, professional licenses, worker compensation, social security number traces and credit reports.

There are four important criteria for an employer to meet to comply with FCRA in using any type of investigative reports on potential employees:

1. Statement of compliance to outside agency by employer that it will honor all FCRA rules;
2. Before obtaining any type of report from the outside agency, the employer needs to have in hand the written consent of the potential employee to the investigation;
3. If the employer finds out information that leads to denial of employment for the investigated employee, the employer must share the report with the employee so he or she knows the substance of the denial;
4. If the employer decides to follow through and deny the employee the position, a Notice of Adverse Action must be provided to the employee explaining the situation.

Originally passed in 1970, FCRA was amended in 2003 when President George W. Bush signed into law the *Fair and Accurate Credit Transaction Act* which reauthorized and amended the FCRA by exempting third-party investigations of alleged employee misconduct from its notice, consent and disclosure mandate. The FCRA also has been amended in other ways in recent years related to the subject of disposal of data

and information that is acquired about potential employees and what to do with that data if the person is not hired, or when they are terminated.

It is important to note that the FCRA does **not** control background investigations conducted internally by the employer such as calling references supplied by the prospective employee. However, it is recommended that the employer conduct its investigation with the FCRA criteria in mind to avoid future potential legal problems.

The important thing to remember is that the statutes put into place by the FCRA provide legal protection not only for the potential employee, but also the employer, assuming the employer complies with the criteria set forth by the FCRA.

Closing
The complexities of balancing the desires and rights of employees with what makes good business sense is an ongoing battle for business owners, managers and executives. Having clear, comprehensive workplace policies in place that all employees have consented to knowing and accepting is key to keeping the peace.