The United States does not have an overarching privacy law. Instead, privacy is protected by a combination and constellation of United States Constitutional provisions, primarily the Fourth Amendment protection against unreasonable searches and seizures by the government; privacy provisions in state constitutions; statutes that are sector and technology specific, such as protections against electronic monitoring and legislation covering medical, banking, video, student and other privacy realms; private contracts, including union contracts, and terms and conditions of electronic use and access; and company-sponsored privacy standards for customers and employees. Our law draws a distinction between private and public employees and also has the added complication that privacy issues are dealt with under both federal and state law.

Courts are constantly resolving how these protections apply in the rapidly changing world of social media, while the federal and state governments consider responsive legislation. The general benchmark courts use is whether there is a “reasonable expectation of privacy,” a principle that may cabin privacy claims where material has been turned over to third parties or publicly disclosed. This summary provides an overview of the current state of employee data privacy, focusing on federal protections for *private* sector employees.

[1] Does your country have laws or regulations that protect the confidentiality of electronic communications?

At the federal level, the privacy of electronic communications is predominantly protected by the Electronic Communications Privacy Act of 1986 (“ECPA”). Two major sections impact an employer’s rights to monitor employees’ private electronic communications: Title I, the Wiretap Act, prohibits intentional
interception of electronic communications while in transmission; Title II, the Stored Communications Act (“SCA”), prohibits intentional unauthorized access to stored communications. 18 U.S.C. §§ 2510–2522. Certain exceptions to these prohibitions give employers rights to review employee communications: under the consent and course of business exceptions, employers can monitor both in-transit and stored communications where one of the involved parties has consented to the access, or where the communications occur in the normal course of business; under the provider exception, an employer can also access any information stored on its system, if such access is necessary to protect its rights as the provider of the electronic service. 18 U.S.C. §§ 2510(5)(a), 2511(2)(d), 2701(c)(1). These exceptions give employers rights to monitor electronic communications sent via employer-owned computers or networks.

The federal Computer Fraud and Abuse Act (“CFAA”) provides an additional layer of protection to employees, prohibiting any access without authorization to most computers, networks or sites that results in damage or loss. 18 U.S.C. § 1030. Accordingly, employers arguably may be liable under the CFAA if they access an employee’s private email or social media accounts without authorization. See, e.g., Glob. Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 631, 636 (E.D. Va. 2009).

[2] If so, are these provisions applicable to electronic communications related to social networks or blogs?

The ECPA and CFAA do not expressly address social media networks or sites. However, in the few cases interpreting the Acts’ application to social media, courts have generally held that their protections extend to non-public social media pages, such as personal Facebook or Twitter accounts. See, e.g., Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 666 (D.N.J. 2013) (holding that non-public Facebook wall posts are covered by the SCA); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010) (holding that MySpace and Facebook wall postings and comments are subject to the ECPA’s protections).

The United States Supreme Court has yet to weigh in on issues related to social media and employee rights. However, in City of Ontario v. Quon, 130 S. Ct. 2619 (2010), the Court held that an employer did not violate the employee’s right to privacy by monitoring text messages sent during work hours on an employer-provided device. Notably, the Court was reluctant to make a broad pronouncement
and said that “[a] broad holding concerning employees’ privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.” Id. at 2630.

[3] If so, are these provisions applicable when information is collected on social networks or blogs during recruitment? In the course of employment for disciplinary or other reasons?

United States federal law places no universal restriction on the ability of employers to monitor publicly accessible social media sites when assessing job candidates, or reviewing employees for disciplinary action. However, such review is illegal if founded on discrimination based on race, national origin, marital status, sex, age, disability, or religion. (State laws often add gender identity and sexual orientation to this list.) The Equal Employment Opportunity Commission has warned against the discriminatory impact caused by Internet screening. Further, third-party recruiters that perform social network screening may be subject to liability under the Fair Credit Reporting Act, 15 U.S.C. § 1681.

Employers could potentially face liability under the ECPA, CFAA and state laws if they access an employee’s private social media accounts without the employee’s permission. Even with the employee’s permission, an employer may violate federal or state law by accessing a private social media account. Some courts have held that access in violation of a service provider’s terms of service is prohibited by the CFAA. Several states have also enacted legislation prohibiting employers from requiring, or even requesting, that an employee or job applicant disclose a user name or password for a personal social media account, though some states provide an exception where the employer has a reasonable belief that the employee’s activity on the site relates to work-related misconduct or illegal activity. See, e.g., Cal. Lab. Code § 980. Several federal measures that protect employee rights in their on-line credentials were introduced in Congress, including the Social Networking Online Protection Act and the Password Protection Act, but have yet to become law.

Because most employment in the United States is at will, employers can generally end employment relationships at any time without notice or reason, subject to anti-discrimination laws. No federal laws protect employees from termination or hiring decisions based on social networking activities. Employees or candidates may raise, however, a potential claim if employers base their hiring or disciplinary
decision on certain prohibited grounds under federal discrimination, whistle-
blower protections, and labor laws. A majority of states have legislation that
prohibits adverse employment actions predicated on off-duty conduct or lifestyle,
including activity on social networking sites, unless the activity can be shown to
damage the company in some way. See, e.g., Cal. Lab. Code §§ 96(k), 98.6.

[4] Are employees allowed to use social networks during work hours? If so, in
what way?

Use of the employer’s computer during work hours is generally regulated by the
employer and there is no affirmative right to undertake personal activities during
work hours. As to non-work hours, companies can implement policies that
regulate employee conduct on social media sites to some extent. For example,
companies may prohibit their employees from making disparaging remarks
concerning the company or other employees or clients. Certain types of speech are
protected, however, including speech concerning wages, work conditions and other
“concerted activity” for the purpose of collective bargaining, mutual aid or

[5] Can an employer monitor the use of social networks by employees during
work hours? Outside of work hours?

Federal law generally does not prohibit private employers from monitoring
employee Internet activity either during or outside of work hours, though some
union contracts or state laws may place other limitations. Employees may find
refuge based on state constitutional provisions or privacy torts under state law
where the employer intruded on the employee’s reasonable expectation of privacy.
This expectation generally does not exist where the device is owned and issued by
the employer, or when the employer has a policy regarding monitoring or Internet
use, and the employee is accessing public Internet forums. However, just as non-
electronic monitoring and eavesdropping may be prohibited to the extent it
constitutes an unfair labor practice, the same principle could be applied to social
media. The law is less clear concerning personal content on websites with
restrictive access settings.

In light of the changing patchwork of privacy laws and the constantly changing
nature of social media, employers are encouraged to adopt social media policies.
Resources


Michael T. Zugelder, *The Legal Limitations on Employers’ Right to Access and Control Employees’ Social Media*, 20 No. 4 HR Advisor: Legal & Practical Guidance ART 3 (July/August 2014)

1 Empl. Privacy Law § A:22