

WILLIAMS KASTNER™



Privacy in the Workplace

Kimberly D. Baker

Todd R. Sorensen

With Special Guest Rashelle Tanner, General Counsel of CRISTA Ministries

Williams Kastner Labor & Employment Fall Update

November 14, 2007

Table of Contents

- PART I. Privacy Issues Prior to Employment.1**
 - A. Lawful Employment Verification and References.1**
 - 1. Application and Interview Questions.....1
 - 2. Requesting Employment Verification and References.3
 - a) Background or Reference Checks.....3
 - b) Pre-Employment Testing.4
 - i. Drug Tests.....4
 - ii. Other Pre-Employment Tests.....6
 - c) Pre-Employment Conviction and Arrest Inquiries.6
 - d) Fair Credit Reporting Act.7
 - 3. Failure to Verify or Obtain Verifications or References.9
- PART II. Privacy Issues During Employment.....10**
 - A. Employee Monitoring: Evolving and on the Rise.....10**
 - 1. Electronic Monitoring Becomes Necessary Practice.....10
 - 2. Biometrics12
 - 3. Blogging and Use of the Internet Beyond the Workplace.12
 - a) Employers Taking Action13
 - b) Tracking Down Anonymous Bloggers15
 - c) Employers Beware17
 - B. Sources of General Privacy Law.....18**
 - 1. Federal and State Constitutional Privacy Rights.18
 - 2. Common Law Right of Privacy.19
 - 3. Washington Privacy Act.21
 - a) Consent May Obviate Privacy Claim.22
 - b) Only “communications” are protected.....22
 - c) Only “private” communications are protected.....23
 - d) Sanctions for Violating Privacy Statute.....24
 - 4. Federal Electronics Communications Privacy Act.24
 - C. Confidentiality of Personnel Records and Information.25**
 - 1. Personnel Records.....25
 - a) Information Maintained in Personnel Files.....25
 - b) Disclosure to the Employee.27
 - c) Disclosure to Others.....27
 - 2. Medical Records.28
 - D. Public Sector: Public Information Requests30**
 - 1. Public Disclosure Act.30
 - 2. Freedom of Information Act.34
- PART III. Privacy Issues Post-Employment.35**
 - A. Misappropriation of Likeness/Infringement35**
 - B. Duty to Warn.....36**
 - 1. Liability for the Duty to Disclose.38
 - 2. Liability for Negligently Providing False Information.39
 - 3. Liability for Common Law Negligence.....40

C. Defamation.....40

PART I. PRIVACY ISSUES PRIOR TO EMPLOYMENT.

A. Lawful Employment Verification and References.

1. Application and Interview Questions.

To ensure that no unlawful discrimination takes place in the hiring process and to effectuate a policy against discrimination, Washington state has guidelines that cover pre-employment inquiries.¹ These guidelines apply to the applicants, references, and inquiries made by third parties such as credit reporting services on behalf of the employer.² Only inquiries about “bona fide occupational qualifications” can be made, and application forms must not contain inappropriate, discriminatory language, or gather information prohibited by law.³ The employer must also be prepared to provide application forms in formats and locations that are readily accessible to applicants with disabilities and/or otherwise assist disabled applicants. The application form should have a statement of the employer’s non-discrimination policy, a certification of accuracy and completeness, a release to allow contact with former employers, and an acknowledgement of the employer’s at-will policy signed by the applicant. A statement of accuracy and completeness may be used to withdraw incomplete applications from consideration and enable an employer to discipline or dismiss an employee if the applicant is found to have provided inaccurate information. In subsequent litigation, a misrepresentation or omission on an application or résumé may constitute after-acquired evidence limiting a plaintiff’s recovery of damages.⁴ A release and waiver may be used by the prospective employer to encourage former employers and reference sources to provide complete information about the applicant instead of the traditional “name/job title/employment date” information that most employers provide out of fear of defamation suits.

¹ WAC 162-12-140.

² WAC 162-12-140; Wash.Prac. vol 1B, Kunsch, § 61.29.

³ RCW 49.60.200.

⁴ See Janson v. North Valley Hospital, 93 Wn. App. 892, 900 (1999).

Application forms may not ask about protected class status, such as age, sex, race, or disability.⁵ This information, if required by the state or federal government, or for some legitimate purposes, must clearly inform the applicant that the information is voluntary, the reasons for asking the information, its use, and safeguards that will prevent use by people processing the application.⁶ If asked for these reasons, the employer should have a written policy that authorizes the inquiries as a means of monitoring its enforcement and that sets out detailed procedures for keeping the responses separate from other records regarding the applicant.⁷ Information collected for these purposes may be gathered on a separate form, on a tear-off page, or by other method, so that the information is not available to the decision maker.⁸ Such information shall be kept confidential, unless necessary to implement affirmative action program, or the compilation and verification of statistics.⁹ It is essential that such information be separate from the employee's application and regular personnel file.¹⁰ Failure to separate this protected information may lead to a claim that the information was used to discriminate against an employee who is a member of a protected class.

Both the state and federal government have created agencies to administer hiring practices. The Equal Employment Opportunity Commission ("EEOC") is the federal agency that has issued hiring guidelines which include pre-employment inquiries relating to sex.¹¹ The agency that governs hiring practices in Washington is the Human Rights Commission. The Human Rights Commission has issued a pre-employment inquiry guide.¹² Prohibited subjects include, but are not limited to, questions regarding: (1) marital status; (2) childbearing plans; (3) ancestry or national

⁵ RCW 49.60.200.

⁶ WAC 162-12-170(2).

⁷ WAC 162-12-170(1).

⁸ WAC 162-12-160(2).

⁹ Id.

¹⁰ Id.

¹¹ 29 C.F.R. § 1604.7.

¹² WAC 162-12.

origin; (4) age (if the inquiry is intended to convey a preference for an employee under the age of 40); and (5) disability. Examples of questions that are permissible and those that are considered unlawful are listed in the Pre-Employment Inquiry Guide at WAC 162-12-140. Washington law prohibits all pre-employment inquiries that unnecessarily reveal race, sex, or membership in other protected classes, whether or not the particular inquiry is explicitly covered in the Pre-Employment Inquiry Guide.¹³ Washington courts have held that even where the violation is facially neutral, if the pre-employment inquiry has a disparate impact on protected groups, it may be deemed to be discriminatory.¹⁴ For example, the Washington State Supreme Court held that a minimum height requirement of 5'9" for a sheriff's deputy position was deemed discriminatory where two Caucasian men were denied positions as a result of their height. The court held that the pre-employment inquiry was an unfair employment practice because of its unfavorable impact on some classes of persons, in particular women and other minority groups.¹⁵

The Americans with Disabilities Act ("ADA") limits questions that may be asked of an applicant and his or her former employer before making a **conditional** offer of employment. Before an offer, the prospective employer may not ask an applicant about: (1) his or her disability; (2) his or her illnesses and/or attendance problems related to those illnesses; or (3) his or her workers' compensation history.¹⁶

2. Requesting Employment Verification and References.

a) Background or Reference Checks.

An employer faces multiple risks when performing a background or reference check. There is a risk of liability for negligent hiring or retention if an employer fails to check

¹³ WAC 162-12-140.

¹⁴ Fahn v. Cowlitz County, 93 Wn.2d 368, 376-77 (1980).

¹⁵ Id.

¹⁶ See 42 U.S.C. § 12101 *et seq.*

references.¹⁷ Likewise, a prospective employer may be in violation of the ADA if it attempts to gather prohibited information. Employers should also be aware of possible claims of defamation or retaliation against the former employer-reference source.¹⁸ As a result, it is prudent to provide a signed release with all requests for references.

b) Pre-Employment Testing.

Employers may engage in pre-employment testing, so long as: (1) all entering employees are subjected to the same examination; (2) the screening is reasonably related to the demands of the position; (3) the information is collected and maintained in separate medical files and treated as confidential; and (4) the results of the examination are used only to determine the ability of an applicant to perform job-related functions.¹⁹ The information should only be disclosed as necessary and only to supervisors or managers requiring the information to determine restrictions on employees' work duties or accommodations, first aid personnel for purposes of emergency treatment, and government officials investigating compliance with the ADA.²⁰ Tests should be closely scrutinized to ensure that they are not discriminatory. The critical distinction to be made is that, while an employer may inquire as to an employee's ability to perform job-related function, the employer may not inquire as to whether the individual has a disability or as to the nature or severity of the disability, unless the inquiry is job-related and consistent with business necessity.²¹

i. Drug Tests.

Private sector employers may require their employees to consent to drug testing as a condition of employment.²² The Washington Supreme Court, however, has found that a public

¹⁷ Haubry v. Snow, 106 Wn. App. 666, 679 (2001); Carlsen v. Wackenhut Corp., 73 Wn. App. 247, 252-53 (1994).

¹⁸ Dicomes v. State, 113 Wn.2d 612 (1989).

¹⁹ 42 U.S.C. § 12112(d)(3); O'Hartigan v. State Dep't of Personnel, 118 Wn.2d 111, 120 (1991).

²⁰ 42 U.S.C. § 12112(d)(3)

²¹ 42 U.S.C. § 12112(d)(4)

²² Roe v. Quality Transportation Services, 67 Wn. App. 604, 609-11 (1992).

employer's pre-hiring drug screening test unconstitutionally invades privacy concerns unless the test is limited to applicants whose duties would genuinely impact public safety.²³ An employer must show a link between the need for drug testing and how it is related to public safety.²⁴

Employers contemplating the implementation of pre-employment drug tests should consider the recommendations of the National Academy of Sciences Committee ("NASC") on Drug Use in the Workplace. The NASC recommends: 1) that tests should be conducted using procedural safeguards and quality control standards similar to those recommended by the National Institute on Drug Abuse; 2) no positive drug-test result should be reported for a job applicant until the result has been confirmed by GC/MS technology; and 3) applicants should have the opportunity to challenge positive results before the information is given to the employer. Additionally, because drug testing can result in potential litigation, it is a good idea to ensure that the employer has retained all relevant documentation. Information on the collection site, records of all chains of custody, temperature, identification, all screening data, including controls and certifying scientist signatures, GC/MS data, positive identification validation reports, and specimen long-term storage, should be retained for possible litigation issues.²⁵

A distinction must be made between employer-mandated drug tests and drug tests to which employees have submitted in the context of a federally assisted drug program. As to the latter, federal regulations require that employers attempting to secure drug test results from a treatment program must first obtain the employee's written consent. The consent form must include: (1) the name of the program or person permitted to make the disclosure; (2) the name or

²³ Alverado v. WPPSS, 111 Wn.2d 424, 440 (1988).

²⁴ Robinson v. City of Seattle, 102 Wn. App. 795, 811 (2000) (pre-hiring urinalysis drug test held unconstitutional because it covered librarians, ushers and accountants).

²⁵ William D. Bremer, Annotation, Validity and Operation of Pre-Employment Drug Testing--State Cases, 96 A.L.R. 5TH 585 (2004) (citing UNDER THE INFLUENCE?: DRUGS AND THE AMERICAN WORKPLACE 187 (J. Normand, R. Lempert, C. O'Brien eds., National Academy of Sciences, 1994)).

title of the individual to which the disclosure is to be made; (3) the name of the patient; (4) the purpose of the disclosure; (5) how much and what kind of information is to be disclosed; (6) the signature of the patient; (7) the date on which the consent is signed; (8) a statement that the consent is subject to revocation at any time except to the extent that the program or person is to make the disclosure has already acted in reliance on it; (9) the date, event or condition upon which the consent will expire if not revoked before; and (10) that the consent is subject to revocation at any time except to the extent that the program which is to make the disclosure has already taken action in reliance on it. Once obtained, these records must be maintained separate from the employees' personnel file, in a secure room, locked file cabinet, or safe and there must be written procedures which regulate and control access to and use of the written records. They may only be released by a federally compliant consent or by order of a court under circumstances specified in 42 C.F.R. § 2.61-67. Employers compelled to produce records in response to such an order should take care to produce only information within the scope of the order.

ii. Other Pre-Employment Tests.

Employers cannot administer lie detector tests unless they are administering the tests to law enforcement employees or persons who manufacture or dispense controlled substances, nor can they test for HIV or hepatitis C unless absence of infection is considered a bona fide occupational qualification for the job.²⁶

c) Pre-Employment Conviction and Arrest Inquiries.

Employers may seek criminal arrest and conviction information if it bears a reasonable relationship to the job, and if such convictions or imprisonment occurred within the last ten years.²⁷ Schools, businesses, hospitals, or other organizations that have direct responsibility for

²⁶ RCW 49.44.120, 49.60.172.

²⁷ WAC 162-12-140.

the care of children, disabled, or otherwise vulnerable adults are permitted to inquire about arrests or convictions.²⁸

d) Fair Credit Reporting Act.

When gathering application information, verifications and references, employers must be cognizant of the federal and state Fair Credit Reporting Act (collectively “FCRA”).²⁹ The federal and state FCRA are similar, but not identical. Where the state and federal laws diverge, employers are required to abide by the law which provides the employee more protection on the issue at hand. The following explanation of recommended practices is accordingly tailored to provide those practices that will satisfy both federal and state law.

Notably, neither the state nor the federal FCRA apply if the employer itself checks the employee’s references. The FCRA governs employers’ procurement and use of “consumer reports” and “investigative consumer reports” from consumer reporting agencies for employment purposes.³⁰ A “consumer report” has information on credit worthiness, credit standing, and character or general reputation.³¹ An “investigative consumer report” has information regarding character, reputation, or mode of living obtained through personal interviews – *i.e.*, workplace investigations.

In practice, FCRA exposure will arise under two circumstances: (1) consumer reports ordered regarding a new employee and (2) consumer reports ordered regarding an existing employee. In either event, the employer must first secure the applicant or employee’s written permission to secure report.³² The employer must also provide notice to the applicant or employee of its intent to use the consumer report in its hiring or employment determination, and

²⁸ RCW 43.43.815-.845; WAC 162-12-140.

²⁹ Federal FCRA 15 U.S.C. § 1681, *et seq.*; Washington FCRA RCW 19.182.010 *et seq.*

³⁰ RCW 19.182.010(4)(a)(ii).

³¹ 15 U.S.C. § 1681a(d).

that notice must be made in a “clear and conspicuous manner,”³³ by use of a standalone disclosure document.³⁴ Pursuant to the Washington FCRA, consumer reports must not contain any records of arrest, indictment, or conviction of a crime from more than 7 years back.³⁵

After securing a consumer report, the employer must take precautions to ensure that the consumer report remains confidential. If the employer intends to make an adverse employment decision based upon any information in the consumer report, the employer must tread carefully, providing the employee adequate notice and an opportunity to be heard. Specifically, the FCRA requires that before terminating an employee, refusing to hire someone, or taking some other adverse employment action based upon information contained in a consumer report, the employer must provide the applicant/employee with:

- (1) a copy of the consumer report;³⁶
- (2) the name, address, and telephone number of the consumer reporting agency providing the report;³⁷
- (3) a description of the consumer’s rights under the FCRA pertaining to consumer reports obtained for employment purposes;³⁸
- (4) a reasonable opportunity to respond to any information in the report that is disputed by the consumer.³⁹

³² 15 U.S.C. ¶ 1681b(bb)(2)(A)(i)-(ii).

³³ Id.; RCW 19.182.020(2)(b).

³⁴ 15 U.S.C. § 1681b(b)(2)(A)(i)-(ii).

³⁵ RCW 19.182.040(1)(e).

³⁶ 15 U.S.C. § 1681b(b)(3)(A).

³⁷ RCW 19.182.020(c).

³⁸ 15 U.S.C. § 1681b(b)(3)(A).

³⁹ RCW 19.182.020(c).

3. Failure to Verify or Obtain Verifications or References.

With so many risks associated with exploring an applicant's background or work history, an employer may not wish to check references and hope for the best. The law, however, imposes a duty on employers to check and obtain information before hiring. Even though the process of obtaining information can be difficult and frustrating, employers should expend the effort to make reasonable and diligent background checks, especially for employees who will have contact with vulnerable individuals, such as the elderly or children.

An employer only breaches its duty to protect third persons from an unfit employee where: (1) the employer fails to use reasonable care to discover the employee's incompetence before hiring; and (2) the alleged injury is proximately caused by the employer's failure.⁴⁰ Thus, an employer who uses reasonable care in pre-employment inquiries has an absolute defense. As employment continues, the employer has a duty to exercise reasonable care to control its employee so as to prevent intentional harm or a risk of bodily injury to others where the employer "knows or should know of the necessity and opportunity" for controlling the employee.⁴¹ As with negligent hiring, "[a]n employer is not liable for negligent supervision of an employee unless the employer knew, or in the exercise of reasonable care should have known, that the employee presented a risk of danger to others."⁴² For instance, in Scott v. Blanchet High School, the school contacted the prospective teacher's previous employers and found that he had "excellent references."⁴³ The school also interviewed the teacher twice and discussed the policies by which he would have to abide. After the teacher allegedly had an affair with a

⁴⁰ See Peck v. Siau, 65 Wn. App. 285, 288 (1992) (quoting Scott v. Blanchet High School, 50 Wn. App. 37, 43 (1987)).

⁴¹ Peck, 65 Wn. App. at 294 (quoting Restatement (Second) of Torts § 317).

⁴² S.H.C. v. Lu, 113 Wn. App. 511, 54 P.3d 174 (2002) (citing Niece, 131 Wn.2d at 48-49); Thompson v. Everett Clinic, 71 Wn. App. 548, 555 (1993) (citing La Lone v. Smith, 39 Wash.2d 167, 171 (1951); John Does v. CompCare, Inc., 52 Wn. App. 688, 694, 763 P.2d 1237 (1988)).

⁴³ 50 Wn. App. 37, 38-39 (1987)).

student, the child's parents brought action for negligent hiring. Rejecting the claim, the court concluded: "the hiring process employed by the school suggests it took reasonable care in hiring [the teacher]. Although certain specific questions identified by [plaintiff] were not asked, the process appears sufficient as a matter of law to discover whether an individual is fit" to be employed.⁴⁴ Again, in Peck v. Siau, where the school district checked the teaching candidate's certification and background prior to hiring, the Court of Appeals held there was no evidence that the district "in the exercise of ordinary care should have known that he was unfit."⁴⁵

To ensure that liability for negligent hiring or retention is avoided, particularly when the prospective employee will have contact with the public, an employer should:

- (1) conduct a thorough pre-employment investigation, asking questions about employment gaps and discrepancies, seeking information which is job-related, and noting responses;
- (2) look for gaps in the employee's employment record and probe. Why did they work for an employer but omit them as a reference? Check references and prior employers whether or not they are listed as references before making a hiring decision; and
- (3) make a record of every action taken to ascertain information about the applicant, including the name of the person at a former employer who provided or refused to provide information during a reference check and the reason for refusal, if applicable.

By following these hiring steps, an employer can minimize the possibility of legal liability for hiring a dangerous employee who causes harm to others.

PART II. PRIVACY ISSUES DURING EMPLOYMENT.

A. Employee Monitoring: Evolving and on the Rise

1. Electronic Monitoring Becomes Necessary Practice.

Employers have always found ways to keep tabs on their employees' activities. As technology evolves, employers are finding new and innovative means of monitoring. According

⁴⁴ Id. at 43.

to a 2005 Electric Monitoring & Surveillance Survey, employer use of electronic monitoring and surveillance has increased 27% since 2001.⁴⁶ The increase should come as no surprise, as employers increasingly have the need to monitor internet use and e-mail in the workplace.

In addition to concerns about the dissemination of company information and quality control of employees' interactions with customers, employers must be aware of their potential liability for failing to monitor internet use which results in harm to fellow employees. According to a 2006 Harris Interactive survey, 6% of all men and 5% of all women with internet access at work admit that they have intentionally viewed internet pornography at work.⁴⁷ Employers subject themselves to potential liability where they fail to monitor such internet abuses, fail to take action, or unwittingly punish whistleblowers. For example, a company called Sierra Aluminum recently paid \$200,000 in settlement to the EEOC, after the EEOC alleged that the company terminated an employee in retaliation for her reporting of an assistant manager's use of his company computer to view pornography.⁴⁸ Employers should have a written policy in place prohibiting use of the internet to access pornography and other websites unrelated to their work. In addition, employers should implement software to block employees' access to pornography and other inappropriate sites and monitor employees' internet activities and electronic communications. Where employees fail to abide by the company's internet and e-mail policies, the employer should take action, document its actions, and treat whistleblowers with caution.

⁴⁵ 65 Wn. App. at 289.

⁴⁶ American Management Association and The E-Policy Institute, The 2005 Electric Monitoring & Surveillance Survey, <http://www.amanet.org/press/amanews/ems05.htm>.

⁴⁷ Armour, Stephanie, Technology Makes Porn Easier to Access at Work, USA TODAY, October 17, 2007, http://www.usatoday.com/tech/webguide/internetlife/2007-10-17-pront-at-work_N.htm.

⁴⁸ Id.

2. Biometrics

Both public and private employers are increasingly making use of technology known as “biometrics.” Biometrics is the use of personal characteristics, such as finger prints, iris prints, voices, gait or walking in order to determine where employees are located and when they have arrived. While typically thought of as a means to control access to restricted areas, these characteristics are now being used to track employees in the same way a “punch-in” clock has traditionally been used. For instance, the City of Berkeley, California, uses hand scan technology in its public works department to determine when its employee arrive at worksites.⁴⁹ The implications of biometrics in the workplace for employee privacy are far reaching. Rather than simply a medical report or a social security number, employers using biometric devices are charged with the task of protecting information so personal and so sensitive as characteristics which define the individual employee. As employee monitoring in the workplace continues to increase and evolve, employers must be aware of the protections the law may afford their employees.

3. Blogging and Use of the Internet Beyond the Workplace.

With new platforms such as Facebook and Myspace, the practice of “blogging” has become routine among employees. “Blogging” may be defined as crafting an “easy-to-publish webpage”⁵⁰ or “blog,” where individuals can “share Internet links, news stories, and personal opinions and diary entries”⁵¹ on the World Wide Web in order to form ongoing communications

⁴⁹ Joyce E. Cutler, “Tracking Systems Raise Privacy, Contractual Concerns, Speakers Say,” BNA, Inc. Daily Labor Report (May 30, 2007).

⁵⁰ Jason Krause, Here is some Advice if you want to Post Without Riling Your Employer, 4 ABA J. eReport 18, (2005).

⁵¹ Jason Boog, Employment Lawyers Finding Bloggers Mean Business pg. 23., Legal Business (accessed October 5, 2006).

on topics of interest.⁵² Not surprisingly, blogging regarding one's personal hobbies, sports, and relationships often spills over into blogging regarding one's life at work, including relationships with an employer's business operations, clientele or competitors, or even workplace management.

There are over an estimated "10 million blogs that exist today, with about 43,000 new ones popping up ever[y] day."⁵³ Blog readership has grown exponentially over the last several years, such that 27% of internet users now read blogs, and over 12% of internet users have posted comments or other materials on blogs.⁵⁴ While most of the blogs may be "relatively benign avenues of personal expression,"⁵⁵ the process of blogging, unlike e-mail, has a potential audience of millions.

a) Employers Taking Action

Many employers may see some benefit in keeping track of employee blogging activities. Blogs provide employees an opportunity to disseminate all kinds of information regarding their employers, from trade secrets, to privileged medical information, to defamatory statements regarding their employers, managers, or customers. Increasingly, employers are keeping their eyes open for employee blogs, and using those blogs either to terminate or take legal action against employees and former employees.

In 2004 there were only about eleven reported cases of U.S. employees fired for blogs. According to Morpheme Tales, a blog website that keeps statistics of fired bloggers, more than

⁵² Blog, Wikipedia, available at <http://en.wikipedia.org/wiki/Blog> (accessed October 5, 2006).

⁵³ Patricia MacInnis, Blog Warning: No policy equals exposure, Workopolis.com, available at <http://www.aolnetscape.workopolis.com/servlet/Content/itbiz/20050704/itbiz-blog?section=itbusiness> (accessed October 5, 2006).

⁵⁴ Lee Rainie, The State of Blogging, Pew Internet & American Life Project, available at http://www.pewinternet.org/pdfs/PIP_blogging_data.pdf (accessed October 5, 2006).

⁵⁵ MacInnis, supra note 53.

40 employees have been terminated for blogging since 2001.⁵⁶ The following are examples of high profile examples of employers struggling with litigation and media exposure⁵⁷ over off-duty blog sites:

- Delta fired an airline attendant, known as Queen of the Sky on her blog site, for allegedly publishing provocative pictures of herself in a Delta Airlines uniform.⁵⁸
- Google fired an employee for writing about the company's financial statements before they were made public.⁵⁹
- U.S. military demoted and fined a soldier for publishing classified information on his blog.⁶⁰

At least two significant blogging incidents have resulted in legal action. In The Permanente Group, Inc. v. Cooper, No. RG05203029 (Cal. Super. 2005), an employee discovered that her former employer, Kaiser, had posted patient information on a public website. The employee posted a link to data on her blog, "Corporate Ethics," and later posted the information itself on the same blog. When Kaiser learned of the blog, it filed suit to enforce the former-employee's confidentiality agreement. Kaiser prevailed on summary judgment. More recently, in Guajome Park Academy, Inc. v. Duperry, Civil No. 06-658 (S.D. Cal. 2006), a Vista, California charter school brought action against former employees who helped to create a web site which served as a bulletin board site for grade information, along with allegations that a

⁵⁶ Morpheme Tales, Statistics on Fired Bloggers, available at www.morphemetales.blogspot.com/2004/12/statistics-on-fired-bloggers.html (accessed October 5, 2006) (The creator of the blog was purportedly eliminated from consideration for a job due to her blog about other employers firing employees).

⁵⁷ Even if employees are not posting blogs about corporations, various (and often-times anonymous) third parties create highly viewed blogs to severely criticize the corporation, such as <http://wakeupalarm.com/> or www.googleareallysucks.blogspot.com.

⁵⁸ Christopher Byrne, Managing the Business Risk of Blogs, Compliance Solutions Advisor Magazine, available at <http://advisor.com/doc/16543> (accessed October 5, 2006).

⁵⁹ Byrne, supra note 58.

⁶⁰ Anne Broach, Army punishes soldier for blog posts, CNET News.com, available at http://news.com/21000-1028_3-5815812.html (accessed 9/27/06).

student's grade was improperly changed. Recently, on August 16, 2007, the court denied the employees' motion for summary judgment, and the litigation continues.

Even beyond bloggers, employers have seen fit to take adverse employment action against employees for off-duty internet offenses. For instance, when the police department for the City of Chandler, Arizona learned one of its officers, Ronald Dible, was selling pornographic images of himself and his wife on the internet, the City terminated Dible for violation of the department's prohibition of conducting "bringing discredit" to the City. While Dible brought action alleging the termination violated his First Amendment rights, in September 2007 the Ninth Circuit Court of Appeals affirmed the district court's entry of summary judgment in favor of the City.⁶¹ The Ninth Circuit held that Dible's speech did not touch a matter of public concern and, thus, was not entitled to First Amendment protection.

b) Tracking Down Anonymous Bloggers

Many bloggers are responding to increased corporate vigilance and the consequent fear of being "dooced" and have begun to blog anonymously. Generally, blogging anonymously can become as technical and secretive as the private or paranoid blogger chooses to become. In fact, there are websites available online to help warn bloggers of the legal risks of their activity and the technical steps to hide one's identity when blogging.⁶² Additionally, there are also websites

⁶¹ Dible v. City of Chandler, 2007 WL 2482147, *8 (9th Cir. Sept. 5, 2007).

⁶² How to Blog Safely (About Work or Anything Else), Electronic Frontier Foundation, available at <http://www.eff.org/Privacy/Anonymity/blog-anonymously.php> (accessed October 6, 2006); Ethan Zuckerman, A technical guide to anonymous blogging - a very early draft, available at <http://www.globalvoicesonline.org/2005/04/13/a-technical-guide-to-anonymous-blogging-a-very-early-draft/> (accessed October 6, 2006).

that assist employers unmask an anonymous blogger.⁶³ Bloggers who attempt to go underground may likely use one or more of the following techniques to hide their identity:⁶⁴

- Use pseudonyms and free webblogging services to avoid true identity;
- Use public computers to avoid personal computer identifying information (IP address);
- Use proxy servers to use third party's IP address instead of personal computer;
- Use encrypted onion routing which routes encrypted text through 2-20 computers and their corresponding IP addresses
- Use Invisiblog.com and MixMaster that encrypts email to post on anonymous weblogging site; the encrypted email is remailed up to 20 times stripping it of its data and using security keys to ensure anonymity

Employers can find employee blogs—even anonymous blogs—using a few basic techniques:

1. Conduct search through internet search engine sites, such as Google, or Technorati and BlogPulse (both Blog search engines). Search strings should be something like “[company name] blog” or “[product name] blog” or for legal blogs “[firm name] blawg.”
2. Search for employee name on search engines.
3. Monitoring employee internet usage from business computer department. Examining records for internet logs, nicknames, aliases, screen names, etc.
4. Identify blog-hosting service and request/compel blogging service to provide information about unique IP address of computer posting web logs on blogging site; or
5. Subpoena information from Internet Service Providers to reveal the identity information of the owner of computer with the IP address.
6. If IP address is a public computer monitor public computers to discover identity of blogger.
7. If necessary, seek further computer technicians to track down anonymous blogger.

⁶³ The websites available for employers lack in technical detail as compared to those aiding anonymous bloggers. *See e.g.* Kevin Berry, “How to Unmask an Anonymous Blogger,” The Corporate Counselor, available at <http://www.law.com/jsp/ihc/PubArticleIHC.jsp?id=1144067964387> (accessed October 6, 2006).

⁶⁴ Zuckerman, *supra* note 62.

c) Employers Beware

If an employer chooses to monitor employee blogging or other off-duty internet use, it should be aware of potential negative legal consequences. Many states have laws prohibiting employers from disciplining or discharging for an employee's lawful conduct during non-work hours.⁶⁵ Even apart from such specific laws, it is important that employers treat information learned in a blog just as they would treat information learned first-hand in the workplace. As such, employers should beware of pitfalls faced in disclosure of information in the workplace, for example:

- A terminated blogger may maintain claims for wrongful termination or invasion of privacy.
- With an employer monitoring a blog, the employee may take the position that the employer was on notice of any complaints of workplace discrimination described in the blog
- If an employer learns of complaints regarding harassment, hostile work environment, health and safety violations, plans for unionizing, or any other form of whistleblowing, an employee fired for such blogging may claim the termination was retaliatory;
- Public employers have the added difficulty of ferreting out any blogging which could be perceived as speech protected under the First Amendment.

⁶⁵ See e.g. Cal. Labor Code §96(k), §98.6.

B. Sources of General Privacy Law

1. Federal and State Constitutional Privacy Rights.

Public employers may be subject to privacy claims arising under the federal and Washington constitutions. Private employers, however, are not subject to constitutional claims of privacy.⁶⁶ Governmental employees are protected by the Fourth Amendment of the United States Constitution which protects “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . .” The Fourth Amendment prohibits the government from engaging in unreasonable searches or seizures, including a public employer’s ability to search its workplace or employees.⁶⁷ If a public employer violates an employee’s constitutional privacy rights, he or she may institute a civil action under 42 U.S.C. § 1983.⁶⁸

Employees of state and local government in Washington are similarly protected by the privacy right established in Const. Art. I, § 7 which states that “[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law.”⁶⁹ It is well settled that Const. Art. I, § 7 provides greater protection to individual privacy rights than the Fourth Amendment of the United States Constitution.⁷⁰ Unlike the federal courts, however, Washington courts have not determined whether a public employee can bring a claim for damages based on a violation of right of privacy under article I, section 7 of the state constitution.⁷¹

⁶⁶ Roe v. Quality Transportation Services, 67 Wn. App. 604, 608-09 (1992).

⁶⁷ O’Connor v. Ortega, 480 U.S. 709, 726, 107 S. Ct. 1492, 94 L. Ed. 2d 714 (1987) (public hospital violated psychiatrist’s right of privacy by searching his office and removing files though recognizing that an expectation of privacy cannot be eliminated by employer practices).

⁶⁸ See City of San Diego v. Roe, 543 U.S. 77 (2004) (finding San Diego Police Department did not violate police officer’s right to freedom of speech pursuant to officer’s 42 U.S.C. § 1983 claim because videotapes showing officer engaged in sexually explicit acts did not address a matter of public concern and were not related to internal workplace grievances or functioning of government offices).

⁶⁹ Const. Art. I, § 7.

⁷⁰ State v. Rankin, 151 Wn.2d 689, 694 (2004).

⁷¹ Reid v. Pierce County, 136 Wn.2d 195, 213-214 (1998).

Unlike public employees, whose privacy rights involve a precarious balancing of their dual identities as employees and citizens, private employees generally have a lesser expectation of privacy. Recently, the Ninth Circuit Court of Appeals clarified the extent of employees' privacy in the workplace in United States v. Ziegler.⁷² In Ziegler, the employer contacted the FBI to report that it caught one of its employees surfing the web for child pornography and consented to FBI's search of the employee's office and sent the employee's hard drive to the FBI.

Considering whether the FBI had violated the employee's privacy rights, the Ninth Circuit held that the employee had a reasonable expectation of privacy against unwarranted government search under the Fourth Amendment, largely due to private nature of his office—he had his own key to the door, and it was a private workspace. However, the Court found the search reasonable based upon employer's consent, and in so doing struck the distinction between employee privacy as against the government and employee privacy as against a private employer: “[E]ven where a private employee retains an expectation that his private office will not be the subject of an unreasonable government search, such interest may be subject to the possibility of an employer's consent to a search of the premises which it owns.”⁷³ Therefore, Ziegler could not have reasonably expected the property was his, free from any type of control by his employer.

2. Common Law Right of Privacy.

Washington courts recognize that all individuals, including private employees, have a common law right of privacy.⁷⁴ The common law right of privacy sets forth the same elements

⁷² Ziegler, 474 F.3d 1184 (9th Cir. 2007)

⁷³ Id. at 1192.

⁷⁴ Reid, 136 Wn.2d at 206.

required under the Public Disclosure Act. There are four privacy torts in Washington: (1) intrusion; (2) publication of private affairs; (3) appropriation of likeness and (4) publication in false light.⁷⁵

The privacy claim of “intrusion upon seclusion” requires the employee to show that there has been: (1) an intentional intrusion into; (2) the employee’s solitude, seclusion, or private affairs; and (3) that the intrusion would be highly offensive to a reasonable person.⁷⁶ Limiting liability to cases in which there was a reasonable expectation of privacy, a Washington court held there was neither an unreasonable nor unwarranted intrusion upon seclusion where a news report showed a videotape of a pharmacy and its occupants when taken from the sidewalk, because any passerby could have reasonably viewed the same scene.⁷⁷

In cases involving the privacy claim of “public disclosure of private facts,” courts, in order to determine liability, evaluate whether the matter that was publicized is one that would be highly offensive to a reasonable person, and is not of legitimate concern to the public.⁷⁸ A Washington court held that a valid action for invasion of privacy existed with regards to public disclosure of private facts where pictures of the corpses of the plaintiffs’ deceased relatives were appropriated and displayed without their approval.⁷⁹

To prove publication in false light, one must establish: (1) publication; (2) of a materially false statement; (3) that would be highly offensive to a reasonable person. Eastwood v. Cascade Broadcasting Co., 42 Wn. App. 88, 91, 708 P.2d 1216 (1985). “The form of invasion of privacy [publication in false light]. . . does not depend upon making public facts concerning the private

⁷⁵ Mark v. Seattle Times, 96 Wn.2d 473, 497, 635 P.2d 1081 (1981).

⁷⁶ See Doe v. Gonzaga Univ., 143 Wn.2d 687, 705-06 (2001).

⁷⁷ Mark v. King Broadcasting Co., 27 Wn. App. 344, 356-57, aff’d sub nom., Mark v. Seattle Times, 96 Wn.2d 473 (1981), cert. denied, 457 U.S. 1124 (1982).

⁷⁸ Reid, 136 Wn.2d at 206.

⁷⁹ Id. at 212.

life of the individual.” Restatement (Second) Torts § 652E, Cmt. a (emphasis added). Finally, to establish misappropriation of likeness, the employee must prove the employer used her name or likeness without consent.

An employer’s first line of defense against privacy is to reduce or eliminate its employees’ expectations of privacy in the workplace.⁸⁰ Employers should effectively communicate to employees that the employer reserves the right to have access to the physical spaces on its premises and the information in its files and information systems. Employers can ensure that they have communicated effectively by obtaining express agreements from employees to this effect; and by making any surveillance devices visible or known to employees.

3. Washington Privacy Act.

Washington’s Privacy Act prohibits all persons from eavesdropping or recording confidential communications.⁸¹ The Act prohibits the interception of “private communication transmitted by telephone . . . or other device,” or “private conversation” without the prior consent of *all* parties to the communication.⁸² A communication is considered to be private: (1) when parties manifest a subjective intent that the conversation is to be private; and (2) where the expectation of privacy is reasonable.⁸³ This Act creates an action for violation of a privacy right that may result in damages and attorneys’ fees. Employers should be cognizant of the Act’s requirements when monitoring or intercepting employee telephone conversations, internet use, or email, even when the purpose is for quality control and customer service.

⁸⁰ Mark, 96 Wn.2d at 497-98; Peters v. Vinatieri, 102 Wn. App. 641, 657 (2000).

⁸¹ RCW 9.73.030.

⁸² RCW 9.73.030(1)(a)-(b); State v. Pejsa, 75 Wn. App. 139, 149 (1994), rev. denied, 125 Wn.2d 1015 (1995).

⁸³ State v. Christensen, 153 Wn.2d 186, 193 (2004).

a) Consent May Obviate Privacy Claim.

If parties to the conversation consent to its monitoring or interception, there is no violation.⁸⁴ Valid consent to tape a telephone conversation may be obtained by announcing to all parties in a reasonably effective manner that the conversation will be recorded.⁸⁵ Consent to record a conversation may also be implied. A Washington court, for example, held that a party leaving a message on an answering machine has given implied consent to the recording because the sole purpose of an answering machine is to record a message.⁸⁶ Likewise, another Washington court held that a person who sends an e-mail message impliedly consents to the possibility that it will be recorded because the sender should know that the message must be recorded by the receiving computer and has the potential of being printed.⁸⁷

In limited circumstances only, consent of one party to the communication may suffice. For example, where a wire communication or conversation conveys threats of extortion, blackmail, bodily harm, “or other unlawful requests or demands,” or which “occur[s] anonymously or repeatedly or at an extremely inconvenient hour,” the conversation may be recorded with consent of only one party to the communication.⁸⁸ Although the relevant case law involves only criminal circumstances, one could reasonably argue that conversations involving harassment or discrimination would fall within this exception.

b) Only “communications” are protected.

The prohibition of recording without the consent of all participants only applies to “communications.” Giving the term its ordinary meaning, a Washington court explained that “communication” was the act of imparting, transmitting, or communicating facts or

⁸⁴ RCW 9.73.030 (1)(a)-(b) to (4).

⁸⁵ RCW 9.73.030(3).

⁸⁶ In re Marriage of Farr, 87 Wn. App. 177, 184-85 (1997), rev. denied, 134 Wn.2d 1014 (1998).

⁸⁷ State v. Townsend, 147 Wn.2d 666, 676 (2002).

information.⁸⁹ The court, however, held that the use of a line trap did not violate state law because it simply traced and recorded the defendant's computer hacking activity by identifying his phone number. The court distinguished between such recordings and the use of a *pen register* device, a form of communication falling within the scope of the statute, which recorded an exchange of dialing information and length of calls.⁹⁰ The court also clarified that video recordings of a person's image are not considered "communications," and the court chose instead to protect only *audio* recordings of an event, thus requiring consent only for audio recordings.⁹¹

c) Only "private" communications are protected.

To be protected under the Washington Privacy Act, the communication must also be truly "private," which is determined by evaluating the "reasonable expectations of the participants" to the conversation.⁹² Courts look at a variety of factors to determine what these reasonable expectations are, including the location, duration, and subject matter of the conversation; the presence or potential presence of a third party; and the role of the non-consenting party and his or her relationship to the party taping the conversation.⁹³ A Washington court held that a conversation between a daughter and her boyfriend on a cordless phone, overheard by the girl's mother who placed the call on speaker phone, was considered private.⁹⁴ However, in another Washington case, a court held that the police department's taping of a conversation between two people on a street corner was not protected because the parties did not have a reasonable expectation of privacy on a busy public street in sight and hearing of any passerby.⁹⁵ Likewise, a

⁸⁸ RCW 9.73.030(2).

⁸⁹ State v. Riley, 121 Wn.2d 22, 33 (1993).

⁹⁰ Id.

⁹¹ Haymond v. Dep't of Licensing, 73 Wn. App. 758, 761 (1994).

⁹² State v. Faford, 128 Wn.2d 476, 484 (1996).

⁹³ Christensen, 153 Wn.2d at 193.

⁹⁴ Id.

⁹⁵ State v. Clark, 129 Wn.2d 211, 228-29 (1996).

meeting at which the parties may reasonably expect that someone will reveal what transpired to others is not considered to result in a “reasonable expectation of privacy” for purposes of the eavesdropping statute.⁹⁶ Therefore, an employer can limit its potential for liability by minimizing employees’ reasonable expectations of privacy in the workplace.⁹⁷

d) Sanctions for Violating Privacy Statute.

Sanctions for violating the privacy statute include compensation for actual losses and mental pain and suffering or, if actual damages cannot be proven, liquidated damages of one hundred dollars per day, not to exceed one thousand dollars, and reasonable attorney’s fees and other litigation costs.⁹⁸ The unlawfully taped information cannot be used as evidence at trial even if it proves the employer’s position. Moreover, the individual who has unlawfully taped a conversation is prohibited from testifying from memory as to the contents of the conversation.⁹⁹

4. Federal Electronics Communications Privacy Act.

The federal law, the Electronic Communications Privacy Act of 1986 (“ECPA”), has similar restrictions on intercepting employee written and oral communications.¹⁰⁰ The ECPA prohibits the acquisition or disclosure of the content of a wire, oral or electronic communication using electronic, mechanical or other device.¹⁰¹ The federal statute applies to the “interception” of a communication – *i.e.*, contemporaneous with its transmission.¹⁰²

⁹⁶ See *id.* at 229-30.

⁹⁷ See Doe v. XYZ Corp., 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005) (holding that an employer who is on notice that an employee is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee’s activities and to take prompt and effective action to stop the unauthorized activity, and that “[n]o privacy interest of the employee stands in the way of the employer’s duty” because the employee had no legitimate expectation of privacy based on company’s e-mail and computer use policy stating that e-mail was the property of the company and that the company had a right to review, audit, access, and disclose any e-mail).

⁹⁸ RCW 9.73.060.

⁹⁹ Schonauer v. DCR Entertainment, Inc., 79 Wn. App. 808, 818-19 (1995).

¹⁰⁰ 18 U.S.C. §§ 2510-2520.

¹⁰¹ 18 U.S.C. § 2511(1).

¹⁰² 18 U.S.C. § 2510(8). See also Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876-78 (9th Cir. 2002) (finding narrow definition of “intercept” [“acquisition contemporaneous with transmission” and not electronic storage])

The primary differences between the federal statute and the Washington Privacy Act are that the federal law permits one party consent¹⁰³ and allows the monitoring of conversations in the ordinary course of business.¹⁰⁴ Also, if an employee is provided notice of intent to monitor, his or her continued employment amounts to implied consent for the interception.¹⁰⁵ Courts have narrowly construed consent notwithstanding the clear statutory language. The statute provides for recovery of minimum statutory damages of \$10,000, actual and punitive damages, and attorney's fees and costs.¹⁰⁶

C. Confidentiality of Personnel Records and Information.

1. Personnel Records.

a) Information Maintained in Personnel Files.

Employers should maintain applications, resumes, employment verifications, background, criminal history, employee eligibility forms, tax and withholding forms, pay rate changes, transfers, demotions, promotions, termination forms or letters, performance reviews, customer complaints and disciplinary actions or counseling, and training orientation in personnel files. Employers may also maintain payroll, benefit records, tax records, paid time-off and other leave records in the personnel file, although this can create cumbersome and unwieldy files.

Employers should *not* maintain self-identification forms for race, disability, etc., investigation notes, statements obtained during investigations or medical information in personnel files. This information should be kept in a separate "manager's file," "investigations

applies to electronic communications (citing Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994)) (holding email "stored on an [employee's] electronic bulletin system, but not yet retrieved by the intended recipients [other employees and not employer], was not an 'interception' under the Wiretap Act [Title I of ECPA].")

¹⁰³ 18 U.S.C. § 2511(2)(d).

¹⁰⁴ 18 U.S.C. § 2510(5).

¹⁰⁵ 18 U.S.C. § 2511(2)(d).

¹⁰⁶ 18 U.S.C. § 2520(c).

file,” or “medical file.” A reference note may be placed in the personnel file directing anyone to see the manager or the Human Resource representative for additional information.

Employers should not have records that reflect possible protected group status or private information on employees’ after-hours behavior, arrest records, personal finances, family background, club memberships, religious affiliations, union activities and political beliefs. These subject areas could be misinterpreted as evidence of discriminatory intent in a subsequent discrimination lawsuit. On the other hand, certain employers are actually required to compile data on applicants’ and employees’ race, gender, ethnic background and veteran’s status, and file an annual EEO 1 report with the federal government. These records should be maintained in separate, limited access files. Employers should recognize that such statistical evidence may be used in a subsequent discrimination lawsuit and its inclusion in an employee personnel file makes it available to the employee and his or her attorney.

Employers should preserve personnel files after an employee leaves the job. Federal equal employment laws related to race, ethnicity, gender, age, religion, and disability require such records to be maintained for at least one year.¹⁰⁷ Wage information must be maintained for at least two years.¹⁰⁸ Employment contracts must be maintained for three years.¹⁰⁹ Also, if the cessation of the employment relationship results in litigation, destruction of personnel files could leave the employer without documentary evidence to support its decision and a court evidentiary finding that the destroyed personnel file would have contained adverse evidence (*i.e.*, the spoliation of evidence).¹¹⁰

¹⁰⁷ 29 C.F.R. § 1602.14 (Title VII and ADA); 29 C.F.R. § 1627.3 (ADEA).

¹⁰⁸ 29 C.F.R. § 1620.32; 29 C.F.R. §§ 516.5-.6.

¹⁰⁹ 29 C.F.R. § 516.5.

¹¹⁰ Brynie v. Town of Cromwell, 243 F.3d 93, 107-08 (2nd Cir. 2001); Kronisch v. United States, 150 F.3d 112, 128 (2nd Cir. 1998).

b) Disclosure to the Employee.

In Washington, an employee has a right to review his or her personnel file once a year upon reasonable request. Irrelevant or incorrect information should be removed. If the employer and employee disagree as to what is relevant or correct, the employee may place a rebuttal or correction into the file for up to two years following termination.¹¹¹ Often employees who are preparing to file a claim or bring a lawsuit will seek to initially review their files so that they can ascertain what, if anything, is in the file. If the employee is given a copy of the contents of his or her file, the employer can presume that those copies will also be shown to the employee's attorney. Even if not given a copy, the employee can still make a list of the contents. Something that should have been in the file, but was not, raises questions in subsequent litigation. Therefore, employers should strive to maintain complete, updated files, with performance reviews, counseling memoranda, or other information that would support its employment decisions in any subsequent action. Supervisors should be encouraged to forward all relevant performance information to an employee's personnel file. A lack of information in personnel files can raise a presumption that the stated reasons for termination were created after-the-fact and a mere pretext for discrimination.

c) Disclosure to Others.

Personnel records should not be disclosed except to the employee, management personnel with a need to know, government officials, or to a third party upon employee authorization or pursuant to a subpoena. Employers should not reveal information about an employee, including work performance, salary, medical information, or personal life to anyone else who does not have a "need to know." There are some exceptions to the general rule. For example, if an employee is disciplined for safety violations, harassment, or other issues of common concern

between the employer and its workforce, the employer *may* have a qualified privilege to discuss the issue with its employees. Any such communication should be narrowly tailored and made only to those with a common interest in the issue.

The legitimate purpose served by the disclosure needs to be carefully evaluated. In Henderson v. Pennwalt Corp., the plaintiff's supervisor discussed with other supervisors the plaintiff's sex life, promiscuity, and her relationship with a co-worker.¹¹² The Henderson court held that, while comments between supervisors regarding an employee's work performance were generally privileged, conversations about an employee's personal life were not so privileged; therefore, the employer could be vicariously liable for the supervisor's slander.¹¹³ The risks associated with disclosure are discussed more fully in Part III below.

2. Medical Records.

The Americans with Disabilities Act ("ADA")¹¹⁴ and the Family Medical and Leave Act ("FMLA")¹¹⁵ mandate that medical information concerning applicants and current or former employees should be kept in files separate from regular personnel files. Medical records must be treated as confidential files.¹¹⁶ Access should be limited to those who have a right and a need to know. An employer may reveal medical information to: (a) managers and supervisors if necessary for them to fashion restrictions on the work or duties of the employee as reasonable accommodation; (b) first aid and safety personnel to perform emergency treatment on the individual; (c) state or federal government officials when investigating compliance with the

¹¹¹ RCW 49.12.240-.260.

¹¹² Henderson v. Pennwalt Corp., 41 Wn. App. 547 (1985).

¹¹³ Id. at 559.

¹¹⁴ 42 U.S.C. § 12112(d).

¹¹⁵ 29 C.F.R. § 825.500(g).

¹¹⁶ 29 C.F.R. § 825.500(g) (citing 29 C.F.R. § 1630.14(c)(1) with reference to ADA confidentiality requirements).

ADA, FMLA or other disability related laws; and (d) insurance companies for insurance purposes.¹¹⁷

The EEOC restricts disclosure of medical information by managers during the hiring process. If a current supervisor is aware of medical information regarding an employee who is applying for a new job within the company, he or she may not disclose that information to the person interviewing the employee or to the new supervisor. If the interviewer already has medical information at the pre-offer stage, he or she may not have to ignore it. Certain questions may be permissible if the interviewer has a reasonable belief that an accommodation may be needed in the new job.

An employer may request the confidential medical records of a current employee when it has a legitimate business reason for doing so.¹¹⁸ To determine job fitness, an employer may demand that its employee undergo an examination and produce his/her medical records.¹¹⁹ Employers should be aware that an individual may be able to maintain an ADA claim based upon the improper disclosure of confidential medical information whether or not the individual is disabled.¹²⁰

¹¹⁷ 42 U.S.C. § 12112(d)(3)(B).

¹¹⁸ 42 U.S.C. § 12112(d)(4)(A) (“A covered entity [employer] shall not require a medical examination and shall not make inquiries of an employee as to...as to the nature or severity of [a] disability, unless such examination or inquiry is shown to be job-related and consistent with business necessity.”).

¹¹⁹ See Giaccio v. City of New York, No. 04 Civ. 3652, 2005 U.S. Dist. LEXIS 642, at *1 (S.D.N.Y. Jan. 19, 2005). (“information obtained in accordance with 29 C.F.R. § 1630.14(c) through periodic physicals and ‘other medical monitoring’...“is to be treated as a confidential medical record”); Medlin v. Rome Strip Steel Co., 294 F. Supp. 2d 279, 293-95 (N.D.N.Y. 2003) (contents of functional capacity evaluation (“FCE”) conducted by physical therapist to determine whether employee could return to work after suffering non-work related injury constitutes confidential medical information under 42 U.S.C. § 12112(d)); Doe v. U.S. Postal Serv., 317 F.3d 339, 344-45 (D.C. Cir. 2003) (employee’s response on FMLA form was “in response to an employer inquiry, and not a voluntary disclosure,” and is subject to confidentiality requirement under 42 U.S.C. § 12112(d)(4)(B)).

¹²⁰ Cossette v. Minnesota Power & Light, 188 F.3d 964 (8th Cir. 1999); Shaver v. Indep. Stave Co., 350 F.3d 716, 722 (8th Cir. 2003).

The Health Insurance Portability and Accountability Act (“HIPAA”) establishes standards for the electronic transmission of certain health information.¹²¹ Under HIPAA, covered entities include only: (1) health care plans, including Medicaid and health providers, who electronically transmit protected health information in connection with health insurance claims or other specified transactions; (2) business associates of covered health plans; and (3) covered health care providers.¹²² Thus, HIPAA will not apply directly to employers unless they offer self-insured health plans or act as “business associates” of covered entities (i.e., health care providers, plans or clearinghouses). For covered entities, HIPAA provides that “Personal Health Information” or “PHI” may not be disclosed without appropriate written consent. PHI includes any information “created or received by a covered health care provider or health plan (or business associate) regarding the provision of health care, payment for health care, or physical or mental condition of a specifically identified individual.”¹²³

For employers which are not covered entities, HIPAA still affects the manner and extent to which an employer may obtain employee medical information. An employer in need of such information must have the candidate or employee complete a modified consent form that complies the federal regulations under 42 C.F.R. Part 2. The form should be modified to include a provision that the information received cannot be redisclosed.

D. Public Sector: Public Information Requests

1. Public Disclosure Act.

The Public Disclosure Act, RCW § 42.17.010 *et seq.*, requires public agencies to make all public records available for public inspection to assure public confidence in governmental

¹²¹ 42 U.S.C. §§ 1320D *et seq.*

¹²² 45 C.F.R. § 160.103.

¹²³ Id.

processes and to protect the public interest.¹²⁴ Public entities have a “positive duty to disclose” public records unless they fall within certain very specific exemptions.¹²⁵ Its purpose is to preserve “the most central tenets of representative government, namely, the sovereignty of the people and the accountability to the people of public officials and institutions.”¹²⁶ The basic purpose and policy of RCW 42.17 is to allow public scrutiny of government, rather than to promote scrutiny of *particular individuals* who are unrelated to any governmental operation.¹²⁷ Washington courts have consistently held that the Act is a strongly worded mandate for broad disclosure of public records.¹²⁸ Because a court is to construe provisions of the Act liberally, to promote complete disclosure of public records, it must view with caution any interpretation of the statute that would frustrate its purpose.¹²⁹ As a result of its goal of complete disclosure, exemptions are narrowly construed, and any agency refusing disclosure has the elevated burden of showing that one of the exemptions applies.¹³⁰

The Act applies only to public records – an obvious but rather important point.¹³¹ Determination of whether a document is public record is *critical* for purposes of the Act.¹³² The Act defines a “public record” as “any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.”¹³³ That may include almost anything maintained by a public or governmental agency, including

¹²⁴ Servais v. Port of Bellingham, 127 Wn.2d 820, 827 (1995).

¹²⁵ ACLU v. City of Seattle, 121 Wn. App. 544, 548 (2004).

¹²⁶ O’Connor v. Washington State Dep’t of Soc. & Health Serv., 143 Wn.2d 895, 905 (2001); Comaroto v. Pierce County Med. Examiner’s Office, 111 Wn. App. 69, 72 (2002).

¹²⁷ Cowles Publ. Co. v. Pierce County Prosecutor’s Office, 111 Wn. App. 502, 510 (2002).

¹²⁸ Amren v. City of Kalama, 131 Wn.2d 25, 31 (1997).

¹²⁹ Kleven v. City of Des Moines, 111 Wn. App. 284, 289-90 (2002).

¹³⁰ ACLU, 121 Wn. App. at 549.

¹³¹ Smith v. Okanogan County, 100 Wn. App. 7, 12 (2000).

¹³² Oliver v. Harborview Medical Center, 94 Wn.2d 559, 566 n.1 (1980).

papers, photos, maps, video, and electronic records (*i.e.*, e-mail).¹³⁴ A Washington court has held that documents in a prosecutor's office files that were compiled for use on cross examination of a child sex abuse defense expert witness were considered "public records" within the meaning of the Act because they were used to carry out governmental functions.¹³⁵ Additionally, another court held that e-mails sent by a former employee of the prosecutor's office to her family members and friends were considered "public records" under the scope of the Act.¹³⁶ Because the former employee had been terminated for excessive e-mail use, and because the e-mails were used in preparation for litigation of her termination, a proprietary function, the e-mails qualified as "public records."

If the sought after records are not "public records" within contemplation of the Act, the government agency is not required to produce them.¹³⁷ Alternatively, even if the documents at issue are public records, the Act exempts from disclosure personal information maintained for employees to the extent that such disclosure would violate the employees' right of privacy.¹³⁸ However, privacy is considered to be invaded or violated only if disclosure would be highly offensive to a reasonable person *and* disclosure is not a legitimate concern to the public.¹³⁹ Washington courts have narrowly construed this privacy right, holding that certain employee performance evaluations, internal investigation reports, and employee complaints are discoverable.¹⁴⁰ The contours of the right of privacy exemption are well drawn by Bellevue John

¹³³ RCW 42.17.020(27).

¹³⁴ RCW 42.17.020(36) and (42).

¹³⁵ Dawson v. Daly, 120 Wn.2d 782, 789 (1993).

¹³⁶ Tiberino v. Spokane County, 103 Wn. App. 680, 688 (2000).

¹³⁷ Smith, 100 Wn. App. at 14-15.

¹³⁸ RCW 42.17.310(b).

¹³⁹ RCW 42.17.255; King County v. Sheehan, 114 Wn. App. 325, 344 (2002).

¹⁴⁰ Ollie v. Highland School Dist. 203, 50 Wn. App. 639, 645, rev. denied, 110 Wn.2d 1040 (1988) (holding that not all information contained in personnel records and evaluations of school district employees is privileged and

Does v. Bellevue Sch. Dist., No. 405, 129 Wn. App. 832, 120 P.2d 616 (2005), where the Seattle Times submitted a PDA request to a school district, seeking documentation of instances in which teachers were alleged to have committed inappropriate sexual acts. In response, the school district, properly, notified the teachers at issue of the request, offering them the opportunity to object, and several did. The court observed that while RCW 42.17.340 renders disclosure preferred, RCW 42.17.210(1)(b) contains an exemption for “personal information in files maintained for employees, appointees, or elected officials of any public agency to the extent that disclosure would violate their right to privacy.” The teachers argued that the disclosure would violate their right to privacy because (1) it would be highly offensive to a reasonable person and (2) it would not of legitimate concern to the public.¹⁴¹ The court drew a line between files which contain “routine performance evaluations” and files which documents specific instances of misconduct. While routine performance evaluations are not be disclosed, documentation of specific instances of misconduct must.

Washington courts have limited an individual’s privacy rights by establishing that even if the disclosure of the information would be offensive to the employee it may still be disclosed if there is a legitimate public interest in disclosure.¹⁴² To be “legitimate,” the public interest must be “reasonable.”¹⁴³ The purpose of the Act is to keep the public informed so that it can control and monitor the government’s function; in order to effectuate that purpose, records of agency expenditures for employee salaries, vacation, sick leave, and taxpayer-funded benefits are of

information about on-duty job performances should be disclosed); Spokane Research & Defense Fund v. City of Spokane, 99 Wn. App. 452, 457 (2000) (holding that a city manager’s performance evaluations were subject to public disclosure because they examined his public job performance and were, therefore, of legitimate public concern); Cowles Publishing Co. v. City of Spokane, 69 Wn. App. 678, 683-86 (1993) (holding that routine police reports filled out when a police dog made contact with a person were not exempt from public disclosure).

¹⁴¹ RCW 42.17.255.

¹⁴² Spokane Research & Defense Fund, 99 Wn. App. at 456-57.

¹⁴³ Tiberino, 103 Wn. App. at 690.

legitimate public interest and are not exempt from disclosure.¹⁴⁴ In construing what “legitimate” means, the Tiberino court held that the public had a valid interest in ensuring that employees were not spending their time on public payroll pursuing personal interests, and the public had a right to see the time spent on, and the quantity of, personal e-mails. However, the public did not have a legitimate interest in the content of personal emails; and as a result, a public employee’s emails were exempt from disclosure.¹⁴⁵

2. Freedom of Information Act.

A related federal statute is the Freedom of Information Act (“FOIA”), which governs disclosure of public records from the federal government.¹⁴⁶ FOIA requires that the federal government release certain agency records, unless the information is exempt or partially exempt from disclosure.¹⁴⁷ Each government agency – e.g., EEOC, OFCCP, DOJ, etc. – enacts its own regulations on production of records. Every government agency must post on its website information about FOIA use.

Agencies must produce (a) final opinions, (b) statements of policy and interpretations, and (c) administrative staff manuals and instructions.¹⁴⁸ Agencies must produce indices so the public can scan potential available information.¹⁴⁹ Agencies must also produce public records unless exempt from disclosure.¹⁵⁰ The requesting party is entitled to a response within 20 working days.¹⁵¹ If objectionable, the agency must identify the reasons therefore. Agencies may object to disclosure of national secrets, internal agency rules, trade secrets or other

¹⁴⁴ Id.

¹⁴⁵ Id. at 691.

¹⁴⁶ 5 U.S.C. §§ 552 *et seq.*

¹⁴⁷ 5 U.S.C. §§ 552(a)(1)(A)-(E).

¹⁴⁸ 5 U.S.C. § 552(a)(2).

¹⁴⁹ Id.

¹⁵⁰ 5 U.S.C. § 552(a)(3).

¹⁵¹ 5 U.S.C. § 552(a)(6).

privileged, confidential information, law, memoranda personnel and medical files, investigatory law enforcement records, employee pay rates, etc.¹⁵²

If an agency refuses to release records, a requestor may file suit to compel production of those records though one cannot recover monetary damages besides attorneys' fees and costs.¹⁵³ Employers should be aware that FOIA does not permit them to prevent disclosure of records through a private right of action.¹⁵⁴

PART III. PRIVACY ISSUES POST-EMPLOYMENT.

A. Misappropriation of Likeness/Infringement

After an employee leaves the company, the employer should remove the employee's name and contact information from its website. Employers who continue to use a former employee's likeness after termination of employment may be liable for misappropriation of likeness, publication in false light, and statutory infringement of an individuals' name, likeness or identity under RCW 63.50.050. For example, in May 2007, the Tenth Circuit affirmed an award of \$57,672 to a former executive of PA Consulting Group as damages for PA Consulting's continued use of the high profile executive's name after his departure from the company.¹⁵⁵ The Tenth Circuit reasoned: "There is no requirement, as PA suggests, that King point to a specific client that he would have procured; the marketing opportunities have value in and of themselves, value that King could have captured but for PA's wrongful conduct. Moreover, it would be manifestly unjust to require that King name a specific lost assignment to prevail on this claim, when it was PA that effectively cut off his communication to those clients."¹⁵⁶

¹⁵² 5 U.S.C. § 552(b).

¹⁵³ 5 U.S.C. § 552(a)(4)(B).

¹⁵⁴ Chrysler Corp. v. Brown, 441 U.S. 281 (1979).

¹⁵⁵ King v. PA Consulting Group, Inc., 485 F.3d 577 (10th Cir. May 8, 2007).

¹⁵⁶ Id. at 592.

In addition, employers who continue to publish materials suggesting a former employee is still affiliated with their company may be liable for publication in false light. While generally one's affiliation with a company would not be "highly offensive," in certain contexts, such as where the company is of ill repute, or where the employee is attempting to compete with her former employer, the continued publication of an affiliation with the employee may be highly offensive.

Finally, one source of liability that employers often overlook is Washington's statutory provision protecting employees' names and images. RCW 63.60.050 provides: "Any person who uses . . . a living or deceased individual's . . . name, voice, signature, photograph, or likeness, on or in goods, merchandise, or products entered into commerce in this state, or for purposes of advertising products, merchandise, goods, or services . . . without written or oral, express or implied consent of the owner of the right" commits infringement." Id. The statute provides for actual damages, defendant's profits, attorneys' fees and costs. In light of the foregoing, it is in the employer's best interest to eliminate references to an employee in its publications after the employee's departure.

B. Duty to Warn.

The employer is in a difficult position when deciding whether to provide a negative or positive reference of a former employee to a future employer. If the former employer provides a falsely positive reference about a violent former employee who goes on to commit a violent act at the new place of employment, it may be liable for negligent or intentional misrepresentation, depending on the state in which the employer is located. If, on the other hand, the employer provides a negative reference that the employee perceives to be false, the employer could find itself liable in a defamation or tortious interference lawsuit. In general, former employers have

no affirmative duty to disclose a former employee's violent tendencies or sexual misconduct to prospective employers.¹⁵⁷ However, once any employer has provided a reference, in some cases, they may be under a duty not to materially misrepresent the former employee's qualifications or character.¹⁵⁸

In a case of first impression, the Washington Court of Appeals appears to have rejected a duty for an employer to disclose information about a former employee.¹⁵⁹ The Richland School court held that an employer did not have a duty to disclose when it had provided favorable references and failed to inform an inquiring prospective employer of an employee's history of reprimands and dismissed charges of child molestation.¹⁶⁰ In Richland School, the Richland School District hired a night custodian, after receiving three letters of favorable recommendation about the custodian from Mabton officials who did not mention the custodian's dismissed charges of child molestation and reprimands that he received at work. Upon investigation of a complaint from a Richland School District parent about the custodian, the Richland School District discovered that the custodian had resigned from the Mabton School District in exchange for dismissal of three counts of child molestation. The Mabton School District, however, subsequently hired him as a substitute bus driver because it thought he was innocent of the charges.¹⁶¹ After discovering this information, Richland paid the custodian approximately \$100,000 in exchange for his resignation, and then sued the Mabton School District for damages

¹⁵⁷ Richland School Dist. v. Mabton School Dist., 111 Wn. App. 377 (2002). See also RCW 4.24.730 ("An employer who discloses information about a former or current employee to a prospective employer...at the specific request of that individual employer...is presumed to be acting in good faith and is immune from civil and criminal liability for such disclosure or its consequences if the disclosed information relates to: (a) The employee's ability to perform his or her job; (b) the diligence, skill, or reliability with which the employee carried out the duties of his or her job; or (c) any illegal or wrongful act committed by the employee when related to the duties of his or her job.").

¹⁵⁸ John Ashby, Note, Employment References: Should Employers Have an Affirmative Duty to Report Employee Misconduct to Inquiring Prospective Employers?, 46 ARIZ. L. REV. 117, 133-42 (2004).

¹⁵⁹ See Richland School Dist., 111 Wn.App. at 380-92.

¹⁶⁰ Id. at 392.

due to misrepresentation of the custodian’s employment record.¹⁶² Richland School contended that Mabton violated a duty to disclose the custodian’s reprimands and molestation charges under the theories of negligent misrepresentation or basic negligence.¹⁶³

The court noted that Washington has adopted two pertinent Restatement sections, § 551 which governs liability for the duty to disclose, and § 552 which governs liability for negligently providing false information; and then analyzed whether a former employer has a duty to disclose.

1. Liability for the Duty to Disclose.

Restatement § 551 sets out liability for failure to disclose.¹⁶⁴ The section reads in relevant part:

One who fails to disclose to another a fact that he knows may justifiably induce the other to act or refrain from acting in a business transaction is subject to the same liability ... as though he had represented the nonexistence of the matter that he has failed to disclose, if, but only if, he is under a duty to the other to exercise reasonable care to disclose the matter in question.¹⁶⁵

The Restatement further explains that a “party to a business transaction is under a duty to exercise reasonable care to disclose to the other...” when there are:

[M]atters known to him that the other is entitled to know because of a fiduciary or other similar relation of trust and confidence between them; and [there are] matters known to him that he knows to be necessary to prevent his partial or ambiguous statement of the facts from being misleading.¹⁶⁶

The Richland School court held that the duty to disclose applies only to a business transaction and arises primarily in a fiduciary relationship when there is a special relationship of trust and confidences between the parties, where one party relied on the specialized knowledge of the other, where a seller has knowledge of a material fact unknown to the buyer, or where

¹⁶¹ Id. at 383.

¹⁶² Id. at 384.

¹⁶³ Id. at 384-85.

¹⁶⁴ Id. at 385.

¹⁶⁵ Id. (emphasis added).

there is a statutory duty to disclose.¹⁶⁷ Upon review of these standards, the court held that a letter of recommendation from a former employer to a potential employer did not qualify as a business transaction involving a fiduciary relationship, and therefore could not be considered a negligent misrepresentation.¹⁶⁸

2. Liability for Negligently Providing False Information.

The Richland School court then noted that liability for false information negligently supplied is set forth in Restatement Section 552, which provides:

One who, in the course of his business, profession or employment, or in any other transaction in which he has a pecuniary interest, *supplies false information* for the guidance of others in their business transactions, is subject to liability for pecuniary loss caused to them by their justifiable *reliance* upon the information, if he fails to exercise reasonable care or competence in obtaining or communicating the information.¹⁶⁹

In applying this section, the Richland School court found that the Mabton School District did not negligently supply false information in its letters of recommendation.¹⁷⁰ Each letter simply extolled the former employee's virtues as a custodian without disclosing his child molestation charges. Further, none of the school officials responsible for hiring the employee testified as to the school district's *reliance* on the letters of recommendation, therefore, Richland School District failed to raise an issue of fact on *justifiable reliance* or on its claim that the

¹⁶⁶ Id. at 385-86.

¹⁶⁷ Id. at 386.

¹⁶⁸ Id. at 386-87. But see Kadlec Med. Ctr. v. Lakeview Anesthesia Assoc., No. 04-0997, 2005 U.S. Dist. LEXIS 10328, at *1 (E.D. La. May 19, 2005) (finding "duty to disclose exist[ed] [in claims for intentional misrepresentation, negligent misrepresentation, and negligence] absent a contractual or fiduciary relationship [where former employer provided a reference letter to prospective employer] because (1) defendant had a pecuniary interest, (2) third party [plaintiff] relied on misinformation supplied by the defendant, (3) plaintiff and defendant had a "special relationship" which existed in part to further communication between health care providers so that future patients could be protected," and (4) "policy considerations weigh[ed] heavily in favor of imposing a duty to disclose information related to a doctor's adverse employment history that risks death or bodily injury to future patients").

¹⁶⁹ Id. at 386 (emphasis added).

¹⁷⁰ Id. at 386.

former employer negligently provided false information.¹⁷¹ This case likely would have been decided differently if Mabton had provided false information that Richland School District then relied upon in hiring the custodian.

3. Liability for Common Law Negligence.

The Richland School court also considered whether Mabton had negligently breached a common law duty of care.¹⁷² While the court recognized that Mabton would be protected by a “common interest privilege,” that would have protected Mabton from any defamation suits if it had chosen to disclose any of the negative information about the custodian, the court declined to extend the privilege to create an affirmative duty to give accurate recommendations.¹⁷³ “[T]he privilege operates as a shield in cases involving slander, not as a sword[.]”¹⁷⁴ Therefore, the court held that Mabton owed no duty of care to disclose the custodian’s conduct.¹⁷⁵ Richland School cited several Washington Administrative Code sections in search of a duty of care, but the court held that such authority did not create an independent duty to disclose material facts in an employment recommendation.¹⁷⁶

C. **Defamation.**

An employee may sue for defamation if the employer or its supervisors share personal information about the employee with those who did *not* have a “need to know.” Defamation claims are also a concern for former employers when a prospective employer conducts a reference check. An employer may be sued by a former employee who learns that the ex-employer

¹⁷¹ Id.

¹⁷² Id. at 389-90.

¹⁷³ Id. at 390.

¹⁷⁴ Id.

¹⁷⁵ Id.

¹⁷⁶ Id. at 391.

provided a bad reference or disclosed negative information to others.¹⁷⁷ This is the reason why an employer should obtain a release from a prospective employee to encourage the sharing of information from former employers. Without said release, former employers are often reluctant to discuss former employees for fear of litigation. For example, in Dicomes v. State, the plaintiff sued for defamation where an employer responded to media inquiries regarding the termination of a “whistle-blowing” employee.¹⁷⁸

Defamation is a false, unprivileged communication that injures the reputation of the person about whom the communication was made.¹⁷⁹ Defamation *per se* exists if the publication injures a plaintiff’s business, trade, profession, or office.¹⁸⁰ There are similarities between defamation and the invasion of privacy tort of “false light” which occurs when an employer places an employee into a false light if such false light is highly offensive to a reasonable person and the employer intentionally or recklessly made such statement placing the employee in a false light.¹⁸¹ This tort was mentioned previously in the “Right of Privacy” section above. Theoretically, the difference between the two torts is that a defamation action is primarily concerned with compensating the injured party for damages to reputation, and the invasion of privacy action is primarily concerned with compensation for injured feelings or mental suffering. However, neither tort is limited to its theoretical basis of recovery.¹⁸² An employee may recover all actual or nominal damages under either theory.¹⁸³

Employer defamation was discussed in Henderson v. Pennwalt Corp where the plaintiff’s supervisor discussed with other supervisors the plaintiff’s sex life, promiscuity, and relationship

¹⁷⁷ See Dicomes, 113 Wn.2d 612.

¹⁷⁸ Id.

¹⁷⁹ Mark v. Seattle Times, 96 Wn.2d at 486.

¹⁸⁰ Caruso v. Local Union No. 690, 100 Wn.2d 343, 353 (1983).

¹⁸¹ Brink v. Griffith, 65 Wn.2d 253, 258-59 (1964).

¹⁸² Id. at 258.

with a coworker. The court held that, while comments between supervisors regarding an employee's work performance were privileged, conversations about an employee's personal life were not privileged. The employer could be vicariously liable for the supervisor's slander.¹⁸⁴

Employer defenses include truth, an employer's qualified privilege, which involves an employer acting without malice in providing truthful, job-related information in response to a legitimate inquiry, and employee consent. Statements made in the public interest are considered to be qualified privilege and within that privilege so long as they were made in good faith without knowledge or reckless disregard for the truth.¹⁸⁵ This conditional privilege extends to statements made in connection with the employer-employee relationship.¹⁸⁶ Thus, if the former employer criticizes the employee's work performance even though such criticism was generally unfounded, the qualified privilege may attach. This qualified privilege can be lost if the false statement is made with malice.¹⁸⁷ Malice means ill will or absence of good faith.¹⁸⁸ An employer acts recklessly if the employer or manager that gave a negative reference did not believe it was truthful or had no reasonable basis for believing it; or unnecessary or unreasonable repetition of the defamatory statement occurred; or the defamatory statement was made in bad faith. In other words, if the former employer knew the employee's performance was in fact good, but instead conveyed the opposite to the prospective employer, the employee may be able to recover from the former employer for defamation. At a minimum, the former employer may have to litigate its good faith if the applicant is not hired.

¹⁸³ Id.

¹⁸⁴ Henderson, 41 Wn. App. at 559.

¹⁸⁵ Bender v. Seattle, 99 Wn.2d 582, 601 (1983).

¹⁸⁶ Henderson, 41 Wn. App. at 559.

¹⁸⁷ See e.g., Jolly v. Valley Publishing Co., 63 Wn.2d 537, 542 (1964) (statements made to a prosecutor were considered to be privileged as long as they were made without malice, in good faith, and with an honest belief of their truth, arrived at after a fair and impartial investigation for such belief).

¹⁸⁸ Id. at 543.

Specific circumstances often determine whether a privilege exists. The court determines that a privilege exists when the matter that is publicized is one that both the publisher has an interest in, and one in which the party who the information is publicized to is reasonably believed to have a corresponding interest.¹⁸⁹ A Washington court found that an employer privilege did exist where two employees were discharged for illegal drug use in the employer's mines.¹⁹⁰ Drug use in the mines posed a severe safety hazard, and the court held that the employer's publication to coworkers of the reason for the plaintiffs' discharge was privileged because the employer and the employees had a common interest in the safety in the mines and in the employer's commitment to enforcing its workplace rules.¹⁹¹

There are circumstances in which an employer will be privileged to convey private information. Many former employees will seek unemployment benefits, and some will file charges of discrimination with federal and state agencies. The employer has a legal privilege to respond to these claims. Information given to these agencies generally cannot form the basis of a defamation claim, and is often considered to be absolutely privileged.¹⁹² Because that information may be discovered either through public disclosure laws or through written discovery in a lawsuit, employers must ensure that information is as accurate as possible.

Employers can protect against defamation actions involving disclosures to third parties. First, an employer should provide only truthful, job-related information. Second, an employer should verify to whom he or she is talking – e.g., by calling the employer to verify the inquirer's position or request written documentation, such as a letter on company letterhead. An employer should not provide references for former employees unless that former employee has provided a

¹⁸⁹ Messerly v. Asamera Minerals, 55 Wn. App. 811, 817 (1989) (questionable precedent on another issue).

¹⁹⁰ Id.

¹⁹¹ Id.

¹⁹² Hill v. J. C. Penney, 70 Wn. App. 225, 238-39, rev. denied, 122 Wn.2d 1023 (1993).

signed release and waiver of liability. If the employer provides only truthful, job-related information, in response to a legitimate inquiry, and has obtained an employee release and waiver, then the employer should have a strong defense against any defamation action.