PRIVACY IN THE WORKPLACE
February 12, 2002

There has always been tension between a company's need and right to obtain information about prospective and existing employees and the concern for individual privacy. Employers understandably want to know whether applicants are qualified and suitable for employment, and whether the performance of existing employees meets applicable standards. In addition, employers want to ensure that employees comply with company rules in order to limit their exposure to lawsuits by employees and third parties.

There are many methods by which employers may investigate, test, and monitor applicants and employees. However, individuals do not give up their right to privacy by applying for or accepting employment. Both state and federal laws place limits on an employer's ability to gather and use information about prospective and existing employees. Employers seeking to monitor employee conduct must be careful not to run afoul of an increasing array of prohibitions.

Employer Control of Employee Relationships

Employment of Relatives

It is not uncommon for problems to arise when familial relationships exist between employees, especially when the employees are in a direct reporting relationship. For many employers, the first line of defense is prohibiting the employment of spouses or relatives. The fears typically associated with the employment of relatives are claims of preferential treatment, retaliation, scheduling conflicts, decreased productivity, disclosure of confidential information (e.g., when one employee has access and the other does not), and general disruption resulting from bringing personal problems to work. No-spouse rules are impermissible by statute in some states, including Oregon (which prohibits policies barring the employment of relatives generally, except in limited circumstances)\(^2\). In addition, no-spouse rules may be challenged as discriminating on the basis of marital status, or as having a disparate impact on women\(^3\). In the public sector, no-spouse rules have been challenged as impermissibly burdening an employee's right to marry.\(^4\)

Public Employees

Public employees enjoy additional Constitutional protections, including the limited right to be protected from inquiries relating to personal and family relationships. Public employees' rights are subject to a balancing of the government's interest in the inquiry and in the regulation of the employee's conduct\(^5\). Generally, questions relating to off-duty sexual activities or sexual relationships are likely to be protected\(^6\). Inquiries into personal, family, and sexual relationships must be justified by the legitimate interests of the employer and tailored narrowly to meet those legitimate interests.\(^7\)
Romantic Relationships Between Co-Workers

With the ever increasing amount of time many people spend at work, it is hardly surprising that many romances begin in the office. Employers have legitimate concerns about romantic relationships between co-workers, particularly those between supervisors and subordinates, because of the substantial risk of liability and office disruption that often result. Employers who are aware of but do nothing about workplace romances face potential claims for sexual harassment and negligent retention, among other things, if the romance turns sour. In addition, it is not unusual for employees aware of a relationship between co-workers to complain about a hostile environment and/or preferential treatment. On the other hand, employers who intrude into their employees' private lives may find themselves subject to claims such as invasion of privacy.

Another problem with office romances is that they may result in domestic violence that spills over to the workplace. Domestic violence is a leading cause of workplace deaths for women.8 Employers who are aware of a potential for violence and who fail to address it may be liable to their employees and third parties for the harm suffered.9 Given the inevitability of office romances, and the substantial risks engendered by them, employers need to formulate an approach to properly manage these relationships. In the last few years, a growing number of employers have adopted express written policies concerning office romance, especially between supervisors and their subordinates. On the extreme side, some employers even utilize "love contracts" and "date-and-tell policies" to manage workplace relationships.

Policies Prohibiting Fraternization

Some employers have reacted to the fear of lawsuits by enacting policies prohibiting any fraternization or dating between co-workers, or limiting such relationships to employees who are not in the same chain of command. In the event of a violation, such policies may provide for the termination of both employees, the termination of the less senior employee, or a decision between the employees as to which one will resign (failing which, the employer may fire one or both). While facially neutral, rules that require the discharge of the less senior employee may have a disparate impact on women (due to the "glass ceiling" effect or the less likely scenario of a male subordinate dating a female supervisor). No-fraternization policies typically prohibit employees from dating co-workers entirely, or prohibit dating relationships between supervisors and subordinates. This type of policy has been upheld in Oregon and many other states10. However, such policies force employers to more closely monitor the existence of workplace relationships. The failure to do so may result in unequal application of the policy (whether real or perceived) and lead to claims of discrimination.11 On the other hand, monitoring employees' behavior may give rise to claims for invasion of privacy, particularly if the employer's means of monitoring employees is intrusive.12
"Date-and-Tell" Policies and "Love Contracts"

A date-and-tell policy allows a company to enforce a notice requirement (the "tell") rather than impose discipline based on the existence of the dating relationship. Notice to the company may be required in all circumstances, or required only if the employees are in a supervisory-subordinate work relationship. Aside from the obvious intrusion into employees' privacy, one ACLU representative has expressed concern that date-and-tell policies may force gay and lesbian employees out of the closet, or compel workers to admit to extramarital affairs to keep their jobs.\textsuperscript{13}

A "love contract" is basically an informed consent agreement under which co-workers acknowledge that their relationship is consensual and not in violation of the employer's anti-harassment policy (which both parties are typically asked to (re)read). Such agreements may also include an acknowledgment that either party may end the relationship without adversely affecting their employment, an agreement to use the employer's complaint procedure if job-related problems arise, and an agreed upon mechanism for resolving any related disputes. Love contracts are particularly useful when a supervisor is involved in a relationship with a subordinate in the chain of command, whether or not the other person is a direct or indirect report.

It is unclear whether the risks and burdens of imposing love contracts and date-and-tell policies outweigh the benefits. Love contracts may not be enforceable; as of yet, they do not appear to have been tested in any court. While love contracts and date-and-tell policies allow employers to reinforce their anti-harassment policies and procedures with the employees most likely to be affected, they also implicate privacy concerns that are likely to be met with resistance by employees who are offended by the intrusion such policies require. Moreover, conditioning an employee's continued employment on compliance with such policies may result in discrimination claims if the policies are not consistently enforced.

Ultimately, employers who wish to address workplace romances in a formal way will want to have a clear written policy on the subject, promulgated as an integral part of a sexual harassment policy. Employers who do not wish to ban workplace relationships altogether can discourage, without absolutely prohibiting, interoffice romances between supervisors and employees, and encourage timely and confidential disclosure of the existence of a relationship to management so that steps may be taken to minimize the impact on the workplace (\textit{e.g.}, changing any direct reporting relationship).

Monitoring Romantic Relationships Between Employees and Non-Employees

Employers may have legitimate concerns about employees leaking confidential information to someone with whom they have a romantic relationship (\textit{e.g.}, where one employee has access to confidential information or where the employee's spouse or partner works for a competitor). Conflict of interest policies and confidentiality agreements may afford employers some measure of protection, but
they will not eliminate the risk that confidential information will be shared with the outsider.

Firing an employee for simply dating a non-employee is risky. For example, in *Rulon-Miller v. International Business Machines*, 208 Cal. Rptr. 524 (Ct. App. 1984), an employee who was fired for dating the employee of a competitor prevailed against the employer on claims for wrongful discharge (based on the implied covenant of good faith and fair dealing) and intentional infliction of emotional distress. The fact that the employer had a written policy promising to protect its employees' right to privacy clearly affected the outcome in the case.14

**Surveillance of Employees**

According to one recent survey, about 78% of companies in the U.S. monitor their employees in some way. Employee Internet use is monitored by 63% of employers; 47% store and review employee e-mail messages; 15% view employees by video; 12% review and record phone messages; and 8% review voice-mail messages.15

- On February 7, 2002, *The Oregonian* reported that Tofle USA in Tualatin fired a production manager who installed a video camera in a women's restroom. The camera was hooked up to his computer. Another employee contacted the police after seeing her picture on his computer. This is a good example of what employers should not do.16
- In another ongoing case, close to 300 workers represented by their union are proceeding with invasion of privacy and intentional infliction of emotional distress claims against Consolidated Freightways. The company monitored employees via two-way mirrors in the company's restrooms in an effort to catch drivers using illegal drugs.17

Videotaping or otherwise conducting surveillance on employees, whether at work or off the job, raises significant privacy issues. The extent to which employers may be liable for surveillance depends on the employees' reasonable expectation of privacy and the nature of the intrusion.18 For example, in one case, an employer conducted surveillance on an employee who had made a workers' compensation claim. Private investigators were hired to videotape the employee, who was filmed engaging in activities outside his home. The employee brought an action for invasion of privacy and trespass. Finding in favor of the employer, the court noted that "if the surveillance is conducted in an unreasonable and obtrusive manner the defendant will be liable for invasion of privacy."19

**Limitations on Surveillance by Public Employers**

The Fourth and Fourteenth Amendments to the U.S. Constitution provide additional protections to public sector employees. The Fourth Amendment protects against unreasonable search and seizure by government agents. The Fourteenth Amendment extends the privacy rights of the Fourth Amendment to
state and local governments. Public sector employers nevertheless have fairly wide latitude in conducting surveillance. For example, in *Vega-Rodriguez v. Puerto Rico Telephone Co.*, 110 F.3d 174 (1st Cir. 1997), the court held that quasi-public employees did not have a cause of action for the employer's continuous video surveillance of their workplace. The employees lacked a reasonable expectation of privacy while working in an open and undifferentiated work area and, therefore, the Fourth Amendment was not implicated: The bottom line is that since . . . [the employer] could assign humans to monitor the work station continuously without constitutional insult, it could choose instead to carry out that lawful task by means of unconcealed video cameras not equipped with microphones, which record only what the human eye could observe.

**Monitoring E-Mail and Voicemail**

Employers may routinely monitor e-mail and voicemail communications for quality control purposes, or find it necessary to do so when employee misconduct is suspected. The New York Times discharged 23 employees in 1999 for disseminating sexually explicit pictures through e-mail at work. More recently, Xerox Corporation discharged 40 employees for misusing company resources by spending excessive time viewing non-work related web sites, including sexually oriented cites. Dow Chemical Company also discharged 50 workers and suspended 200 others for handling pornographic or violent e-mail. In fact, one judge recently stated that "*** abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible." Needless to say, an employee who has not consented to or been notified of such practices may be motivated to cry foul if he or she discovers that the employer has accessed what was thought to be a private communication. Moreover, in some circumstances, monitoring of telephone calls, voicemail, e-mail and Internet access may be a crime. When conducted with care and forethought, however, monitoring can generally be undertaken without violating state or federal laws governing access to electronic communications.

In general, employers can reduce their risk of liability by distributing written policies notifying employees that voicemail, e-mail and other electronic communication devices are the property of the employer and intended for business use. Employees should also be expressly informed that they have no legitimate expectation of privacy in such communications and that their voicemail, e-mail and Internet use may be monitored and reviewed. When addressing e-mail, employers need to think about other related issues, such as the appropriate storage and deletion of e-mail and ensuring that e-mail complies with the employer's policies applicable to harassment, discrimination, and confidentiality, among other things. An electronic systems policy should prohibit the use of threatening, harassing, or discriminatory content in electronic communications.
The Right to Associate

The federal Americans with Disabilities Act (ADA) and its state counterpart both prohibit discrimination in employment based on association with someone who is disabled. See 29 CFR § 1630.8; ORS 659A.112(2)(d). Thus, for example, an employer may not reject an applicant out of concern that the applicant will miss work to care for a spouse or child with a disabling illness. Oregon law also prohibits employers from discriminating against an individual because of the race, religion, color, sex, national origin, marital status or age of any other person with whom the individual associates. The Oregon law has been interpreted to preclude discrimination on the basis of sexual orientation.

Medical Information

ADA/FMLA

Both the ADA, the Family Medical Leave Act (FMLA), and corresponding state laws limit employers' ability to obtain medical information. Under the ADA and Oregon law, an employer may require a medical examination and/or inquiry about an employee's disability only when the inquiry is job related and consistent with business necessity. Medical examinations are also permissible (1) after an offer of employment has been made and prior to the commencement of the employment duties, if all entering employees are subjected to such an examination regardless of disability; and (2) as part of a voluntary health program available to employees at a worksite. Medical information and records obtained by employers must be collected and maintained on separate forms and in separate medical files and treated as a confidential medical record. Direct communication with an employee's health care provider is permissible with the employee's consent. Under the FMLA and Oregon law, employees requesting leave for a serious health condition may be required to provide a medical certification completed by their health care provider. If the employer has reason to doubt the validity of the employee's medical certification, the employer may require the employee to obtain a second opinion from a health care provider designated by the employer (when the first and second opinions differ, a third opinion may be required). However, the employer is not permitted to communicate directly with the employee's health care provider. Many state statutes also restrict the right of employers to copy medical records or disclose medical information concerning an employee to a third person. In addition to the risk of claims under the ADA, the FMLA, and similar state laws, employers who inappropriately disclose an employee's medical information to third parties may be subject to claims for intentional infliction of emotional distress and invasion of privacy. Notwithstanding the prohibitions on the disclosure of medical records, medical information may be shared with supervisors as needed to facilitate the accommodation of an employee's work restrictions or disability.
information may also be shared with first aid and safety personnel as needed for possible emergency evacuation and treatment. In addition, information may be released for purposes mandated by law, provided that the results of the examination are used only in accordance with the law.

**HIPAA**

The Health Insurance Portability and Accountability Act of 1996, or HIPAA, is a federal law addressing the privacy, security, and transmission of identifiable health information of an individual (called "protected health information" or "PHI"). While HIPAA applies primarily to designated covered entities "healthcare providers, health plans, and health care clearinghouses" certain provisions of the law extend to employers. Prior to HIPAA, state laws governed the privacy of a person's medical information. Accordingly, those protections varied from state to state. HIPAA establishes a national "floor" of minimum protections which must be afforded to PHI. State laws may impose stricter privacy and security protections, but may not provide less.

HIPAA restricts the disclosure of personal information related to an individual's health care or payments for health care. Covered information is personally identifiable: where the health care data can be linked to a person's name, social security number, employee number, or any other identifier, which includes any information created or received by a provider, health plan, insurer, or employer, that relates to past, present, or future health care or payments. There has been much confusion among employers as to how HIPAA affects their operations. HIPAA does not directly apply to employers who are not health care entities or insurers. However, HIPAA's definition of a group health plan includes most employee welfare benefits plans that are subject to ERISA, provided the plan has 50 or more participants or is administered by a third-party organization. Most employers who provide ERISA benefits to their employees will, therefore, need to adhere to HIPAA's requirements for all group health plans. The obligations are more rigorous if the employer plays an active role in the management of its health plan. Although the effective date for compliance with the privacy regulations is 2003 for most employers (small plans are granted an additional year), all affected employers should be thinking about compliance now.

Consider all of the situations in which employers maintain or have access to their employees' PHI: pre-employment screenings, fitness for duty examinations, workers' compensation claims, administration of health plans, claims for disability or sick leave, OSHA compliance, and family medical leave. Under HIPAA's privacy regulations, employers are not entitled to access or use PHI in making employment-related decisions unless the employee specifically authorizes its disclosure and use. The regulations list a number of requirements the group health plan must meet before it may release medical information to the employer (or other benefits plan sponsor, if different from the employer). Specifically, the health plan must ensure
that the plan document is amended to provide that the employer shall do all of the following:

- Only disclose medical information as permitted by the plan documents or as required by law;
- Not use or disclose the medical information for employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of the employer;
- Ensure adequate separation of records and employees is established and maintained between and the group health plan and the employer;
- Ensure that agents and sub-contractors of the employer agree to abide by the same restrictions and conditions as the employer in regard to the use of medical information received from the group health plan;
- Report any improper use or disclosure of any medical information to the group health plan;
- Allow individual employees to inspect and obtain copies of medical records about themselves, to the extent required by HIPAA;
- Allow individual employees to amend medical records about themselves, to the extent required by HIPAA;
- Provide individual employees with an accounting of disclosures of medical information made within the six years prior to the request for such accounting, to the extent required by HIPAA; and
- Make the employer's internal practices, books, and records relating to the use and disclosure of medical information available to HHS for purposes of auditing the group health plan's compliance with HIPAA.

It is important that employers who act as both the sponsor and administrator of their own group health plan understand their obligations under HIPAA. As HIPAA's privacy obligations for group health plans change with the level of medical information flowing between the group health plan and the employer, such employers will want to establish group health plan operating procedures and benefits plan document provisions specific to their unique arrangements. The civil penalties for violating HIPAA include $100 for each violation, up to a maximum of $25,000 for violating a particular requirement of the law. Criminal penalties range from $50,000 and one year in federal prison for wrongful disclosure, up to $250,000 and ten years in prison for a deliberate offense with intent to sell protected health information.45

HIPAA Compliance Questions for Employers

- Are medical records and physical examination results maintained in separate medical files" Is access to the files secure?
- Do you have a policy restricting access to employee records (employee, union, consent by employee, medical records)?
- Are those with access to medical records trained regarding confidentiality requirements, including requirements associated with last chance agreements and HIV records?
• **HIPAA:** Do the same people in the organization handle both employment and benefits-related data? Have you taken steps to ensure that no one in your organization is accessing health information acquired by your employee benefit plans for other purposes?
• **HIPAA:** Have you amended your plan documents to specify permissible uses and disclosures of health information to the employer/plan sponsor?
• **HIPAA:** Has staff been assigned to develop and implement HIPAA policies? Has a HIPAA Privacy Officer been designated?
• **HIPAA:** Have responsible employees been trained on appropriate uses and disclosures of protected health information?
• **HIPAA:** Have contracts with "business associates" with whom the organization shares protected health information (such as technology vendors, plan administrators, etc.) been redrafted to assure that they are in full compliance with HIPAA (HIPAA makes an employer liable for the violations of its business associates if the employer is aware of the associate's wrongful disclosures)?

**OSHA 300 Log - Privacy Concerns**

Non-exempt employers are required to record and report recordable work-related fatalities, injuries, and illnesses on the OSHA 300 Log (or OSHA 300-A, DCBS Form 801 or equivalent forms). However, in certain types of cases, such as those involving mental illness, sexual assault, and other cases in which the employee asks for his or her name to be kept off the list, employees' names should not be entered on the OSHA 300 Log. Instead, the employer is required to enter "privacy case" on the log and keep a separate, confidential list containing the identifying information. In addition, under OAR 437-001-700(14) Forms:

(j) If you voluntarily disclose the forms to persons other than government representatives, employees, former employees or authorized representatives, you must remove or hide the employees' names and other personally identifying information, except for the following cases:

- To an auditor or consultant hired by the employer to evaluate the safety and health program;
- To the extent necessary for processing a claim for workers' compensation or other insurance benefits; or
- To a public health authority or law enforcement agency for uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required under Department of Health and Human Services Standards for Privacy of Individually Identifiable Health Information, 45 CFR 164.512.

**Illegal Drug Use**
It is generally considered acceptable, and even desirable, to restrict by policy the use of illegal drugs by employees, particularly if the employer wishes to discipline or discharge employees who test positive or are convicted of a drug-related crime. A drug test is not considered a medical examination under the ADA, and illegal drug use is not a protected activity under the ADA or most state disability laws, including Oregon.\textsuperscript{49}

There are no cases interpreting the common law right to privacy in Oregon in the context of random drug testing. Cases from other states suggest that the employee's privacy rights must be balanced against the employer's legitimate interests in maintaining a drug-free work place to determine whether the intrusion on the employee's privacy was "highly offensive to a reasonable person."\textsuperscript{50} Public employers face additional restrictions on drug testing pursuant to the Fourth Amendment.\textsuperscript{51}

The implementation of an on-the-job drug testing program requires careful thought and planning. Drug testing can be performed pre-employment (generally after an offer of employment has been made but before the employee begins work); after a work-related accident, when there is reasonable suspicion that an employee is under the influence of drugs; or randomly (using some type of lottery system). Each type of testing has its own costs, benefits, drawbacks and legal risks (the discussion of which is beyond the scope of this memorandum). In general, an employer must consider such issues as what to do if an employee refuses to take the test, what steps will be taken following a positive test result (termination, post-identification drug monitoring, warnings, second chances, or treatment programs), modification of employment forms and applications to advise applicants of pre-employment testing, maintaining the confidentiality of medical records, protection of reformed drug addicts under the state and federal disability laws,\textsuperscript{52} and evaluation of the program to ensure it is meeting the employer's needs.

**Alcohol Testing**

Testing for alcohol is considered a medical examination under the ADA, and may be administered only when the employer has reasonable grounds to believe an employee is impaired at work.\textsuperscript{53} Under state law, employers may administer a breathalyzer or blood alcohol test only if the employee consents.\textsuperscript{54} If the employer has reasonable grounds to believe an employee is intoxicated, the employer may require, as a condition for continuation of employment, the administration of a blood alcohol test by a third party or a breathalyzer test.\textsuperscript{55}

**Genetic and Brain-wave Testing**

On February 8, 2000, President Clinton signed Executive Order 13145, prohibiting discrimination in federal employment based on genetic information. President Clinton stated:

[F]ear of misuse of private genetic information is already very widespread in this nation. Americans are genuinely worried that their genetic information will not be
kept secret, that this information will be used against them. As a result, they are reluctant to take advantage of new breakthroughs in genetic testing ****. If we do not protect the right to privacy, we may actually impede the reach of these breakthroughs in the lives of ordinary people, which would be a profound tragedy. The EEOC has also taken a stand against genetic screening. The EEOC began a case against Burlington Northern in February of 2001, when it filed a petition for preliminary injunctive relief in an Iowa federal district court. The EEOC claimed in its petition that the railroad had ordered employees to take blood tests to see if they carried a genetic trait called Chromosome 17 deletion (some studies suggest that a person with that trait is more likely to develop some forms of carpal tunnel syndrome) without their voluntary and informed consent. The testing resulted in the filing of six individual charges with the agency. Approximately 20 workers, all of whom filed injury claims based on carpal tunnel syndrome, were tested between March 2000 and February 2001.

The EEOC took the position that genetic testing is a medical examination, and that the employer's testing violated the ADA because it was not job-related and consistent with business necessity. Another separate action to challenge the testing on was filed on behalf of the Brotherhood of Maintenance of Way Employees. Three days after the suits were filed, the railroad issued a release announcing that it would no longer submit workers to genetic testing. In early March, the company mailed a letter to all employees apologizing for the company's failure to fully disclose and explain the testing to workers. Ultimately, the employer agreed to not require employees to submit blood for genetic testing, conduct genetic testing on blood already obtained, act on the results on genetic testing already performed, or retaliate against workers who opposed the testing. The EEOC also issued a letter of determination finding that the railroad violated ADA requirements relating to medical examinations and inquiries, violated confidentiality requirements by releasing test results, and wrongfully retaliated against workers who objected to the testing.

In Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260 (9th Cir. 1998), employees of Lawrence (a government-operated research institution) alleged that black and female employees were singled out for added nonconsensual testing, and therefore, defendants had selectively invaded the privacy of certain employees on the basis of race, sex, and pregnancy. The testing consisted of testing "their blood and urine for intimate medical conditions - namely, syphilis, sickle cell trait, and pregnancy." The employees alleged that this testing "violated Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act (ADA), and their right to privacy as guaranteed by both the United States and California Constitutions." The Ninth Circuit allowed the federal and state privacy claims and the Title VII claims to go forward, stating:

[Consent] to a general medical examination does not abolish one's privacy right not to be tested for intimate, personal matters concerning one's health-nor does consenting to giving blood or urine samples, or filling out a questionnaire. As we have made clear, revealing one's personal knowledge as to whether one has a particular medical condition has nothing to do with one's expectations about actually being tested for that condition.\textsuperscript{57}
In Oregon, employers may only conduct genetic testing of an employee or applicant with informed consent for the sole purpose of determining a *bona fide* occupational qualification. Employers are otherwise prohibited from directly or indirectly subjecting any employee or applicant to a genetic or brain-wave test. \(^{58}\) Oregon also has enacted a general genetic privacy act.\(^{59}\) One of the purposes of the Act is to "protect against discrimination by an insurer or employer based upon an individual's genetic characteristics." \(^{60}\) Failure to follow the informed consent, retention and disclosure requirements may result in a private or state civil action, as well as criminal penalties. \(^{61}\)

**Polygraph Testing**

The federal Polygraph Protection Act permits the use of lie detectors on employees only in connection with an ongoing investigation of theft, industrial espionage or similar actions. The Act expressly forbids asking the employee questions regarding religion, race, politics, sexual behavior, or labor organizations. \(^{62}\) Oregon employers may not subject any employee or applicant to a polygraph or "psychological stress test," even if he or she consents. \(^{63}\)

**Off-Duty Tobacco Use**

Under Oregon law, it is an unlawful employment practice to require that an employee refrain from using lawful tobacco products during non-working hours. The statute permits such a restriction when it is a *bona fide* occupational requirement or when a collective bargaining agreement contains such a restriction. \(^{64}\)

**Religion**

Both federal and state laws prohibit employers from discriminating on the basis of an employee's religion. \(^{65}\) In addition, Oregon law prohibits discrimination against those with degrees in theology and those seeking religious occupations (i.e., with respect to the provision of existing tuition reimbursement or equivalent programs). \(^{66}\) Religious discrimination occurs when religion is made a term or condition of employment, when conduct of a religious nature creates a hostile or offensive working environment, or when employment terms or conditions infringe on an employee's religious beliefs or practices. \(^{67}\) Consequently, employers should not inquire about an employee's religious beliefs or availability for work (other than availability consistent with the position sought), except as necessary in connection with a religious accommodation. \(^{68}\)

**Bad Credit, Criminal Conduct**

The Fair Credit Reporting Act (FCRA) \(^{69}\) regulates an employer's ability to conduct and use credit or criminal background checks in evaluating current or prospective employees. Employers must obtain written permission from the
applicant or employee to obtain criminal background information or a consumer credit report, and must provide notice of certain rights they have under the Act (for example, the employee has the right to obtain a copy of the report and challenge its contents). The employer must also notify the employee if it uses the results of the report in refusing to hire, promote or retain the employee. Some states also impose requirements on the use of credit reports for employment purposes.70

Some state laws also require employers to notify applicants if they intend to conduct a criminal records check, and provide certain disclosures regarding the employee's rights under Title VII.71 Other states limit the time period for consideration of criminal conviction records, in other words, the employer should not access convictions older than seven years (Washington) or 10 years (District of Columbia) or 15 years (Massachusetts). Due to the wide variance in statutory regulation of criminal records from state to state, employers must check their local laws before conducting criminal background checks.

It may be a violation of Title VII of the Civil Rights Act to use arrest, as opposed to conviction records, in connection with hiring and termination decisions. As minorities are arrested in numbers disproportionate to their representation in the population, the effect of using arrest records is to exclude a disproportionate number of minorities from employment. Some state laws also limit the circumstances under which arrest records may be considered.72 However, in some states, employers may lawfully consider arrest records if there is a sufficient relationship between the arrest and successful job performance (e.g., where it appears that the employee or applicant engaged in conduct which led to an arrest, and the conduct is job-related and relatively recent).73

**Other Off Duty Conduct**

There are a number of reasons why employers want to use their employee's off-duty conduct in taking personnel actions, such as increased health insurance costs due to smoking or other high risk activities, conflicts of interest (moonlighting), decreased productivity (drug or alcohol use), or moral concerns (upholding community standards as a means of projecting a corporate image). Employee challenges to an employer's right to consider off-duty conduct are generally based on statutory restrictions or invasion of privacy claims.

Whether an employer should take adverse action against employees based on off-duty conduct, criminal or not, depends on the existence of any express prohibitions on consideration of the conduct. Assuming no such prohibitions exist, the employer should consider the severity of the misconduct and its relationship to the job. For example, an employee who works with cash should be treated differently if he or she is convicted of drunk driving, as compared to being convicted of theft or embezzlement.

To prevail in a claim for invasion of privacy, the employee must show that: (1) the employer intentionally intruded (2) upon the employee's private affairs or concerns, and (3) the intrusion would be highly offensive to a reasonable person.74
Social Security Number Confidentiality

Identity theft is a hot topic, and social security numbers are a key target in cases of identity theft. Employers should be aware of privacy concerns connected to social security numbers, as government restrictions on their use appear likely to increase. Currently, Section 7 of the Federal Privacy Act of 1974 provides that any government agency requesting an individual to disclose her social security number must inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it. California recently enacted a law that prohibits any person or entity, not including a state or local agency from using an individual's social security number in certain ways, including posting it publicly or requiring it for access to products or services.

Appendix

Electronic Communications Privacy Act (Federal Law)

Title I of the ECPA, 18 USC §§ 2510-2522, prohibits interception of "electronic communications," defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce." Id. § 2510(12). Title II of the ECPA, 18 USC §§ 2701-2711, prohibits access and disclosure of electronic communications. Titles I and II prohibit different behavior in that Title I concerns "interception" of communications in transmission, whereas Title II concerns "access" and "disclosure" of stored electronic communications. See U.S. v. Moriarty, 962 F. Supp. 217, 221 (D. Mass. 1997) (stating that interception requires intercepting or accessing "while in transmission"); Bohach v. City of Reno, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) (explaining that statutes distinguish between "interception" of electronic communication at the time of transmission as opposed to retrieval of communication after it has been put into "electronic storage"). Title I of the ECPA proscribes the interception of electronic communications. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 USC § 2510(4). The ECPA prohibits anyone from intentionally intercepting any electronic communication, or disclosing or using an electronic communication if he or she knows that such communication was obtained through unlawful interception. See 18 USC § 2511(1)(a),(c),(d). Section 2511(1)(b) also prohibits interception of any oral communication unless the person intercepting the communication is a party to it. See id. § 2511(2)(d). However, there are several relevant exceptions to this broad prohibition. First, because "electronic communication" includes only a communication that "affects interstate or foreign commerce," intra-office e-mail is not be covered by the ECPA. Second, the provider of the electronic communication service, or the
provider of the facilities used in the transmission of such communication, may intercept, disclose, or use that communication if such activity is conducted during the normal course of the individual's employment, and is necessary to the service or to the protection of the rights or property of the provider of that service (known as the "business use exception"). See id. § 2511(2)(a)(i). Third, the prohibition does not apply where one of the parties to the communication has given prior consent to such interception. See id. § 2511(2)(d). Fourth, it shall not be unlawful for anyone to intercept or access electronic communications made on a system that makes the communication "readily accessible to the general public." Id. § 2511(2)(g). Under these exceptions, an employer may lawfully intercept and access electronic communications in transmission.

Violators of the ECPA may be fined or imprisoned for up to five years. See id. § 2511(4)(a). Violators may also be liable for civil damages and attorney fees. See id. § 2520.

1. Access. Title II of the ECPA prohibits anyone from "intentionally access[ing] without authorization a facility through which electronic communication service is provided." 18 USC § 2701(a). However, this prohibition does not apply to conduct authorized "by the person or entity providing a wire or electronic communications service." 18 USC § 2701(c)(1); See also Bohach, 932 F. Supp. at 1236 (construing § 2701(c)(1) as allowing service providers to do as they wish when accessing communications in electronic storage). In addition, as stated above, the ECPA does not apply to electronic communications that do not affect interstate commerce. Therefore, if the e-mail is purely intra-office, or if the employer provides the e-mail service, the employer may lawfully access the contents of any e-mail. The exception probably does not apply, however, if the employer uses an outside e-mail or voicemail service.

Violators of the prohibition against accessing e-mail or voicemail may be fined or imprisoned for up to six months, unless such violation is malicious or for commercial profit, in which case the sentence may be one year for the first offense and two years for the second offense. See 18 USC § 2701(b). Violators may also be liable for civil damages and attorney fees. See id. § 2707.

2. Disclosure. Title II also prohibits any person or entity that provides an electronic communications service to the public from knowingly divulging to any person or entity the contents of a communication while in electronic storage by that service. See id. § 2702(a). A person or entity may, however, divulge the contents of a communication to the intended recipient of such communication, or as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service. See id. § 2702(b)(1), (5). In addition, all the exceptions from Title I, partially listed above, also apply to this prohibition. See id. § 2702(b)(2). Because this prohibition concerns providers of e-mail services to the public, an employer-provided e-mail service is not likely covered. Moreover, an employer that satisfies any of the exceptions under Title I will avoid liability for disclosure under Title II.

Recent Cases Under the ECPA:
Fraser v. Nationwide Mutual Insurance Co., 135 F. Supp.2d 623 (ED Pa 2001) (Employer, whose policy stated it could monitor its e-mail system, did not violate ECPA when it viewed archived e-mails of sales agent. Employer searched e-mail after the employee stated that he had organized a group of sales agents who would go to a competitor unless it made certain concessions).

Konop v. Hawaiian Airlines, 236 F.3d 1035 (9th Cir. 2001), withdrawn (9th Cir., August 28, 2001) (employee owned secured web site where he posted messages critical of his employer. His employer improperly gained access to the password-protected web site. The court held that the employer violated the ECPA).

ORS 165.540 (Oregon Law)

Oregon prohibits the following activities with respect to "telecommunications," which broadly includes "the transmission of writing, signs, signals, pictures and sounds of all kinds by aid of wire, cable or other similar connection":

[N]o person shall:
Obtain or attempt to obtain the whole or any part of a telecommunication *** to which such person is not a participant, by means of any device, contrivance, machine or apparatus *** unless consent is given by at least one participant.

(d) Obtain the whole or any part of a conversation or telecommunication from any person, while knowing or having good reason to believe that such conversation, telecommunication or radio communication was initially obtained in a manner prohibited by this section.

(e) Use or attempt to use, or divulge to others any conversation, telecommunication or radio communication obtained by any means prohibited by this section.

ORS 165.540(1)(a), (c), (e). A violation of any of these provisions constitutes a Class A misdemeanor. See ORS 165.540(9).

The Oregon statute differs from the ECPA in at least the following respects: (1) the prohibitions in ORS 165.540 apply to intra-office e-mail, as well as interstate e-mail; (2) the Oregon statute does not provide as broad exceptions to the interception, access, or disclosure of the contents of e-mail, such as the federal exceptions for legitimate business use and the access by the provider of the e-mail service; and (3) the Oregon statute does not provide any private right of action for civil damages. As a general rule, under the Oregon statute, the employer may intercept, access, or disclose e-mail and voicemail communications only if the employee has consented to such action. No court has interpreted ORS 165.540 with respect to the interception, access, or disclosure of e-mail or voicemail.

1 This memorandum contains a summary of information obtained from laws, regulations, court cases, administrative rulings and legal publications, and should not be viewed or relied upon as legal advice. Ater Wynne LLP urges readers of
this memorandum to consult legal counsel regarding specific legal issues and factual circumstances.

2 See ORS 659A.309 [formerly ORS 659.340].

(1) Except as provided in subsection (2) of this section, it is an unlawful employment practice for an employer solely because another member of an individual's family works or has worked for that employer to:

   (a) Refuse to hire or employ an individual;

   (b) Bar or discharge from employment an individual; or

   (c) Discriminate against an individual in compensation or in terms, conditions or privileges of employment.

(2) An employer is not required to hire or employ and is not prohibited from barring or discharging an individual if such action:

   (a) Would constitute a violation of any law of this state or of the United States, or any rule promulgated pursuant thereto, with which the employer is required to comply;

   (b) Would constitute a violation of the conditions of eligibility for receipt by the employer of financial assistance from the government of this state or the United States;

   (c) Would place the individual in a position of exercising supervisory, appointment or grievance adjustment authority over a member of the individual's family or in a position of being subject to such authority which a member of the individual's family exercises; or

   (d) Would cause the employer to disregard a bona fide occupational requirement reasonably necessary to the normal operation of the employer's business.

(3) As used in this section, "member of an individual's family" means the wife, husband, son, daughter, mother, father, brother, brother-in-law, sister, sister-in-law, son-in-law, daughter-in-law, mother-in-law, father-in-law, aunt, uncle, niece, nephew, stepparent or stepchild of the individual.

3 See, e.g., Ross v. Stouffer Hotel Co., 879 P.2d 1037 (Haw. 1994) (no-spouse rule violates state law against discrimination based on marital status unless one of several statutory exemptions applies); Fitzpatrick v. Duquesne Light Co., 601 F. Supp. 160 (W.D. Pa. 1985), aff'd, 779 F.2d 42 (3d Cir. 1985) (anti-nepotism policy did not constitute sex discrimination where it was facially neutral and evenly applied in a nondiscriminatory manner).

4 See, e.g., Montgomery v. Carr, 101 F.3d 1117 (6th Cir. 1996) (upholding a no-spouse rule, stating that in the absence of direct or substantial interference with
the right to marry, the applicable level of scrutiny is the "rational basis" test, which invalidates a policy only if it fails to advance a legitimate governmental interest or if the means of advancing the interest is unreasonable; Parks v. City of Warner Robins, 43 F.3d 609 (11th Cir. 1995) (rejecting arguments that an anti-nepotism policy denied plaintiff's right to marry, infringed on the right to intimate association, or had a disparate impact on women, in violation of the Equal Protection Clause); Shahar v. Bowers, 114 F.3d 1097 (11th Cir. 1997) (rejecting employee's freedom of association and other constitutional claims based on employer's withdrawal of offer of employment after learning of same-sex "marriage").


6 Id.; see also, S. Elizabeth Wilborn, Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace, 32 Ga L Rev 825 (1998); but see, e.g., Schowengerdt v. United States, 944 F2d 483 (1991) (rejecting right to privacy claim based on military regulations requiring bisexual's discharge from military).

7 See generally, Martin Wald and Jeffrey D. Kahn, Privacy Rights of Public Employees, 8 Lab Law 301, 315 (1990).


9 See, e.g., Tanatchangsang v. Owens-Brockway, 172 Or.App. 470, 21 P.3d 97, review allowed, 332 Or. 430, 30 P.3d 1183 (2001), in which a female employee notified her employer of threats and violence committed by her ex-boyfriend/co-worker who, after being placed on leave, returned to the workplace drunk, shot and killed the employee and then himself. The woman's family sued the employer and the security company that had been hired to guard the plant. The trial court granted summary judgment for the employer and the Court of Appeals affirmed, finding that worker's compensation provides the exclusive remedy for the employee's death. The case is currently on appeal to the Oregon Supreme Court.


invasion of privacy where they independently conducted surveillance on a co-worker at social events to confirm rumors of fraternization); *Stiver v. Olsten Kimberly Quality Care*, 2001 U.S. App. LEXIS 23807 (9th Cir 2001) (unpublished opinion) (employee who claimed he was fired for his extramarital romantic relationship with a coworker sued for invasion of privacy and wrongful termination).


16 See also, *Von Heeder v. Safeway, Inc.*, 2001 U.S. Dist. LEXIS 19681 (2001) (three female employees sued after manager allegedly peeked through ceiling vent to view them using the restroom). It should be noted that under Oregon law, it is a criminal offense to videotape another person in a state of nudity without permission to do so. See ORS 163.700:

(1) Except as provided in ORS 163.702, a person commits the crime of invasion of personal privacy if:

a. The person knowingly makes or records a photograph, motion picture, videotape or other visual recording of another person in a state of nudity without the consent of the person being recorded; and

b. At the time the visual recording is made or recorded the person being recorded is in a place and circumstances where the person has a reasonable expectation of personal privacy.

(2) As used in this section:

a. "Makes or records a photograph, motion picture, videotape or other visual recording" includes, but is not limited to, making or recording or employing, authorizing, permitting, compelling or inducing another person to make or record a photograph, motion picture, videotape or other visual recording.

b. "Nudity" means uncovered, or less than opaquely covered, post-pubescent human genitals, pubic areas or a post-pubescent human female breast below a point immediately above the top of the areola. "Nudity" includes a partial state of nudity.

c. "Places and circumstances where the person has a reasonable expectation of personal privacy" includes, but is not limited to, a bathroom, dressing room, locker room that includes an area for dressing or
showering, tanning booth and any area where a person undresses in an enclosed space that is not open to public view.

d. "Public view" means that an area can be readily seen and that a person within the area can be distinguished by normal unaided vision when viewed from a public place as defined in ORS 161.015.

(3) Invasion of personal privacy is a Class A misdemeanor.


21 Id. at 181.

22 See generally, I Know What You E-Mailed Last Summer; Legal Update Employee Monitoring 46(1) ASAP 93 (Jan. 2002).


Apparently, some states are willing to go to the extreme to combat one aspect of Internet abuse: South Carolina reportedly enacted a law that penalizes IT workers by up to six months in jail and $500 in fines if they come across child pornography in the course of their work and fail to report it. See transcripts from Monitoring Employee Online Behavior, Talk of the Nation (2/11/2002).

24 See 18 USC §§ 2510-2522, 2701-2711 (Electronic Communications Privacy Act, or ECPA) , which prohibits certain conduct with respect to e-mail and voicemail, and allows states to enact stricter prohibitions; see also, Brown, Developing Corporate Internet, Intranet and E-Mail Policies, 520 P.L.I. 347, 352 (1998). Oregon has adopted stricter prohibitions than the ECPA. See ORS 165.540. A brief summary of relevant portions of the ECPA and Oregon law are attached as an appendix to this memorandum.

25 Not all employers are willing to go this far. Interestingly, just a few months ago a 14-judge committee on automation and technology for the federal courts decided to remove a section of a proposal on employee Internet use for federal court employees (additional considerations also apply to public employees when considering e-mail policies). The original proposal would have essentially eliminated the employees' right to privacy when using e-mail and the Internet. Instead, the approved policy allows some monitoring of Internet use but keeps e-mail private. Judges apparently want their privacy, too.

26 See, e.g., Meloff v. New York Life Ins. Co., 51 F.3d 372 (2nd Cir 1995) (employee sued for defamation and discrimination after employer sent her co-
workers an e-mail stating that she had defrauded the company by her use of a credit card).

27 See 29 CFR § 1630.8; see also, Hartog v. Wasatch Academy, 129 F.3d 1076 (10th Cir. 1997) (upholding dismissal of a teacher because his adult son, who suffered from bipolar affective disorder, attacked and threatened several school community residents; while court acknowledged "association discrimination" is prohibited by the ADA, it found for the employer, reasoning that the ADA does not require reasonable accommodation for the disabilities of relatives or associates and the son posed a "direct threat" to the employer's workplace).

28 See ORS 659A.030 [formerly ORS 659.030], which provides in relevant part:
It is an unlawful employment practice:

a. For an employer, because of an individual's race, religion, color, sex, national origin, marital status or age if the individual is 18 years of age or older or because of the race, religion, color, sex, national origin, marital status or age of any other person with whom the individual associates, or because of a juvenile record, that has been expunged pursuant to ORS 419A.260 and 419A.262, of any individual, to refuse to hire or employ or to bar or discharge from employment such individual. However, discrimination is not an unlawful employment practice if such discrimination results from a bona fide occupational requirement reasonably necessary to the normal operation of the employer's business.

b. For an employer, because of an individual's race, religion, color, sex, national origin, marital status or age if the individual is 18 years of age or older, or because of the race, religion, color, sex, national origin, marital status or age of any other person with whom the individual associates, or because of a juvenile record, that has been expunged pursuant to ORS 419A.260 and 419A.262, of any individual, to discriminate against such individual in compensation or in terms, conditions or privileges of employment.

30 42 USC § 12112(d)(4)(A); ORS 659A.136 [formerly ORS 659.448].
31 42 USC § 12112(d)(3) and (4); ORS 659A.136(2) [formerly under ORS 659.448]; ORS 659A.133 [formerly ORS 659.447].42 USC § 12112(d)(3) and (4); ORS 659A.136(2) [formerly under ORS 659.448]; ORS 659A.133 [formerly ORS 659.447].
32 42 USC § 12112(d)(2)(i); ORS659A.133(3)(b) [formerly under ORS 659.447].
33 See EEOC Enforcement Guidance on Disability-Related Inquiries and Medical Examinations of Employees Under the Americans with Disabilities Act (ADA) (7/27/00) (question 11).
34 29 CFR § 825.305; ORS 659A.168 [formerly 659.482].
35 29 CFR § 825.307; ORS 659A.168(1) [formerly under ORS 659.482].
37 See, e.g., ORS 659A.133 [formerly ORS 659.447].
38 42 USC § 12112(d)(2)(i).
(3) Partial Exemptions:

(a) If your company never had more than ten (10) employee during the last calendar year, you do not need to keep OR-OSHA injury and illness records unless the Director informs you in writing that you must keep records. However, all employers covered by the Oregon Safe Employment Act must report to OR-OSHA any workplace fatality or the hospitalization of three or more employees (See (21) below).

(A) The partial exemption for size is based on the number of employees in the entire company.

(b) If your company had more than ten (10) employees at any time during the last calendar year, you must keep OR-OSHA injury and illness records unless your business is in a specific low hazard retail, service, finance, insurance or real estate industry in Table 1. If so, you do not need to keep OR-OSHA injury and illness records unless the government asks you to keep the records under 437-001-0700(23).

(c) If any of your company's establishments are in a nonexempt industry, you must keep OR-OSHA injury and illness records for all your establishments unless your entire company is partially exempted because of size under 437-001-0700(3)(a).

(4) Alternate or Duplicate Records. If you create records to comply with another government agency's injury and illness recordkeeping requirements, those records meet OR-OSHA's recordkeeping requirements if OR-OSHA accepts the other agency's records under a memorandum of understanding with that agency, or if the other agency's records contain the same information as this standard requires you to record. Contact your nearest OR-OSHA office for help in determining if your records meet OR-OSHA's requirements.

47 OAR 437-001-0700. The OSHA 300 form is the "Log of Work-Related Injuries and Illnesses," the 300-A is the "Summary of Work-Related Injuries and Illnesses," and the DCBS Form 801 or equivalent is the "Worker's and Employer's Report of Occupational Injury or Disease."

48 OAR 437-001-700(14)(g).

49 42 USC § 12114(a)(1994); 29 CFR § 1630.3(a) (1998); ORS 659A.124 [formerly ORS 659.442]. However, Oregon and a handful of other states permit the use of marijuana for certain qualifying medical reasons. See, ORS 475.300 to 475.346; OAR 333-008-0000 et seq. Consequently, an Oregon employer must
carefully consider the circumstances before taking any action against a protected employee who tests positive for marijuana.


52 Individuals who were addicted to drugs, but are not currently using drugs illegally, are protected under the ADA and Oregon Law. 29 CFR §1630.3(b)(1),(2); ORS 659A.124 [formerly ORS 659.442].

53 See EEOC Enforcement Guidance: Preemployment Disability-Related Questions and Medical Examinations (7/27/00) (question 2, disability related inquiries).

54 See ORS 659.840, 659A.300.

55 Id.


57 135 F.3d 1260, 1270 (9th Cir. 1998).

58 ORS 659A.303 [formerly ORS 659.036].

59 See ORS 192.531 et seq.

60 ORS 192.533(2)(d).


62 See 29 USC § 2007(b).

63 See ORS 659A.300 [formerly ORS 659.227].

64 See ORS 659A.315 [formerly ORS 659.380].

65 See 42 USC § 2000e-2(a)(1), ORS 659A.030(1)(b) [formerly ORS 659.030(1)(b)].

66 ORS 659A.318.

67 See Meltebeke v. Bureau of Labor and Indus., 322 Or. 132, 903 P.2d 351 (1995), in which an evangelical Christian owner of a small painting company was held not liable for religious harassment, although he invited an employee to church multiple times, tried to call him at home to encourage him to go to church, told him he had to be a good Christian to be a good painter, and told him he wanted to work with a Christian so he would not have to worry about theft. Surprisingly, the court held that the employer established an affirmative defense based on the rights of conscience and religious practices under Article I, Sections 2 and 3 of the Oregon Constitution. The court reasoned that the employer had no knowledge that his religious practice created an intimidating, hostile, or offensive working environment. See id. at 151. The court's holding has been criticized as inconsistent with federal law. See note 10, Dworkin, supra.

68 See 29 CFR §1605.3(b)(3).

69 15 USC § 1681b.

70 See, e.g., Cal. Civil Code §1785.20.5; see also, Cal. Civil Code §§1786.16, 1786.20.

71 See, e.g., ORS 181.555(2)(b), 181.560.
See, e.g., Wash. Admin. Code § 162-12-140 (fair employment inquiries under Washington law); Cal. Lab. Code § 432.7 (prohibiting the use of arrest records in making employment decisions).


Restatement (Second) Torts § 652B (1977); see McClain v. Boise Cascade Corp., 271 Or. 549, 533 P.2d 343 (1975) (unobtrusive surveillance of workers' compensation claimant outside his home was not actionable invasion of privacy). Illustrative cases include: Jackson v. Rohm & Hass Co., No. 1906 (Pa. C.P., Philadelphia County, Oct. 22, 2001), in which an employee was awarded $150,000 by a jury in Philadelphia based upon claims against his employer for invasion of privacy, negligent infliction of emotional distress, breach of duty of reasonable investigation, and civil conspiracy in connection with the employer's internal investigation of the employee's relationship with a co-worker. The employee claimed he was grilled by an attorney and member of the employer's security department, who inquired about his after-work date with a co-worker two weeks earlier. The employee was told his co-worker made certain accusations following their evening together. His employer's intent was apparently to head off a possible sexual harassment lawsuit against the company. The plaintiff alleged the questioning not only reached "an extreme degree of intrusion," but focused on non-work conduct.

French v. United Parcel Service, 2 F. Supp.2d 128 (D. Mass. 1998). In this case, a long-term manager invited three supervisors out to a beer festival. After returning to the manager's home and consuming a fair amount of alcohol, one of the supervisors into a violent rage, was injured, and went to the hospital. After a period of time, the manager decided to report the incident to the company. The company demoted the manager, who then quit and sued the company for invasion of privacy, wrongful termination, and intentional infliction of emotional distress, among other claims. The employee objected to the company's insistence that he disclose details about an incident that occurred at home after work hours. Massachusetts provides statutory protection against "substantial and serious interference with*** privacy." Mass. Gen. L. Ch. 214, § 1B. Nevertheless, the court dismissed the privacy claim, finding that a fellow employee's drinking was not a "highly personal" or "intimate" fact, the company had a right to information that reasonably bore on the job and that, in this case, the employer's right to know the information outweighed the employee's right to privacy.

See Civil Code § 1798.85, which provides in relevant part:

(a) A person or entity, not including a state or local agency, shall not do any of the following: (1) Publicly post or publicly display in any manner an individual's social security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public. (2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity. (3) Require an individual to transmit his or her social security number over the Internet unless the connection is secure or the social security number is encrypted.
(4) Require an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Web site. (5) Print an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. Notwithstanding this provision, applications and forms sent by mail may include social security numbers. (b) Except as provided in subdivision (c), subdivision (a) applies only to the use of social security numbers on or after July 1, 2002. (c) Except as provided in subdivision (f), a person or entity, not including a state or local agency, that has used, prior to July 1, 2002, an individual's social security number in a manner inconsistent with subdivision (a), may continue using that individual's social security number in that manner on or after July 1, 2002, if all of the following conditions are met: (1) The use of the social security number is continuous. If the use is stopped for any reason, subdivision (a) shall apply. (2) The individual is provided an annual disclosure, commencing in the year 2002, that informs the individual that he or she has the right to stop the use of his or her social security number in a manner prohibited by subdivision (a). (3) A written request by an individual to stop the use of his or her social security number in a manner prohibited by subdivision (a) shall be implemented within 30 days of the receipt of the request. There shall be no fee or charge for implementing the request. (4) A person or entity, not including a state or local agency, shall not deny services to an individual because the individual makes a written request pursuant to this subdivision. (d) This section does not prevent the collection, use, or release of a social security number as required by state or federal law or the use of a social security number for internal verification or administrative purposes.