Employee Data Privacy – United States

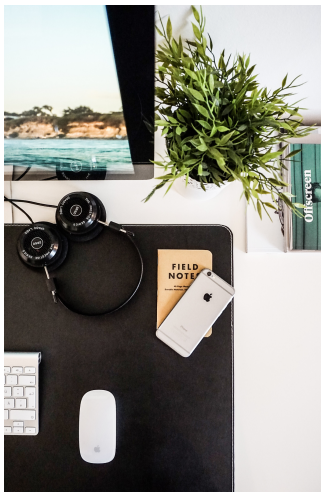
Data Privacy Laws and Regulations

What laws apply to the collection and use of individuals' personal information?

Data privacy laws have become more prominent in recent years. As the amount of personal information available online has grown substantially, there has been an enhanced focus on the processing of personal data, as well as the enforcement of such laws.

There is no overarching national law with respect to employee privacy in the United States. Rather, employers are subject to a patchwork of federal and state laws, depending on the type of information and particular context described:

Background Reports: In order to request background check reports on applicants or employees from consumer reporting agencies, companies need to comply with the requirements of the Fair Credit Reporting Act (FCRA) and state laws. Before obtaining such a report, an employer must get the individual's consent using a stand-alone form with a clear and conspicuous disclosure that the employer may use the report for decisions related to employment. The individual must give their written authorization for the employer to procure the report.



If an adverse action will be taken based on the results of the report, notify the individual in advance of taking the adverse action. This includes giving the individual a copy of the consumer report and a copy of "A Summary of Your Rights Under the Fair Credit Reporting Act," along with any state required notice.

Finally, after adverse an action is taken (if applicable), give the applicant or employee a final adverse action notice, including the identity and contact information for the source of the report, a statement that that entity (i.e. the background check vendor) did not take the adverse action and cannot explain why it was taken, and a notice of the right to dispute accuracy or completeness and to get an additional free copy of the report within 60 days.

Criminal History: Many states, cities and counties have enacted laws which prohibit employers from asking applicants about criminal history on job applications (aka ban-the-box). These laws require that employers wait until later in the recruiting process before asking applicants about their criminal history or conducting background checks. In certain cases, these laws require that employers wait until after the conditional offer of employment before obtaining information from any source about a job applicant's criminal history.

Credit Checks: Some states and cities have a general prohibition on giving employers access to a job applicant's credit history. These laws contain varying exceptions for different categories of employees, such as employees with: significant supervisory authority, access to confidential business information, the authority to execute contracts or, engage in significant financial transactions.

Drug Tests: Several states require employers to provide notice and/or obtain the individual's consent before conducting drug tests on applicants and employees. In addition, the Federal Motor Carrier Safety Administration has established requirements for conducting drug tests in the trucking industry.

Employee Monitoring: The Federal Wiretap Act (18 USC § 2510-22) and state corollaries, generally prohibit the interception, or real-time capture of wire, electronic or oral communications without the consent of at least one party to the communication.

Workplace monitoring can constitute an interception for purposes of federal and state wiretap laws (For example, keystroke logging, screenshot capture, and monitoring telephone calls). Employers should obtain employee consent to real-time monitoring techniques, and, when legally required, the consent of all parties to the communication. The level of consent that is necessary can vary based on the type of monitoring.

Note that under decisions from the National Labor Relations Board (NLRB), use of video surveillance in the workplace can be a subject of mandatory collective bargaining, and must be addressed with a labor union, if applicable (e.g., Colgate-Palmolive Co., 323 NLRB 515, 515 (1997) (holding that use of hidden cameras in the workplace is sufficiently "germane to the work environment and outside the scope of managerial decisions lying at the core of entrepreneurial control" as to require an employer to bargain over them)).

Employee electronic monitoring becoming more common are also subject to states laws. In Delaware and Connecticut, employers are required to provide notice of electronic monitoring to employees (e.g., 19 Del. C. § 705; Sec. 31-48d).

Social Security Numbers (SSNs): Laws in many states require companies to take extra care when collecting and using SSNs (e.g., Cal. Civ. Code § 1789.85; NY Gen. Bus. Law § 388-ddd; N.Y.S. Lab. Law § 203-d). When companies collect SSNs, they are generally required to:

- never publicly post SSNs;
- avoid transmission of SSNs over the internet, unless through an encrypted secure connection;
- not use SSNs as an account number or other regular identifier; and,
- limit printing SSNs on hard copy documents where possible and ensure that any hard copy documents with SSNs are properly disposed of through cross-shredding or similar methods.

Biometric Information: Laws in certain states limit collection and use of biometric information. The Illinois Biometric Information Privacy Act and Texas Biometric Information Privacy Act:

- require a written policy which sets out the retention schedule for the information (no longer than three years after the individual's last interaction with the business) and guidelines for destruction;
- require notice and express written individual consent, in advance of biometric information being collected;
- prohibit the sale of information; and,
- require the employer to protect biometric information as it would protect other confidential and sensitive information.

Health Information: Under the federal Health Insurance Portability and Accountability Act (HIPAA), Family and Medical Leave Act (FMLA), Americans with Disabilities Act (ADA) and Genetic Information Nondiscrimination Act (GINA), employers must maintain the confidentiality of certain health-related information and limit access to a need-to-know basis.

The changing data protection landscape

A number of states have taken steps towards developing broad data privacy laws to protect "consumer" data. California, Colorado, Utah and Virginia have each enacted data protection laws which become effective in 2023, and Iowa has also enacted a broad data protection law which goes into effect January 1, 2025. There have also been efforts to enact an overarching data privacy law at the federal level. The definition of "consumer" in these data privacy bills vary, with some proposals specifically exempting employee data used in the employment context.

California was the first state to implement a broad privacy law, the California Consumer Privacy Act (CCPA). The CCPA established several consumer rights for California residents, including the right to: (a) know about the personal information (PI) collected by a covered business about an consumer, the sources of the information, the purpose for use, and the third parties (if any) to whom the PI is disclosed; (b) opt-out of the sale of personal information; and (c) request the deletion of personal information collected and maintained by the business.

In October 2019, the CCPA was amended to exclude personal information that is used solely for employment purposes (i.e., recruiting information from applicants, personal information from employees for payroll and HR, etc.) from most CCPA requirements and rights. Covered businesses are still required to provide a "notice at collection" to applicants, employees, contractors, and board members that describes the categories of PI to be collected and how that information will be used.

In November 2020, the California Privacy Rights and Enforcement Act (CPRA) was approved and amends the CCPA. Effective January 1, 2023, the CPRA, in its entirety, applies to all human resources data and provides additional privacy rights to individuals which include the right to correct personal information that has been collected from the individual, the right to limit the use and disclosure of sensitive personal information, and the right to opt out of sharing personal information. The CPRA also imposes vendor contracting requirements and creates a California agency dedicated to enforcing privacy rights.

The Federal Trade Commission (FTC) is the primary regulator of consumer data at the federal level through its use of Section 5 of the FTC Act, which prohibits unfair or deceptive trade practices. The FTC has charged companies victimized by data breaches with unfair or deceptive trade practices on the theory that the security breaches were the result of the failure to live up to representations about information in the company's privacy policy or to adopt reasonable security measures for personal information. The companies targeted by the FTC in these cases run the gamut from healthcare to hospitality to retailers.

Last updated May 2023.