New technology and social media opportunities have opened a Pandora’s Box for employers and HR professionals. At work and at home, employees can access e-mail, the Internet, and social networking sites such as Twitter and Facebook, allowing them to work more efficiently and communicate more broadly. But it also creates a range of legal, moral and ethical dilemmas for employers as they strive to balance the legitimate need to know what is happening in the workplace with employee rights to privacy.

Can You Fire Someone Because of Online Conduct?

Given the prevalence of online activity, employers routinely discover objectionable conduct or communications by their employees on Twitter, blog postings, or Facebook pages. A worker may express dissatisfaction with work, pay, a manager or coworkers, post unprofessional photographs or reference getting drunk or being hung over at work. Perhaps more disconcerting is an employee disclosing confidential employer information.

For private (non governmental) and non-union employers who have engaged employees on an at-will basis, the default presumption is that an employee can be terminated for any reason or no reason, and certainly for disparaging the employer or its products, goofing off at work, being drunk at work, or for similar activities frequently tweeted or blogged about. However, there are exceptions to this general rule.

For example, in union and non-union workplaces, an employer may not interfere with an employee’s right to organize under the National Labor Relations Act, may not retaliate against a whistleblower or because the employee asserts his or her employment-related rights (for example, asking to be paid overtime) and may not discriminate against an employee because of his or her race, religion, age or other protected status.

Any time an online posting touches upon these potential risk factors, the employer must evaluate the risk before terminating or disciplining the employee. Although an objectionable and disrespectful tweet may not initially appear to implicate these concerns, closer consideration might show that the employee postings touch upon potentially protected issues.

For example, an employee may, in a moment of frustration, post that “my manager sucks and my company sucks. The room I work in is too cold, and they are so cheap they don’t even pay us for the time
it takes to get into our uniforms once we get to work. Me and my co-workers are signing a petition to complain.” A posting such as this should be analyzed to determine whether the employee may have a claim as a whistleblower or under the applicable wage and hour laws or under the union-organizing laws (the National Labor Relations Act).

**Vetting Job Applicants On Line**

Employers also must be careful in accessing job applicants’ online communications. Viewing personal web pages or blog posts to learn of a potential employee’s judgment or reputation may seem like a way to avoid hiring mistakes, but it puts employers at risk of exposure to information about an applicant’s protected class.

It would not be unusual to learn from a candidate’s blog or Facebook page, for example, that the candidate is a minority (which may not be obvious from having met the individual), a union activist, of a particular religion, planning to have children, has a disability or has filed workers’ compensation claims. Even if the employer does not base its hiring decision on these criteria, which would be illegal, simply learning such information renders the employer more vulnerable to discrimination claims.

Employers are struggling with how to articulate fair and uniform standards by which to evaluate online information about job candidates. An employer may take steps to screen the hiring decision-maker from protected class information embedded in social media. Employers can do this by outsourcing the task to a third party with instructions to screen out protected class information (or instructions to just provide information on limited criteria, e.g., evidence of illegal activity).

As an alternative, the employer can designate a “neutral” individual internally to research the candidate’s social networking information, screen out protected class information, and provide the remaining data to the decision-maker.

**Develop a Social Media Policy**

Although social media policies are in the news, relatively few companies actually have implemented them. A recent Ethics and Workplace Survey by Deloitte LLP showed that only 17 percent of employers have policies in place to examine and minimize potential risks to reputation related to use of social media. At the same time, almost half of employees surveyed stated that they regularly visit one or more social media sites four or more times per week. More than 53 percent of employees stated that “social networking pages are none of an employer’s business.”

A social media policy (and/or related training) can help educate employees on why it sometimes is the employer’s business to know what an employee is doing or saying online. Well thought-out policies and procedures may pay off by saving the employer time and expense of unwanted litigation in the future.

Leslie Bottomly (Portland, OR) and Kathy Feldman (Seattle, WA) are partners in Ater Wynne LLP’s Labor and Employment Group. Contact them at lgb@aterwynne.com or klf@aterwynne.com.