Data Privacy Laws Zeroing in on Employees' Rights

Data privacy continues to be a primary focus of several recently enacted or amended state laws. Employees' right to privacy is of particular interest in light of the various ways personnel can maintain connectivity to the digital world throughout the workday. The ease of which applications and devices track, collect and process personal information warrants the need to establish clearly defined rules for acceptable employment practices that comply with applicable data privacy laws. In recent years, there has been a notable expansion of employee data privacy rights with the proliferation of employment-related privacy laws and increased recognition of employee privacy by companies. This is especially evident through the enactment of state employee monitoring laws, the expiration of the employer exemption under the California Consumer Privacy Act (CCPA) and the implementation of employee specific privacy policies.

Employee Monitoring

States are trending towards increasing transparency and privacy in the workplace by passing laws that require employers to notify employees if they are monitoring them.

In May of 2022, New York became one of the latest states to recognize the importance of employee privacy through the enactment of its employee monitoring law. The law requires private employers with a place of business in New York to provide employees with written notice if the employer monitors or intercepts employee emails, internet access or usage, or telephone conversations. The written notice must communicate that "any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system . . . may be subject to monitoring at any and all times by any lawful means." For information on New York's electronic monitoring law, you can read our prior blog post here.

New York followed the lead of Connecticut and Delaware, both of which have enacted similar employee monitoring laws. Along the same lines, in Texas, employer monitoring of employee electronic communications is considered an invasion of privacy. An employer may monitor its own phone system in order to ensure that employees are using the system for its intended purposes. However, employers must inform employees that this monitoring may be taking place.

Based on these efforts, it is likely that other states will follow the trend and pass legislation that seeks to limit and/or require notice to employees of monitoring activities taking place in the workplace.

Employee Data Under the CCPA

Since California enacted the CCPA in 2018, employers have been taking note to see how the law will apply to data collected and maintained about their employees. Until now, employment data has been specifically exempt from most of the CCPA's requirements. However, as a result of amendments to the CCPA contained in the California Privacy Rights Act (CPRA) that went into effect Jan. 1, 2023, many categories of employee data are now subject to the CCPA's requirements. Employers will now have to

comply with certain obligations with respect to processing employee data.

Beginning in 2023, the CCPA broadly applies to employee data. Employee data will now be treated as any other commercial information, and covered employers will need to add employee and human resources data to their ongoing compliance efforts. In the employment context, personal information could include an employee's contact information, insurance and benefits elections, bank and direct deposit information, emergency contacts, dependents, resume and employment history, performance evaluations, wage statements, time punch records, stock and equity grants, compensation history and many other forms of data routinely collected throughout the employment relationship. Moreover, the CPRA introduces the concept of "sensitive personal information," which includes financial information, social security numbers, communications content, health information and biometrics, that must now be considered and addressed by the employer.

In order to comply with the CPRA, employers must prepare and provide a privacy notice to an employee or job applicant at or before the time personal information is collected, entered into specific data processing agreement with vendors, respect employee rights requests pursuant to CCPA with regards to their personal data, as well as other compliance steps.

For more information about the amendments contained in the CPRA, you can read our prior blog post here.

Employee Specific Privacy Policies

As privacy continues to be of growing concern among businesses, employees and consumers, it is imperative that employers adopt comprehensive and robust policies about privacy to let their employees know how their personal data will be collected, processed, stored and shared. These policies are essential for any company that requires the use and disclosure of an employee's personal data for business purposes. Important employee privacy policies include general employee privacy policies, bring your own device policies, acceptable use policies, employee monitoring policies and biometric collection policies, to name a few. These policies increase transparency between the employer and employees, as well as set privacy expectations for employees.

Most often, employee privacy policies are implemented as a means to comply with applicable workplace privacy regulations and legal requirements, such as those under the CCPA/CPRA and any state employee monitoring laws mentioned above. For example, the Illinois Second District Court of Appeals recently held that Illinois' Biometric Information Privacy Act (BIPA) requires private entities to publish written data retention and destruction policies simultaneously or prior to collecting biometric data, and in certain circumstances to receive employee consent prior to collection.

Effective policies should define what constitutes personal information and the means by which it may be collected. Further, the policy should clearly stipulate situations in which an employee should not assume that their data or communications are private. For example, an employee does not have a reasonable expectation of privacy in phone calls, texts, emails and social media communications that are transmitted on company-owned equipment. Similarly, software and websites that are not required for business purposes may be restricted according to the policy or blocked to prevent any issues. The policy should also specify under what conditions employee data will be disclosed.

In 2022 and heading into 2023, legislative developments and the increased individual awareness

about personal data privacy are emphasizing the importance of employee privacy efforts. Employers must be aware of the evolving legal landscape that is increasing recognition of employee privacy and remain up to date on any new obligations that may result.

If you have any questions about the above or employee privacy, please contact Gianelle Duby; Amber Lawyer, CIPP/US & CIPP/E; Shannon Knapp, CIPP/US; or any attorney in Bond's cybersecurity and data privacy practice.