

# EMPLOYEES' RIGHT TO PRIVACY IN WASHINGTON

By Nick Beermann

## I. Introduction

Employers may have a need to inquire into their employees' personal lives for such purposes as determining fitness for a particular position, ensuring productivity and preventing illegal activity in the workplace. Such inquiries often raise legal issues for public sector employees in Washington in light of state and federal constitutional provisions that grant citizens a right to privacy. Private employers use of employees' private information, however, also raises legal issues that private and public employers alike should be aware of. As one Washington court recently stated, "As to privacy of employees, employer-employee relations tend to be heavily regulated . . . ."<sup>1</sup>

The following article discusses these issues and provides a broad outline for employers to refer to when dealing with employee privacy.

### A. **The Constitutional Right to Privacy**

As creatures of statute, public employers are state actors subject to the constraints and protections of the State and Federal Constitutions. Article I, section 7 of the Washington Constitution provides that "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." The Fourth Amendment to the United States Constitution similarly protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." Both rules apply only to governmental entity intrusion into individual privacy and do not apply to private employers. Courts have interpreted Washington's Constitution as providing greater protection to citizens than the Fourth Amendment, but public employers should be aware of both.

Washington courts have interpreted Article I, section 7 of the Washington State Constitution as providing two rights of privacy to public employees: the right to nondisclosure of intimate personal information and the right to personal autonomy. The first of these rights (nondisclosure of intimate personal information) typically arises through issues about information that is routinely held in an employee's personnel file. For example, under state constitutional guidelines, a government entity could potentially be held liable for disclosing information such as medical information, addresses of individuals, phone numbers of individuals, names of family members of employees, records reflecting termination and leave, financial information and Social Security information.

The second right to privacy granted by Washington's Constitution is the right to personal autonomy. Under this right, public employers could potentially be held liable for such conduct as drug testing, pat-down searches of employees, employee locker or desk searches and other forms of employee monitoring.

---

<sup>1</sup> *Robinson v. City of Seattle*, 102 Wn. App. 795, 811, 10 P.2d 352 (2000).

Notwithstanding a public employee's right to privacy under the Washington Constitution, public employers will not be held accountable for unconstitutional invasion of employees' privacy where the employer has a compelling governmental interest in such invasion so long as any invasion is minimal and tailored to meet such interest. For example, pre-employment drug testing is a common function in many municipalities where the duties of a particular position implicate public safety such that there is potential harm to the public if such duties are performed by a person who abuses drugs. Thus, where municipalities identify a need to drug test employees for purposes of public safety and limit such testing to those employees who could directly harm the public, the employer can drug test employees without fear of liability. As evidenced by a recent Washington Supreme Court opinion, however, where a public employer subjects all of its employees to pre-employment drug testing but fails to offer evidence of the link between the need for drug testing and public safety for certain employees, the public employer's drug testing policy may be struck down as unconstitutional.<sup>2</sup>

In addition to drug testing, public employers may also have a compelling governmental interest (the most common being ensuring public safety) in workplace searches of employees or their personal effects. Public and private employers may also wish to search an employee's office, furniture, locker or possessions for reasons such as retrieving company property, eliminating illegal contraband, finding evidence of employee misconduct or searching for weapons.

There are no reported Washington court cases involving employee searches. But the United States Supreme Court has held that a public hospital violated an employee physician's right to privacy under the Fourth Amendment of the U.S. Constitution when it entered his office and removed personal items such as files and medical records while he was on administrative leave during a sexual harassment investigation. The Court reasoned that the search was unlawful because the physician had a "reasonable expectation of privacy" in his office, desk and files because of the manner in which the physician kept such materials.<sup>3</sup> Nevertheless, the Court stated that public employees' expectations of privacy in their offices, desks, and file cabinets, "may be reduced by virtue of actual office practices and procedures, or by legitimate regulation, so long as such regulation is reasonable."

Under Supreme Court guidelines, a search will be reasonable where (1) it is justified before it occurs, i.e. for work-related purposes such as job performance or for suspicions of employee misconduct; and (2) the search is reasonably related in scope to the circumstances that justified interference in the first place. In other words, employers cannot search for drugs under the guise of searching for a missing file.

Searches, however, need not be reasonable if the employee has no legitimate expectation of privacy in the area being searched. Under Supreme Court guidelines, employers may avoid having to articulate a valid reason for a search if it is firmly established and practiced that an employee has no reasonable expectation of privacy. Many employers have therefore adopted

---

<sup>2</sup> See *Robinson, supra* (determining that the City of Seattle failed to prove what duties implicating public safety necessitated drug testing all of its employees, including accountants, ushers and librarians and holding that the City's drug testing policy was unconstitutional).

<sup>3</sup> *O'Conner v. Ortega*, 480 U.S. 709 (1987).

policies to reduce the possibility of an employee claiming a reasonable expectation of privacy. The following is an example:

Information, possessions or objects stored or kept on or in the Employer's or clients' computers, network, equipment, voice mail, e-mail, on-line accounts, or in offices, desks, work stations, closets and other physical spaces within the firm or on firm property are subject to inspection by the firm without notice, and should not be considered private.

Employee monitoring is another form of search that could potentially violate the privacy rights granted employees under the state or federal constitutions. As with other searches, monitoring must be reasonably justified before it is undertaken and limited to the narrow purpose for which an employer implements it, unless an employee has no reasonable expectation of privacy. A sample general policy that eliminates an expectation of privacy in employee e-mail and voice mail is as follows:

You may be given access to the Employer's and the clients' computers, computer networks, software, on-line services, voice mail, electronic mail, offices, desks, workstations or other information recording devices. Your use of these items is solely for the Employer's benefit and no personal use of such items shall be permitted without prior Company approval. Company reserves the right to withdraw any approval it has given for personal use of the foregoing items, with or without notice. Any information, possessions, or objects stored or kept in or on any of the foregoing items or within the physical spaces of the Company or on Company property are subject to inspection by the Company without notice, and should not be considered private.

Neither of the foregoing policies will provide a public employer complete immunity from disgruntled employees claiming constitutional violations, but when combined with a consistent practice, such policies should assist public employees in reducing employees' expectation of privacy.

As can be seen by the foregoing examples, state and federal constitutional provisions grant public employees a right of privacy that public employers should consider when implementing policies that infringe on employees' personal lives. Such examples are by no means complete, and are only a sampling of the many aspects of privacy issues faced by public employers under the state and federal constitutions. As is discussed in the next section, in addition to the foregoing constitutional considerations, public employers are subject to a host of privacy regulations affecting all employers, public and private.

## **B. The Common-Law Right to Privacy**

Public and private employers alike may have heard employees claim that their privacy has been invaded without fully realizing what that statement means. Washington recognizes a theory of liability based on common law invasion of privacy. The right of privacy encompasses four

distinct kinds of invasion of four different interests, each of which represents an interference with the right to be left alone. The four torts are:

- Intrusion upon the plaintiff's seclusion or solitude, or into his or her private affairs;
- Public disclosure of embarrassing private facts about the plaintiff;
- Publicity which places the plaintiff in a false light in the public eye; and
- Appropriation for the defendant's advantage of the plaintiff's name or likeness.

Many employees' claims for common law invasion of privacy fall under the first three torts and typically arise through employer comments about former employees to former employees' potential employers or through what employees perceive to be an improper intrusion into the private affairs of the employee.

To be held liable for invasion of privacy, an employer must generally intend to harm an employee through public disclosure of information related to the employee, which must be conveyed to a substantial number of people, and be "highly offensive" to a reasonable person. While the majority of cases brought by aggrieved employees for invasion of privacy in Washington have failed, employers should nevertheless take care to ensure that communications regarding their employees to the public are screened for accuracy and do not convey information that an objective person would view as offensive or cast an employee in a false light. Additional steps employers may wish to consider to avoid invasion of privacy claims against them include:

- Limiting the information provided to potential employers of former employees about such former employees.
- Obtaining the consent of the employee prior to any publication or announcement regarding the employee to a third party.
- Not disclosing confidential medical information pertaining to an employee.
- Limiting the number of persons with access to an employee's personal information, such as that contained in an employee file.
- Ensuring that all employee records kept are accurate and up to date and permitting employees to inspect their employee files from time to time to ensure such accuracy.

### **C. Other Employment Privacy Considerations**

Constitutional and common-law rights to privacy are just one aspect of the regulatory scheme facing public and private employers alike. The following are additional regulations relating to employee privacy rights that Washington employers should consider.

## 1. The Public Disclosure Act (Only Pertains to Public Employers)

Public employers are subject to Washington's Public Disclosure Act, RCW 42.17, which requires that all public records be disclosed to persons requesting them, unless such records are exempt from disclosure. By broad definition, a public record includes employee records or employee information possessed by a public employer. If such records were to be disclosed, an employee could potentially have an invasion of privacy claim against the employer if the information conveyed satisfied one of the four prongs of the invasion of privacy torts discussed above. Fortunately, the Public Disclosure Act exempts from disclosure "personal information maintained for employees . . . or elected officials of any public agency to the extent that disclosure would violate their right to privacy."<sup>4</sup>

Courts examining what constitutes the right of privacy discussed in the Public Disclosure Act's exemption have stated that the right of privacy applies "only to the intimate details of one's personal and private life" or information that an employee would not normally share with strangers. Further assistance is provided by statute, which provides that disclosing information invades a person's right to privacy only if disclosure (1) would be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public.<sup>5</sup>

Not all employee records are exempt from public disclosure, even though they potentially fall under the exemption for employee records. For example, in a wrongful termination case in which the plaintiff sought "personnel evaluations and records of the performance and discipline of other employees," the court held that the records, with some deletions, should have been disclosed:

[N]ot all information contained in personnel evaluations and personnel records of school district employees is privileged; information about public, on-duty job performances should be disclosed. Deletion of the employees' names and identifying details would protect the privacy of employees.<sup>6</sup>

Another court held that the internal investigation files of several law enforcement agencies concerning complaints filed against police officers would not violate the officers' privacy: "Although the officers may be embarrassed by the release of their names in conjunction with the information in these files, the disclosure of the details of an officer's misconduct, while in the performance of his public duties, is not highly offensive."<sup>7</sup>

As indicated by the foregoing court decisions, not all employee records are exempt from disclosure by a public employer, despite employer concerns of liability premised on invasion of privacy. Court interpretations will vary depending on the material disclosed, the type of disclosure made, and the impact upon by public of such disclosure. Employers generally will have a qualified privilege to disclose employee information under the Public Disclosure Act upon a good faith belief that such disclosure does not violate an employee's right to privacy.

---

<sup>4</sup> RCW 42.17.310(b)

<sup>5</sup> RCW 42.17.255; *Cowles Pub'l Co. v. State Patrol*, 44 Wn. App. 882, 724 P.2d 379 (1986).

<sup>6</sup> *Ollie v. Highland School District 203*, 50 Wn. App. 639, 645, 749 P.2d 757, rev. denied, 110 Wn.2d 1040 (1988).

<sup>7</sup> *Cowles Pub'l Co. v. State Patrol*, 44 Wn. App. 882, 724 P.2d 379 (1986).

Nevertheless, employers should be aware of the Public Disclosure Act's requirements and its potential for interference with employee privacy rights.

## **2. More on Monitoring: Washington's Privacy Act, RCW 9.73**

As mentioned above, public and private employers alike have many reasons to monitor their employees, including to ensure sufficient employee performance and productivity, and to discourage illegal or unproductive conduct. To that end, many employers seek to monitor their employee phone and email communications. Doing so, however, may be illegal under Washington's Privacy Act, RCW 9.73. The Privacy Act states that it is unlawful to record "any private communication transmitted by telephone . . . radio or other device between two or more individuals using any device . . . designed to record and/or transmit said communication . . . without first obtaining the consent of all the participants in the communication."<sup>7</sup> The statute is considered one of the strictest in the nation. Violations create a private right of action for damages and attorney's fees, and evidence obtained in violation of the statute is inadmissible.

Courts interpreting the Privacy Act have held computer communications via email and Internet communications qualify for protection. Given that the plain language of the statute covers phone communications, an employer's recorded monitoring of employee email or telephone traffic will violate the statute unless the participants involved in the communication (the employee and the person the employee is communicating with), consent to such monitoring.

Under the statute, a party is deemed to have consented to a communication being recorded when another party has announced in an effective manner that the conversation would be recorded, or where a communicating party has consented to having his or her communication recorded. Courts have held that a person who calls someone else or sends an email will impliedly consent to recording based on their expectation that someone will either answer the communication or because the person expects to leave a message or email.<sup>8</sup> An employer will thus have the implied consent of a person who calls or emails the employer's employee. But to avoid violating the statute, an employer must also obtain the consent of the employee should it seek to monitor employee voice mail or email communications in compliance with the law. To do so, employers who seek to monitor their employees frequently draft policies warning employees that their communications may be subject to monitoring, or obtaining employees' express written consent upon hiring to communications monitoring. A sample policy might include the following:

You may be given access to the Employer's and the clients' computers, computer networks, software, on-line services, voice mail, electronic mail, offices, desks, workstations or other information recording devices. Your use of these items is solely for the Employer's benefit and no personal use of such items shall be permitted without prior Company approval. Company may monitor and record any communications you make or receive to or from third parties outside of the Company with or without prior notice to you.

---

<sup>7</sup> RCW 9.73.030(1)(a).

<sup>8</sup> *State v. Townsend*, 147 Wn.2d 666 (2002).

Before adopting a monitoring policy, employers should consider the costs involved, the effect such policy will have on employee morale, and whether to allow personal use of employer resources on the employees' own time. Employers should also be advised that *ad hoc* implementation of monitoring could give rise to discrimination claims as employers may be perceived as using such policy against employees on account of the employee's race, sex, union activities or other protected status. Thus, monitoring should be carefully considered in light of the context in which it occurs.

### **3. Privacy of Medical Information**

An additional area implicated by employee privacy rights in Washington is employer access to and disclosure of employee medical information. Employers have access to employee medical information for a number of reasons, such as physical capacity evaluations, worker's compensation information, disability information, or information obtained as a health plan administrator. However, collection and dissemination of such information may lead to violations of the Americans with Disabilities Act (the "ADA"), the common law right to privacy and, if the employer qualifies as a covered entity, the privacy regulations under the Health Insurance Portability and Accountability Act ("HIPAA").

The ADA generally requires employers to collect and maintain all information obtained from employee medical examinations and inquiries on separate forms, in separate medical files, as confidential medical records of the employee. The Equal Employment Opportunity Commission recommends that employers ensure the security of employees' medical information by (1) keeping the information in a file in a separate, locked cabinet, apart from personnel files; and (2) designating a specific person or persons to have access to the medical file. Exceptions to these rules exist for supervisory personnel who require access to a medical file to determine necessary work restrictions because of a disability, or for purposes of determining a reasonable accommodation.

Similar to the confidentiality requirements of the ADA, for employers qualifying as health plans (which includes self-insured entities) and medical practitioners who bill electronically, HIPAA's privacy and security regulations prohibit the disclosure of protected health information (including employee medical records maintained by an employer covered by HIPAA) without consent and require that such "covered entities" take certain steps to safeguard against unauthorized disclosure of such information. While the specific requirements of HIPAA are beyond the scope of this material, such requirements generally require that all health information be separated and accessed only by a limited number of persons so as to avoid disclosure.

To avoid potential discrimination claims under the ADA and liability under HIPAA<sup>9</sup>, employers should consider taking the following steps with respect to employee medical information:

- Keep employee medical and health information in a secure location, separate from the employee's personnel file.

---

<sup>9</sup> Given the scope of regulation under HIPAA, employers qualifying as covered entities under HIPAA should consult legal counsel regarding the requirements for HIPAA's privacy and security regulation compliance.

- Permit access to employee health and medical information only by a limited number of people or a point person.
- Obtain employee consent and authorization for disclosure.
- Provide employees written notice of the employer's privacy practices with respect to health information.
- Permit employees to access their own health information maintained by the employer.
- Adopt a clear policy and procedure for disclosure.

## **II. Conclusion**

In light of the amount of time employees spend at their jobs, and because of their own business reasons, employers frequently confront employee privacy issues that may raise legal implications. The foregoing article discusses some of the legal issues facing public and private employees with respect to the privacy rights of their employees and is by no means complete and should not be used a substitute for additional legal advice.

---

*Nick Beermann is an associate in the Labor & Employment Practice Group of the Seattle office of Ogden Murphy Wallace, P.L.L.C. He can be reached by email at [nbeermann@omwlaw.com](mailto:nbeermann@omwlaw.com) or by phone at (206) 447-7000. This article is a broad, general outline, and is not intended to provide legal advice, nor does it create an attorney-client relationship. For more information, contact Nick Beermann or another employment law attorney at Ogden Murphy Wallace, P.L.L.C.*