# Workplace Privacy

## *Here's how to stay on top of this continually changing — and dangerous — realm of employment law*

12

***Judith Ashton and Gary M. Feldman***

In the last decade, the law of workplace privacy has been transformed. Computer use has increased exponentially in nearly every workplace. Employers are extraordinarily challenged to monitor and control use, to protect workers from unseemly transmissions, and to preserve confidential information. Technology also allows for precise drug and genetic testing and for close video monitoring of workers. Employers must make informed decisions as to when these tools are appropriate and what legal strictures apply.

The American workforce continues to diversify as the population has grown to include many more people whose first language is not English. These workers must be accommodated and integrated into the work environment. Moreover, applicants and employees are becoming extremely sophisticated about their privacy rights – and their lawyers more creative about expanding the kinds of claims that are actionable. And as if this were not enough to manage, state legislatures and the U.S. Congress continue to legislate actively in the area of employee privacy.

Corporate decision-makers can ill afford to ignore these transformations in workforce demographics and the law of workplace privacy. Rather, they must not only understand them and respond to them, but must also anticipate the inevitable changes to come and be prepared to address them capably.

In this chapter, we'll look at the seven main areas in the workplace privacy realm:

- references and background investigations;
- testing for illegal substances;

*Judith Ashton, a shareholder at Davis, Malm & D'Agostine, P.C., specializes in advising corporate clients and individual employees on employee-employer relations issues. She may be reached at jashton@davismalm.com. Gary M. Feldman, also a shareholder at the firm, advises employers and business executives in all aspects of employment-related issues and policies. He may be reached at gfeldman@davismalm.com.* *The authors thank Lori A. Jodoin, a Davis Malm associate, for her able research assistance.*

- genetic testing;
- monitoring computer usage, e-mail and instant messaging;
- 'personal' privacy issues such as romantic relationships;
- video and audio monitoring; and
- record retention and disposal.

## References and Background Investigations

While most Western European employers have long been limited to asking applicants job-related questions, in the United States, employers were once free to inquire about almost anything in an applicant's life. Today, however, federal and state laws prohibit employers from asking applicants many types of questions in application forms and interviews. They also bar employers from asking outside sources for certain information about applicants unrelated to their ability to perform the job. For example, an increasing number of states forbid questions about marital status and sexual preference and limit inquiries concerning criminal history. Both federal and state laws prohibit inquiries about age (employers may ask whether the applicant meets legal age requirements); disability (unless related to whether the prospective employee can, with or without accommodation, perform job functions or would endanger his, hers or others' health or safety); and questions about other legally protected statuses (race, sex, etc.).

Employers should conduct annual audits of all pre-employment information gathering processes, including application forms, interview procedures and background investigations, to ensure that no unlawful inquiries are made. Equally essential in the audit is to ensure that every employee who participates in the hiring process (this includes all interviewers and decision-makers) knows exactly which inquiries are legal and which are not. Disappointed applicants are increasingly aware of their legal protections and may take action regardless of whether the decision not to hire them had anything whatsoever to do with an illegal inquiry.

Lawsuits regarding references employers give about former employees have burgeoned over the past several years. Without a doubt, this trend will grow in 2006. Some of the cases in this minefield of litigation have been brought by those unhappy that their ex-employers disclosed certain information. Predictably, other cases have been initiated by those unhappy that information was *not* disclosed. Many theories have been advanced by litigants, including defamation, invasion of privacy, fraud, negligent misrepresentation and retaliation.

### *'Defamatory Self-publication'*

Several state courts have recently embraced a new legal theory called "defamatory self-publication." In such a case, the terminated employee claims that she was fired for reasons that were false and, in applying for another job, she must necessarily inform the prospective employer why she was fired. Essentially, she claims that by firing her for false reasons, her former employer has compelled her to defame herself. Such a claim seems to turn the longstanding "at-will" employment doctrine on its head. This doctrine provides that an employer can let an employee go for any reason, or no reason, unless doing so violates a contract or is discriminatory.

Nonetheless, courts in Arkansas, California, Iowa, Kansas, Michigan, Minnesota, Missouri, Montana, North Carolina and Vermont have allowed such claims. In a 1996 case, for example, a retail store department manager, fired for an attempted theft that she did not commit, was allowed to sue the ex-employer that had accused her, for self-defamation. The court ruled that the employer should have foreseen when it falsely accused her of theft that she would have to disclose to prospective employers the reason she was given for her termination. In that decision, the court made no distinction between an ex-employer actually giving a false reference and the terminated employee providing that information to a prospective employer on her own. Other states have rejected the doctrine. These states include Colorado, Connecticut, Hawaii, Massachusetts and Tennessee. The jury is still out elsewhere.

### *Breach-of-contract Claims*

Terminated employees have also been successful recently in breach-of-contract claims against their ex-employers. In these decisions, the employers gave negative references to prospective employers in spite of either agreements to provide positive references or agreements not to disclose negative information about former employees. For example, one Connecticut trial court allowed a man to sue his ex-employer for telling a prospective employer that he had been fired (from his job as a nurse for making medication-related errors) because he and the former employer had entered into a termination agreement. The agreement required the ex-employer to expunge any references in his file to his termination and to allow him to resign voluntarily.

### Eight Steps to a Successful Reference Policy

Given the volatility of the law, a written policy concerning references is essential. In developing such a policy, an employer should take the following eight steps.

(1) Know the reference laws in the states in which the company operates.

(2) Develop a written policy for giving references that includes, at the least, the names of those who will respond to requests, information on what will be provided (either with employee consent or without it), as well as a procedure to document the reference given. Include in the policy a procedure under which reference information will be provided without employee consent when legally required.

(3) Ensure uniformity in approach, except for special situations when the law requires disclosure or when a non-disclosure agreement has been executed.

(4) Provide a procedure for the responder to acquire the information he or she needs to give an accurate reference.

(5) Train those responsible for responding, emphasizing what to do in situations in which a termination agreement has been executed, situations in which the employer knows that an ex-employee had engaged in dangerous behavior, and circumstances in which there is pending litigation with the employer. These situations should always entail consultation with legal counsel, as should situations in which the responder has any doubt about what to do.

(6) Train all other employees to refer all reference requests to the named responders.

(7) When negotiating termination agreements, pay special attention to non-disclosure clauses. Do not agree to them if the law might require disclosure. Inform responders of such agreements.

(8) Always check references of prospective employees thoroughly to confirm qualifications, to screen out employees who have had serious problems elsewhere and to limit "negligent hire" claims.

Terminated employees engaged in discrimination litigation against their ex-employers have also prevailed in retaliation cases under federal and state discrimination laws when they have been given negative references, claiming those references were given to punish them for filing the discrimination claims.

#### *Negligent Misrepresentation*

Based on these cases, employers might well think that their best approach to reference requests would be to enforce a blanket rule to never respond to any reference request, regardless of whether or not they have entered into a non-disclosure agreement with the ex-employee. But this strategy could well come back to haunt an employer. In fact, outside parties who have no relation whatsoever to the company that has fired an employee have recently been successful in suing the terminating company because of an inaccurate positive reference it gave about an employee it fired. In one case, a vice principal of a middle school was hired based on positive references given by schools that had previously employed him. At all three schools, he had been accused of sexual improprieties with students; at two of them he had been pressured to resign. A student at the vice principal's new employer was allowed to sue one of his *previous* schools for making negligent and fraudulent misrepresentations to *her* school by recommending this alleged sexual predator for hire.

#### *State Immunity Laws*

In response to the increase in successful cases concerning references and to encourage ex-employers to provide recommendations about ex-employees, more than 30 states have enacted legislation that gives employers immunity in certain circumstances when they give references. These statutes differ widely and must be analyzed with care. The Arizona statute, for example, provides immunity for references given in good faith. The state presumes the former employer has acted in good faith in providing a reference if it employs fewer than 100 employees. For larger employers, good faith is presumed if the employer has a regular practice to provide references. The presumption may be overcome upon a showing of malice, recklessness or intent to mislead. California's statute provides immunity only if the reference is *requested* (and not *offered* by the employer), the facts given relate to job performance or qualifications, there is "credible" evidence to support the facts, and the reference was not given maliciously.

## Testing for Illegal Substance Use

The sale and use of illegal substances continue to plague the United States. Given that over 70 percent of substance abusers are gainfully employed, every employer of some size is bound to encounter the problem of illegal drug use.

Employers may want to consider testing job applicants and current employees for evidence of illegal substance usage. An American Management Association (AMA) survey published in 2004 indicates that drug testing is performed by nearly 62 percent of the United States companies sampled. Fifty-five percent test new hires and 44 percent test current employees. The law in this area is somewhat contradictory. Federal law requires testing of those employed by some government

contractors. Transportation and nuclear power plant employees must be tested under circumstances detailed in Department of Transportation regulations. Whether and when other employees may be tested is a matter of continually developing federal and state law.

State laws differ widely in their restrictions on testing. Generally, the laws are more lenient in allowing testing of job applicants than of current employees. Most states also regulate whether testing may be done on a random basis, in circumstances when there is a suspicion of drug abuse, or after an accident. They also regulate the circumstances under which an employee who fails a test may be terminated.

**Seven Steps to a Successful Drug Testing Policy**

Employers considering whether to test for illegal substances should first determine whether testing is required or prohibited by law. Next, answer this question: Is testing appropriate for this workplace or for particular job categories here? If it is, the following seven steps should be taken.

(1) Review all applicable legal requirements with counsel and bargain with unions if the current workforce is unionized. Employers are not required to bargain with unions about testing applicants for jobs covered by union contracts.

(2) Determine under what circumstances testing will be performed, who will be tested and how often, what drugs will be tested for, what type of test will be performed and by what independent laboratory.

(3) Describe notice, consent and release procedures.

(4) Always confirm positive tests by a second, highly reliable test.

(5) Describe the actions to be taken if a test is positive (as well as what constitutes a positive test). Will substance abuse treatment be provided? Will it be required?

(6) Inform all employees and applicants of the policy.

(7) Establish confidentiality rules to protect employees' and applicants' privacy during the process.

## Genetic Testing

Genetic testing by employers is a controversial practice that may well engender federal legislation in 2006. The 2004 AMA survey indicates that approximately 15 percent of those surveyed now conduct some type of genetic testing. To test, the employer's testing personnel takes a sample of blood, other bodily fluid, or tissue from the employee or applicant in order to screen for inherited diseases or susceptibility to certain diseases. For example, employers screen applicants for the multitude of diseases caused by a genetic defect, such as Tay Sachs disease, Huntington's disease, hemophilia or cystic fibrosis, or for genetic variations that might make someone more susceptible to an occupational disease.

The test can also be used to monitor genetic damage over time – damage that might be caused by exposure to hazardous workplace conditions. For example, some employers monitor current employees to determine whether their exposure to potential cancer-causing agents in the workplace has caused genetic mutations. Typically this testing is done at the request of employees or their unions – although it is arguable that this type of monitoring is required under OSHA rules in workplaces where conditions might expose employees to genetic damage.

Nonetheless, many people are concerned that testing results will be used to deny employment to people who are fully able to perform job functions or who may have susceptibility but do not actually have – and may never have – the genetic disease to which they are susceptible.

Moreover, such results could be used to discriminate against those in legally protected classes – that is, those more prone to a particular genetic trait than others because of their race or national origin. Caucasians are more likely to inherit cystic fibrosis, for example; Ashkenazi Jews are more likely to inherit Tay Sachs; and those of African origin are more likely to inherit the sickle-cell trait. For these reasons, the states have begun to regulate genetic testing – a trend that will continue in 2006. Currently, more than 30 states have statutes confronting this issue in different ways. In some, such as Massachusetts, genetic testing of job applicants is banned, and it cannot be performed on current employees without their consent. Furthermore, results of these tests may only be used to counsel employees; no adverse action may be taken against an employee based on test results. Other states are less strict. In New York, for example, testing may be performed without consent if the occupational environment could cause an increased risk of genetic disease.

Congress is considering legislation to regulate genetic testing by employers. In its present form, the legislation would prohibit employers from using genetic information to discriminate against applicants and employees and from requesting genetic information unless it is used to monitor the biological effects of toxic substances in the workplace.

## Monitoring Computer Usage, E-mail and Instant Messaging

It takes only a cursory review of electronic communications use in the workplace to conclude that technology developments have far surpassed employers' abilities to manage their misuse by workers. Not only do studies establish that employees are spending what could be productive work time chatting on the computer or surfing the Internet (one study estimates that 70 percent of the visits to pornography sites are initiated from the workplace), but confidential information is leaking outside of corporations through such use. Computer misuse has led to countless lawsuits by employees claiming sexual harassment and discrimination of all types.

**Seven Steps to a Successful Electronic Monitoring Policy**

(1) Perform audits of all aspects of computer use in the workplace.

(2) Create, implement and distribute written policies to manage such communications. Such policies should include provisions on permissible uses, a clear statement that personal e-mails and IMs are not private and that the employer may review these communications and all other aspects of an employee's computer usage at any time.

(3) Train employees about these procedures.

(4) Use software designed to secure the computer system.

(5) Develop a procedure to monitor Internet use, e-mail and IM.

(6) Control inappropriate incoming and outgoing communications.

(7) Develop a policy to save information when required and to purge other information on a regular basis.

Furthermore, thoughtlessly sent e-mails and instant messages (IMs) are used more and more as material evidence in claims brought under securities and other laws. Finally, many employees have the view (almost always mistaken) that their "personal" e-mails and IMs at work are private. It is not recommended that personal e-mail, IM and

Internet use be prohibited. (Experience indicates that this prohibition is akin to prohibiting employees from breathing.) Nonetheless, computer use can be controlled, certain Internet sites can be placed out of bounds, and random monitoring can establish whether computer misuse is undermining business goals.

A Neilson Internet usage study recently found that the average workplace computer user spends almost seven hours (one full workday) on the Internet each week. E-bay, Charles Schwab, E-trade and Fidelity all made the list of the 10 most popular websites in this study. A recent AMA survey also highlights the problem. Almost 90 percent of the employees surveyed in 2004 engaged in personal e-mail correspondence at work. The majority also uses IM for personal use. Most of the organizations surveyed do not use IM software technology at all to monitor, purge, retain or archive IM – even though employee IMs regularly contain sexual content, disparaging remarks and confidential information. While almost 80 percent of the employers surveyed have a written e-mail policy, only 20 percent have a policy on IMs. Most employers do not monitor internal e-mail or internal IMs at all and 40 percent do not monitor external e-mail. Employers are woefully lax in retaining and deleting e-mail and IM properly and are wholly unprepared for the huge litigation risks e-mail presents. In fact, barely half of the companies surveyed conduct any e-mail policy training at all.

The serious problems caused by this lack of management and training are exemplified by several cases. As one *Wall Street Journal* reporter has noted, New York Attorney General Eliot Spitzer "has built an awe-inspiring career on indiscreet e-mail." The writer cites an e-mail sent by a Merrill Lynch executive calling a technology stock he was urging the public to buy a "POS" (an acronym for a very derogatory phrase). Similarly, in a Citigroup stock analyst's e-mail Spitzer obtained, the analyst admitted that he upgraded his rating of AT&T stock because he wanted Citigroup's CEO to help him get his children into a selective preschool in New York City. The reporter also mentions the famous Wyeth Pharmaceutical e-mail used by plaintiffs in the successful Phen-Phen litigation in which a Wyeth executive makes fun of "fat people who are a little afraid of some silly lung problem." The 2005 firing of Boeing's chief executive is also instructive. He was actually fired for violating the company's fraternization policy, but his affair with an employee was discovered when another employee intercepted a graphic e-mail to his paramour.

## 'Personal Privacy' Issues

Given recent trends, 2006 is expected to bring increased litigation and legislation about the extent to which employers may manage and control employees' "personal" conduct as well as their activities outside of work. Three areas require special attention:

- romantic relationships;
- physical appearance; and
- English-only rules.

### *Romantic Relationships*

Romantic relationships that seep into the workplace causing legal issues are virtually ubiquitous. They will continue as long as human sexual attraction continues; a review of recent litigation suggests that human sexual attraction is not on the wane.

Countless workers meet their future spouses at work – a recent study indicates that 44 percent of coworkers who date marry each other. Many others, however, begin relationships at work that lead to the courthouse, not the altar. The legal consequences of these failed relationships are endless: Employees sue their employers and their supervisors when a relationship ends over changes in work conditions, poor evaluations, demotions, salary decreases and termination; employees make claims of harassment after a breakup; employees who are not dating a supervisor sue when supervisors favor the employees they are dating; and on and on.

A few states (New York and California, for example) limit an employer's right to control employees' lawful romantic relationships with their coworkers. But "non-fraternization" policies prohibiting romantic relationships between direct supervisors and their supervisees are allowed in every state. Prudent employers not only adopt them, but also train supervisors about the grave consequences of dating people they supervise. On countless occasions, one serious error in judgment by a supervisor has dismantled a career. Regardless of the dire consequences of this conduct, however, a 2003 AMA survey on workplace dating found that only 12 percent of the employers surveyed had non-fraternization policies. Rampant litigation in this area makes it mandatory that every employer:

- examine its workplace to determine what potential litigation may be lurking there;
- adopt a rational (and legally sound) policy;
- enforce real, consistent penalties for violations, and
- train the workforce on the law and the employer's policy.

#### Sexual Harassment Investigations Raise Privacy Issues

Sexual harassment investigations also raise privacy issues for both accusers and those accused. The EEOC and many states require that employers provide accusers with assurances of confidentiality "to the extent possible" unless to do so would impede an investigation. Certainly, there are many occasions during sexual harassment investigations when the accuser's name and details about his or her allegations must be disclosed to the accused and to witnesses in order to flush out what actually occurred, but employers are counseled to disclose this information only on a "need to know" basis and to direct everyone interviewed not to disclose the information further.

No statutes protect the privacy of the accused in these investigations. And, while those accused have generally been unsuccessful in post-investigation lawsuits alleging such claims as defamation and invasion of privacy, it is prudent and judicious to take the same precautions to protect the confidentiality of the accused that are taken to protect the accuser. It is crucial, however, that no one involved in a harassment investigation be promised complete confidentiality under any circumstances. Confidentiality procedures should be incorporated into every employer's written sexual harassment investigation policy.

### *Physical Appearance*

Employer rules concerning employee physical appearance and attire at work will continue to precipitate legislation and litigation. A few states prohibit "gender-related" rules on employee appearance. In the vast majority of states where there is no legislation, employees file lawsuits regularly. In one federal court, a female employee sued the Harrah's casino for requiring her to wear makeup including face powder, blush and mascara ("in complimentary colors") as well as lip color, teased, curled or styled hair, stockings and nail polish as part of its "Image Transformation Program." The 9th U.S. Court of Appeals upheld the requirement in December 2004 but the case continues. The full court reheard the case but had not decided it as of October 2005. Employers are well advised to seek legal assistance before requiring employees to appear at work in "gender stereotypical" clothing, makeup or hairstyle.

Cases also abound involving weight discrimination, discrimination based on prohibitions on wearing religiously related attire and even cases over body art (tattoos and piercings). Again, only an employer that is knowledgeable about the "lifestyle" law in the states in which it operates can create a rational policy – and make rational hiring and firing decisions – in this realm.

### *English-only Rules*

Cases concerning English-only rules will only increase as the U.S. population and workforce become more culturally diverse and more workers are employed whose first language is not English. Not surprisingly, these employees want to speak their first language at work. However, their employers and coworkers may feel excluded from their conversations or have concerns about how non-English usage affects work performance and safety. The Equal Employment Opportunity Commission (EEOC) prohibits English-only rules, when applied at all times and places during work hours, and permits such rules only when they are justified by business necessity – for example, to communicate with English-speaking customers and supervisors or to permit a supervisor to monitor the employee's performance adequately. Absent the ability to show that workers have used language to exclude others in the workplace, that this exclusion has affected the business negatively, and that no another alternative exists to remedy the situation, English-only rules are not otherwise allowed.

Some states, such as California and Illinois, have their own legislation prohibiting English-only rules except when employees are performing direct work duties. Several courts have allowed broader English-only rules, permitting employers to apply such rules at any time during work hours. For example, a federal court in Kansas has accepted as non-discriminatory an employer's requirement that English be spoken at all times during working hours, except during lunch and rest periods.

The English-only issue continues to be in flux. Employers should seek and follow legal advice before implementing an English-only rule that they cannot establish is required by the legitimate needs of the business.

## Video and Audio Monitoring

A 2005 AMA survey shows that over one half of the 526 respondents now conduct video surveillance of employees and almost 20 percent record telephone calls of employees in selected job categories. Employers that do so must ensure that such monitoring complies with myriad legal requirements. Monitoring that does not comply can put employers at risk for both civil and criminal penalties.

Under the federal Electronic Communications Privacy Act (ECPA), employers may videotape employees under certain circumstances, but may not record oral communications except in very limited situations. Even the use of cameras that do not record sound is subject to limitations. In organizations with union workers, video monitoring is a mandatory subject for collective bargaining. Recording activity violates federal labor law when it is an attempt to coerce employees not to engage in organizing activities. In many states with privacy statutes or their own video surveillance laws (for example, Connecticut and California), video monitoring in private non-work areas, such as restrooms and locker rooms, is unlawful. Congress is considering legislation to prohibit employers from videotaping or audiotaping employees in restrooms, dressing rooms or other places in which it is reasonable to expect that employees will change their clothes. Many states also prohibit audio recording in any circumstance without the consent of both parties to the conversation (Massachusetts, for example).

The ECPA prohibits audio recording or listening without the prior consent of at least one party to the conversation or when done by a subscriber to a telephone system in the ordinary course of business. The latter means that if an employer is monitoring in the ordinary course of business and learns that the employee's call is a personal one, the monitoring must stop. There is some confusion about whether the statute allows employers to access voicemail information in their systems. Employers should obtain the advice of legal counsel as to how the ECPA has been interpreted in their jurisdiction.

## Record Retention and Disposal

Employers must take special care to protect the confidentiality of records relating to their employees. This is especially true for records containing medical information because of HIPAA requirements (see Chapter 18). Numerous laws, both federal and state, contain employee record retention requirements and even requirements as to how and when these records may be disposed of. The laws change and expand (seeming never to contract) regularly. These laws include, but are not limited to, the federal Age Discrimination in Employment Act, Title VII of the Civil Rights Act, OSHA, ERISA, the Fair Labor Standards Act and federal immigration laws. The Federal Fair Credit Reporting Act (FCRA) is just one example. The statute regulates how employers do background checks using an outside service. The statute requires notice to the employee or applicant and written authorization as well as certain disclosures about such background checks when an adverse employment decision is (or may be) made based on the information received. As of June 1, 2005, if an employer disposes of any of the information obtained in the background check it must take "reasonable" measures to protect against unauthorized access, such as burning or shredding or permanently destroying information stored in a computer.

**Six Steps to a Successful Records Handling Policy**

(1) Conduct regular audits of recordkeeping procedures (including electronic communications).

(2) Adopt and implement a retention schedule taking into account applicable federal and state law, as well as applicable statutes of limitations on claims.

(3) Make duplicates of records, when prudent.

(4) Adopt and implement a policy consistent with state and federal laws that allows employees access to their personnel records. The policy should include provisions on how employees may request records, how often records may be requested, how quickly requests will be responded to, which records will be made available, whether the employee may make an explanatory statement for the file when he or she does not agree with statements in the records, and a copying process and payment requirements for copying.

(5) Adopt and implement hard copy disposal and e-mail and IM purge policies consistent with applicable law, ensuring that confidential records are burned, shredded or otherwise destroyed permanently.

(6) Regularly update record-handling policy as legal requirements change. The Office of the Federal Register publishes a list of all regulations requiring record retention and disposal. This list should be consulted regularly.

## Conclusion

Our nation's privacy laws are complex, constantly evolving, and sometimes even contradictory. Prudent employers will not ignore them, but rather will adapt to them with care, implementing policies and procedures to manage privacy issues day-to-day and modifying those practices as legal changes inevitably occur.

**Resources**

For a detailed discussion of workplace privacy issues, see *Workplace Privacy: Real Answers & Practical Solutions*, published by Thompson Publishing Group. Go to www.thompson.com.



*Excerpted from* Human Resources 2006: Answers to Your Top 25 Questions, *available from Thompson Publishing Group. For more information or to order this 250-page book, call 800-677-3789 or go to http://www.thompson.com and click on "Employment Law."*