Schwabe
WILLIAMSON & WYATT®

Jean Ohman Back
Schwabe, Williamson & Wyatt, PC
1211 SW Fifth Ave., Suite 1900
Portland, Oregon 97204
Telephone: 503-796-2960
Facsimile: 503-796-2900
Email: jback@schwabe.com

WORKPLACE BEHAVIOR AND PRIVACY ISSUES[1]

Workplace behavior and privacy issues in the workplace constitute one of the hottest topics for most employers. This is because workplace behavior affects employee performance and affects workplace culture. In addition, privacy in the workplace encompasses a broad range of issues, from what an employer can learn about an employee prior to hire, and what an employee's privacy rights are with respect to employer monitoring at work, to what an employee's privacy rights are with respect to social media and emails.

This presentation will discuss the current privacy issues that exist in the employment, and termination stages, and the development of statutes and case law to address these issues. It will also discuss what an employer can do or should do to monitor an employee's off work behavior.

A. EMPLOYEE SEARCHES

An employer's ability to search an employee's workspace, clothing, desk, and personal items depends on the particular circumstances involved in the reason for the search, and whether the employee has an expectation of privacy in the item being searched. Employees have a greater expectation of privacy when dealing with more invasive searches, such as searches of their bodies, clothing, or personal items. Employees have a lesser expectation of privacy when the search is of employer property, such as the employee's desk, locker, computer, or company-provided cell phone, as long

[1] Some of the information contained in these materials was patterned on chapters (with permission) in the *Oregon Human Resources Manual*, published by Associated Oregon Industries ("AOI"), edited by Jean Ohman Back and authored by the labor and employment lawyers at Schwabe, Williamson & Wyatt. AOI offers the *Oregon Human Resources Manual* for sale each year.

as the employer has dispelled the employee's expectation of privacy by announcing its right to and intent to search in a policy or other communication.

Public employees generally have a greater expectation of privacy than private employees because of the protections provided by the Fourth Amendment of the United States Constitution, which applies to public employers, and which guarantees "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of themselves and/or their property." This privacy right is not limited. Employers can reduce a public employee's expectation by informing the employee that employer-owned areas and equipment may be searched, although an employer cannot condition an employee's job on an employee's willingness to comply with employer searches. Public employers are not required to obtain a subpoena to perform a search, but they must establish the reasonableness of the search. Factors that courts look at to determine reasonableness include whether there is credible evidence of misconduct, the scope of the search, whether the employee has a strong expectation of privacy in the area (i.e., clothing or a purse as opposed to a desk or locker), and whether the search is limited.

B. MONITORING EMPLOYEE COMMUNICATIONS

Employers are generally allowed to monitor activity that occurs on systems and devices that are owned by the employer as long as the employer has policies in place that dispel any right to privacy that an employee may think exists. The reasons most commonly cited as to why an employer should monitor its email, phones and other computer systems and devices include, but are not limited to:

- To protect the company's trade secrets;

- To protect the security of the company's computer system and data by avoiding introduction of harmful viruses and by preventing the dissemination of confidential information;
- To guard against and reduce the risk of liability for sexual harassment; and
- To prevent a loss of productivity by monitoring whether employees are using the systems for personal non-work activities during work hours.

Monitoring in the workplace can occur in a variety of ways, including:

1. MONITORING EMAILS

Except with respect to certain limited circumstances, employers are allowed to monitor an employee's emails sent and received on employer-owned systems as long as the employer has dispelled the employee's right to privacy with an electronic communications policy. A recent exception to this long established rule came about in December 2014, when the National Labor Relations Board ("NLRB") issued its decision in *Purple Communications, Inc.*,[2] which held that an employee's use of an employer's communications systems during non-work time for "concerted rights" activities are statutorily allowed under Section 7 of the National Labor Relations Act ("NLRA"). Under Section 7, an employee has the right to communicate in the workplace about the terms or conditions of employment—for example, communications with at least one other employee about wages, hours, supervisors, benefits, etc. The NLRB held that an employer who has chosen to provide its employees with access to its computer system may not prevent employees from communicating about union activities, including organizing to form a union, as long as such discussions occurred during non-working

[2] 361 NLRB 126 (2014).

hours. The exception to this rule allows an employer to totally ban the non-work use of email under "special circumstances" in order to maintain production and discipline. Unfortunately, the Board did not state what "special circumstances" might entail, and further indicated that special circumstances would rarely exist.

Purple Communications is not the only limitation on an employer's ability to monitor its computer systems. An employer must also keep in mind that there are state and federal laws in place that limit the ability to monitor an employee's communications and to obtain access to an employee's websites that are accessible only through private passwords. Those laws will be discussed more fully below.

2. MONITORING TELEPHONE CALLS

As long as an employer has a good electronic communications policy that announces to employees that employees have no privacy right with respect to employer-owned devices, employers generally can monitor employee phone calls on employer-owned phones and phone systems. This includes cell phones provided to employees and voicemail and text messages. Employers may have valid reasons to do this—for example, monitoring phone calls with customers and clients. Although the *Purple Communications* decision dealt only with emails, the NLRB did leave open the possibility that it could be expanded at some time in the future to address other devices, such as telephones. At this time, however, it is limited to emails.

The right of employers to monitor phone calls includes monitoring text messages on its employer-owned devices. For example, in *City of Ontario v. Quon*,[3] the U.S. Supreme Court found that a police officer's personal text messages on a government-

[3] 130 S. Ct. 2619 (2010).

owned pager were not private and the employer/police department had the right to view the messages—even though public employees (unlike private employees) have Fourth Amendment rights against unreasonable search and seizure since their employer is the government. The important lesson to be learned from the *Quon* case is that an employer's policy regarding monitoring need not specify every means of communication subject to the policy. Employees must assume that any electronic device provided by an employer may be subject to monitoring, whether or not such a device is specifically mentioned in a written policy.

3. RECORDING TELEPHONE CONVERSATIONS

It is legal in Oregon for an individual to record a telephone conversation between himself or herself and another person without notifying the other participant(s) of the recording (assuming all participants in the call are physically located in Oregon). This is a fairly commonplace occurrence and is good reason for employers to be wary of engaging in detailed telephone conversations on sensitive employment-related matters.

It is, however, illegal in many states to obtain or attempt to obtain any part of a telecommunication or radio communication to which a person *is not a participant* by means of any device, unless consent is given by at least one participant. "Obtain" has been defined by the courts to include intercepting, as well as recording, by means of a device. (An exception to this law allows a person to obtain a telecommunication or radio communication without consent in his or her own home.) This means that an employer should not record employee telephone conversations unless employees have notice that the company may engage in such monitoring and the employees provide consent to the

monitoring. A comprehensive electronic communications policy in an employment manual can provide means of employee consent to monitoring.

4. KEYSTROKE MONITORING

Keyboard monitoring can track key words typed on a keyboard and can also track how fast employees are typing. Nearly half of employers use technology to track content, keystrokes, and time that an employee spends at the keyboard.[4] No statute prohibits an employer from using this technology on employer-owned systems.

It would, however, violate the Stored Communications Act (discussed below) for an employer to obtain passwords to an employee's private accounts by using keystroke monitoring. In *Rene v. G.F. Fishers, Inc.*,[5] the company utilized keylogger software and acquired the employee's passwords to her personal email account and personal checking account using the software. The company then reviewed and discussed the messages and contents. The employee complained about the access and was subsequently fired for "poor performance." She filed suit against the employer alleging the company violated the Stored Communications Act ("SCA"). While the court did not address certain factual issues under the SCA (e.g., whether the company accessed the employee's email messages before the employee opened them), it held that by alleging that the employer accessed her email messages, the employee had satisfied the burden of asserting a violation of the SCA.

---

[4] Privacy Rights Clearinghouse, "Workplace Privacy and Employee Monitoring," http://www.privacyrights.org/fs/fs7-work.htm.

[5] 817 F. Supp. 2d 1090, 1094 (S.D. Indiana 2011).

5. MONITORING INTERNET USE

Employers are also allowed to monitor an employee's use of the Internet on employer-owned systems as long as the employer has dispelled the employee's right to privacy with an electronic communications policy.

C. STATUTORY LIMITATIONS ON MONITORING

1. The Electronic Communications Privacy Act ("ECPA")

Congress passed the Electronic Communications Privacy Act of 1986 ("ECPA")[6] in reaction to increasing concern that new threats to civil liberties were being made possible by emerging technology. The ECPA is the controlling federal law dealing with surveillance and monitoring through telephone and other electronic means. Although the ECPA itself protects individuals against *government surveillance*, it does not provide a means of protection for employees against employers. It does, however, authorize two other federal laws of which employers should be aware: the Wiretap Act and the Stored Communications Act.

a. The Wiretap Act

The Wiretap Act forbids employers, among others, from intercepting, using, and disclosing any oral, wire, or electronic communication of employees. Employees can recover actual and punitive damages plus attorneys' fees and costs from employer violations of this Act.

(1) Oral Communications

An oral communication is anything "uttered by a person exhibiting an expectation that such communication is not subject to interception under such circumstances

---

[6] 18 U.S.C. §§ 2510-20, 2701-11.

justifying such expectation." In other words, an oral communication can be as informal as water-cooler conversation or as formal as a customer's complaint. Conversations among employees, even in a public work space, can sometimes be protected "oral communications" if spoken in private beyond the hearing range of others.

(2) Wire Communications

This category includes communications transmitted on any system that can function in interstate commerce and covers telephone and facsimile communication.

(3) Electronic Communications

Electronic communications include many of the communications that are widely used in today's workplace, such as:

- email,
- voicemail,
- text messages,
- messages transmitted over the Internet in blogs or on social networking sites, such as Facebook.

(4) Interception

Interception under the Wiretap Act is "acquisition of the content of any wire, electronic, or oral communications through the use of any electronic, mechanical, or other device." Courts have interpreted interception in a variety of ways. One court held that a defendant intercepted a communication when she retrieved and forwarded to her own personal mailbox a voicemail message from the intended recipient's mailbox before it had been received by the recipient. In another case, a court held that viewing an email message on the plaintiff's computer screen did not constitute "interception."

(5) Exceptions

The Wiretap Act's general prohibition on interception has some major exceptions:

- **The government exception.** The federal government is allowed to intercept certain communications in the interest of national security. The Federal Communications Commission is also allowed to intercept communications.
- **The general public communication exception.** Anyone may intercept communication intended for the general public, such as communications transmitted over radio waves.
- **The hacker exception.** A person can intercept communications transmitted by a computer trespasser or "hacker" if the owner of the computer authorizes the interception and has reason to believe such contents will be relevant to the investigation.
- **The device exception.** A person may use a pen register (a machine that writes down the phone numbers dialed from a particular telephone line) or a trap and trace device (a machine that records the phone numbers that come into a particular telephone line) without violating the Wiretap Act.
- **The service-provider exception.** This exception enables owners of a communications system (such as a communications server) to routinely review communications in order to manage and safeguard the system's information.

- **The party participant exception.** A party may intercept its own communications.
- **The consent exception.** If one party to the communication consents, there can be no "interception" of the communication. Courts have not yet defined prior consent, but it is clear that written consent by an employee is the strongest defense against an ECPA claim.

(6) Personal Phone Calls

Courts are less inclined to allow interception of employee communications where employers are attempting to monitor the content of personal phone calls. In monitoring communications, an employer should stop the interception as soon as it realizes the communication is of a personal nature. This does not limit an employer's right to discipline an employee for excessive personal phone calls while at work.

b. The Stored Communications Act

The Stored Communications Act ("SCA")[7] forbids unauthorized "access" to an "electronic communication while it is in electronic storage." Stored communications can take many forms, but they most commonly include computer files and email messages that have been archived.

(1) Exceptions

One important exception to the SCA is when a provider of wire or electronic communications service—such as an Internet provider—is given access to an employer's stored electronic communications, which would presumably enable the employer to monitor email that is archived on its communication system.

---

[7] 18 U.S.C. § 2701-12.

Another exception to the SCA allows access to stored electronic communications that have been made by, or sent to, a user if the user consents.

The SCA also includes an exception that allows an employer to access stored communications on a system for the purpose of safeguarding the employer's business interests. The boundaries of this exception will likely depend on the minimum level of access necessary to safeguard the employer's interest.

Finally, exclusively internal email systems provided by employers might be outside the scope of the SCA entirely, because such a service would not technically be provided to the public.

Case Illustrations

Pietrylo v. Hillstone Restaurant Group[8]

The plaintiff, an employee of the Hillstone Restaurant, created a MySpace page for fellow employees to "vent" about the restaurant; it was a personal and password-protected web page with an invitation-only user group. The MySpace posts complained about the restaurant, customers, and supervisors. A supervisor obtained a username and password from a hostess who felt coerced into providing the information. The plaintiff was discharged for violating a policy requiring professionalism and a positive attitude.

The jury awarded plaintiff $3,403 plus punitive damages of $13,612.

Konop v. Hawaiian Airlines Inc.[9]

The company accessed an employee pilot's secure website using another employee's log-in information (with his permission), even though the site's terms

---

8 2009 U.S. Dist. LEXIS 88702 (D.M.J. Sept. 29, 2009).

9 302 F.3d 868 (9th Cir. 2002).

prohibited access by management and prohibited authorized users from allowing others to access the site. The website contained vigorous criticisms of the airline's management and labor concessions. The company disciplined the pilot.

The court found the airline violated the SCA and that the exception to the Act (where permission to view is granted by a "user") did not apply because the authorized employees had not actually "used" the site themselves.

Pure Power Boot Camp v. Warrior Fitness Boot Camp[10]

An employee planned to leave his job to start his own company. When he resigned, his employer was able to access his personal email accounts, which he had logged into while at work, using a password that automatically "popped up." The company found damaging evidence related to the employee's pre-resignation activities.

The court found that the company's email policy was not specific enough to put the employee on notice that personal email viewed over the company's computers would be accessed by the company. The court also determined that the employee leaving his password on the computer did not create an implied consent to view his personal email accounts.

The court ruled the employer's conduct violated the SCA and that the damaging emails obtained in violation could not be used against the employee even though they would have been discoverable in the course of litigation.

D. OFF THE JOB BEHAVIOR

Have you ever wanted to discipline or terminate an employee for something that the employee did off the clock? Have you ever received complaints about something that

[10] 587 F. Supp. 2d 548 (S.D.M.I. 2008).

one of your employees did outside of the workplace? Have you ever worried about damage to your company's reputation from off-duty conduct by your employees?

Concern about off-duty conduct by employees is nothing new. Employers have long recognized that what employees do off the clock may affect the workplace on the clock. Even worse, what employees do off the clock may be a source of potential liability for employers.

Although concern about employee off-duty conduct is nothing new, technology is changing the types of issues and challenges that employers are facing. Email—for better or for worse—has fundamentally changed communication both inside and outside of the workplace. Personal blogs and Internet sites like Facebook also present a host of new issues for employers, as the private lives of employees are made public.

Some examples of employee off-duty conduct that commonly raises concern for employers include:

- Moonlighting
- Criminal activity
- Fraternization
- Drug and alcohol use
- Internet activity
- Union activity
- Political activity
- Employee conduct that the employer finds immoral or unethical, even if not illegal

Although new technology gives rise to new issues with employee off-duty conduct, employers can take comfort in the fact that the best practices for regulating employee off-duty conduct remain largely unchanged. This presentation will review those best practices and the analytical steps that employers should apply in evaluating any situation involving employee off-duty conduct.

1. HOW TO APPROACH SITUATIONS INVOLVING OFF-DUTY CONDUCT

You are considering whether to discipline or terminate an employee for something that the employee has done off the clock. What considerations should guide your decision-making?

No matter what the situation is, three basic questions should be your guide:

a. Is it lawful for me to take an employment action based on the conduct at issue?

(Or, stated differently, <u>can</u> I regulate this conduct?)

b. Is it wise for me to take an employment action based on the conduct at issue?

(Or, stated differently, <u>should</u> I regulate this conduct?)

c. If I decide to take an employment action based on the conduct at issue, have I protected myself from a potential employment claim based on my adverse employment action?

(Or, stated differently, have I executed my employment decision according to the best practices?)

The answers to those three questions are critical to minimizing potential liability from any employment decision involving off-duty conduct by employees. Although each

situation must be evaluated individually, some general considerations are discussed below.

2. CAN I REGULATE THIS OFF-DUTY CONDUCT?

The first question in evaluating employment decisions relating to employee off-duty conduct is whether you can regulate the conduct at issue. Most Oregon and Washington employers are at-will employers, meaning that they have a right to terminate an employee for no reason or for any reason not prohibited by law. Other employers—whether by union agreement or otherwise—are bound by contract to only terminate employees for "just cause." At-will employers obviously have much more freedom than "just cause" employers. Nevertheless, all employers should think about some of the same considerations in deciding whether to take an employment action based on an employee's off-duty conduct. Those considerations include:

- Is the off-duty conduct protected by law?
- What are the privacy rights of the employee in this situation?
- Is there a legitimate business reason for regulating this off-duty conduct?

Finally, as a practical matter, employers also should consider how a jury is likely to view the employment action if a claim were brought.

a. Is the Off-Duty Conduct Protected by Law?

In evaluating whether you can regulate an employee's off-duty conduct, the first question to ask is whether the off-duty conduct is protected by law. Although this is not an exhaustive list, some common examples of legally protected off-duty conduct include:

- Marital status,
- Religion,

- Sexual orientation,
- Concerted activity by employees, 29 USC § 157
- Off-duty tobacco use,
- Wage garnishment for child support,
- Pregnancy,
- Military service,
- Association with members of a protected class,
- Off-duty marijuana use in some states,
- Other conduct protected by substantial public policy (e.g., jury duty)

In addition to statutory protections, many states recognize the claim of wrongful discharge for at-will employees. Essentially, the wrongful discharge doctrine prohibits employers from terminating employees for carrying out important societal duties or well-established public policies. For example, Oregon courts have found that employers may not terminate employees for the following conduct on the grounds of public policy:

- Serving on a jury, *Nees v. Hocks*, 272 Or 210 (1975)
- Refusing to sign a false statement, *Delaney v. Taco Time Int'l*, 297 Or 10 (1984)
- Threatening to report patient abuse, *McQuary v. Bel Air Convalescent Home*, 69 Or App 107 (1984)
- Refusing to make a false allegation against a co-worker, *Thorson v. Dept. of Justice*, 171 Or App 704 (2000)

The wrongful discharge doctrine is commonly used as the basis for employee claims when no other protection exists. Because conduct protected under the wrongful

discharge doctrine is always evolving, employers should always consider whether the employee off-duty conduct at issue implicates any important public policies.

b. What Are the Privacy Rights of the Employee in This Situation?

In addition to examining whether the conduct at issue is legally protected, employers also should consider the privacy rights of the employee in deciding whether to regulate an employee's off-duty conduct. Some state law recognizes a common-law right to privacy. Employers may be liable to employees for violations of that right. As a general matter, the right to privacy protects against:

- Intentional and unauthorized intrusions into private matters that would be highly offensive to a reasonable person
- Publicizing private information that would be highly offensive to a reasonable person and that is not a matter of public concern
- Knowingly or recklessly publicizing false information about a person that would be highly offensive to a reasonable person

As a practical matter, employers should be particularly cognizant of privacy considerations when investigating employee off-duty conduct. The general rule is that no invasion of privacy occurs when an employer merely observes conduct that is "out in the open." But employers may not engage in surveillance of employees that is intrusive, such as peering into an employee's windows or trying to get an employee's medical or psychiatric history without a release.[11]

---

[11] *See McLain v. Boise Cascade Corp.*, 271 Or 549 (1975) (unobtrusive surveillance of employee during daylight hours of activities that could have been observed by passersby not invasion of privacy); *Leggett v. First Interstate Bank*, 86 Or App 523

EMPLOYER TIP!

In addition to the common-law privacy rights of employees, employers also should be cognizant of statutes and regulations that affect employees' privacy rights, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Fair Credit Reporting Act (FCRA).

c. Is There a Legitimate Business Reason for Regulating This Off-Duty Conduct?

Finally, in deciding whether to regulate the off-duty conduct at issue, employers also should consider whether there is a legitimate business reason why the employee off-duty conduct should be regulated. Stated differently, employers should ask if there is a reasonable nexus between the employee's off-duty conduct and the identified harm to the employer's legitimate business interests.

For "just cause" employers, the identification of such a nexus is a necessity. Absent a legitimate business reason, the regulation of employee off-duty conduct is unlikely to satisfy the "just cause" standard. But even at-will employers should consider whether a legitimate business reason exists to regulate the off-duty conduct at issue. In the absence of a legitimate business reason to regulate the off-duty conduct, employers are more vulnerable to claims that the off-duty conduct is a mere pretext for a discriminatory or otherwise unlawful employment action. If an employee brings a claim, a jury also is more likely to side with employers who regulated the off-duty conduct at issue for legitimate business reasons.

(1987) (meeting with employee's psychologist without a release may constitute invasion of privacy).

The following list sets out some common legitimate business reasons for regulating off-duty conduct:

- Concern about the off-duty conduct damaging the company's reputation
- Concern about the off-duty conduct causing workplace disruption
- Concern about the off-duty conduct harming employee morale
- Concern about the off-duty conduct rendering the employee unable to perform his or her job functions adequately
- Concern about potential legal liability for the off-duty conduct from other employees
- Concern about potential legal liability for the off-duty conduct from third parties

When identifying whether a legitimate business reason exists to regulate employee off-duty conduct, employers should think hard about whether a reasonable person would recognize the potential harm to the business from the off-duty conduct. If the potential harm is not readily discernible, then it will be more difficult to argue that a legitimate business reason exists to regulate the conduct.

EMPLOYER TIP!

Identifying a legitimate business reason for regulating employee off-duty conduct is critical in the event that a claim is brought for any adverse employment action. A mere claim that the off-duty conduct offends the sensibilities of the business owner or management may not be enough.

3. SHOULD I REGULATE THIS OFF-DUTY CONDUCT?

After evaluating whether you *can* regulate the employee off-duty conduct, the next question is whether you *should* regulate the conduct at issue.

In most circumstances, the decision whether to regulate employee off-duty conduct is a matter of business judgment. If it is permissible to regulate the off-duty conduct and a legitimate business reason exists to do so, then it often makes sense for employers to respond to off the clock conduct by employees.

In some circumstances, off the clock conduct by employees risks creating legal liability for employers from other employees or third parties. In those circumstances, employers not only can, but should, regulate the off-duty conduct at issue.

As a general rule, employers are only liable for conduct by employees that is within the course and scope of the employee's employment. To fall within the course and scope of employment, Oregon law has three requirements:

- The conduct occurred within the time and space limits of the employment (i.e., on the jobsite and during work hours);
- The conduct was of the type that the employee was hired to perform;
- The employee was motivated, at least in part, to serve the employer.

For example, if a bouncer for a tavern attempts to eject a rowdy patron and, in doing so, is excessively forceful and harms the patron, the tavern owner may be liable for the bouncer's conduct because the bouncer acted on the job to serve the tavern owner.

Although the "course and scope" requirement limits many claims against employers for employee off-duty conduct, other claims do exist. First, Oregon has a unique rule that employers may be liable for conduct outside of the course and scope of

employment if the employer directly enabled the employee to commit the misconduct. This type of claim affects only a limited number of employers.

Second—and more commonly—employers may face negligence claims for off-duty conduct by employees in some circumstances. Some common examples of negligence claims for employee off-duty conduct include:

- Employee breach of confidentiality
- Employee publication of personal or confidential information
- Employee misappropriation and use of trade secrets or other confidential information
- Identity theft claims
- Other negligent hiring, supervision, or training claims

Finally, employee off-duty conduct can create liability for employers from other employees. Common risk areas for employment claims based on off-duty conduct include sexual harassment claims or sexual discrimination claims.

4. BEST PRACTICES FOR REGULATING OFF-DUTY CONDUCT

When employee off-duty conduct has the risk of creating liability or otherwise damaging the employer, employers should follow the best practices for regulating the conduct. As a start, employers need to anticipate and prepare for the need to regulate employee off-duty conduct before it happens. When the need to regulate off-duty conduct arises, employers also need to walk carefully and thoughtfully through this thorny issue.

a. Policies, Policies, Policies

If you haven't already, you should identify areas of employee off-duty conduct that may be sources of liability or risk for your business. Do you have employees who regularly handle or have access to confidential information? Do you have employees who work with children or other vulnerable populations? Do you have employees who frequently fraternize with each other?

Once you identify potential areas of liability or risk for your business, then you should examine whether you have policies governing such behavior.

Common examples of employment policies relating to employee off-duty conduct include:

- Moonlighting policies
- Drug and alcohol policies
- Criminal activity policies
- Fraternization policies
- Internet policies
- Confidentiality policies

In drafting policies, it is often helpful to tie the policy to a business interest or, stated differently, identify the reason for the policy in the policy itself. Employers also should include training about policies—particularly policies relating to common risk areas such as sexual harassment and confidentiality issues—and should document those training efforts.

b. Enforce Policies Consistently and Evenly

Good policies and training only go so far in protecting employers. To avoid risk and liability, employers also must be willing to enforce policies. In the context of employee off-duty conduct, this is particularly important. Selective or inconsistent enforcement of policies relating to off-duty conduct may give rise to discrimination or other claims. Moreover, policies will not protect employers from negligence claims from third parties for employee off-duty conduct if the policies are not enforced.