Complying with New York's Recently Adopted Employee Privacy Law

March 28, 2024

On March 12, 2024, a new privacy law for employees and job applicants went into effect in New York, prohibiting employers, in certain circumstances, from requesting or requiring access to an employee's or applicant's "personal account," such as an account on a social media platform. In passing Assembly Bill 836 ("A836"), New York joins a number of other states, including California, Connecticut, Colorado, Illinois, Michigan, and New Jersey, that have passed laws regulating access to employees' and applicants' personal social media accounts.

While the law places restrictions on employers' ability to request or require access to personal accounts of employees, it is limited in scope to purely personal accounts and contains important exceptions. For example, the law includes specific exceptions related to regulatory compliance that will allow employers to monitor and retain employee communications as necessary under federal law, including under regulators' recordkeeping requirements, which have been the focus of ongoing sweep investigations by the SEC and CFTC into the use of off-channel communications at registered broker-dealers and investment advisers. Still, employers should carefully evaluate the scope and structure of their internal policies and procedures to ensure that they are in compliance with this new statute.

Overview of the Law

On September 14, 2023, New York Governor Kathy Hochul signed into law A836, which adds Section 201-i to the New York Labor Law and prohibits employers from requesting, requiring, or coercing any current employees or job applicants to "disclose any username and password, password, or other authentication information for accessing a personal account through an electronic communications device." The law also prohibits requiring access to the personal account in the presence of the employer and reproducing information obtained from the personal account through prohibited means.

Under the new law, employers may not penalize or threaten to penalize an employee for his or her refusal to disclose any of the information specified above. Furthermore,

employers cannot refuse to hire any job applicant as a result of the applicant's refusal to disclose such information.

"Personal account" is defined under the statute as "an account or profile on an electronic medium where users may create, share, and view user-generated content, including uploading or downloading videos or still photographs, blogs, video blogs, podcasts, instant messages or internet website profiles or locations that is used by an employee or an applicant exclusively for personal purposes." Importantly, A836 applies only to purely personal accounts, and it does not prohibit the collection of communications made using business applications or mixed-use personal accounts containing both business and personal communications. Therefore, employers have a right to access employees' accounts that are used for business purposes on an employer-issued device, though employers do not have a right to access purely personal accounts on these devices unless one of the exceptions discussed below applies.

Notably, the statute does not specifically mention that it applies to personal text, mobile messaging or email accounts utilized on employees' personal devices. A plain reading of the statute would indicate that it does not apply to such accounts, though there is some ambiguity based on statements by the bill's sponsor regarding the need to protect "login information to email accounts and other extremely personal accounts."[1] Regardless, as noted, A836 applies only to purely personal accounts, which means that it does not prohibit the collection of communications made using business applications or mixed-use personal accounts containing both business and personal communications. Therefore, an employer could undertake such a collection in connection with legal matters such as litigation, regulatory responses, or investigations. Furthermore, the statute provides an affirmative defense if the employer is acting "to comply with requirements of a federal, state or local law." For these reasons, employers will still be able to access messages sent or received on mixed-use personal platforms when responding to SEC or DOJ subpoenas or conducting internal investigations.

Exceptions to the Law

There are a number of exceptions to this prohibition that allow an employer to access personal electronic devices and accounts of employees in certain scenarios, including:

- requesting or requiring employees to disclose access information to an account provided by the employer where the account is used for business purposes and prior

[1] "Governor Hochul Signs Legislation to Strengthen Workers' Rights in New York State" (Sept. 14, 2023), https://www.governor.ny.gov/news/governor-hochul-signs-legislation-strengthen-workers-rights-new-york-state.

notice was given to the employee of "the employer's right to request or require such access information";

- requesting or requiring employees "to disclose access information to an account known to an employer to be used for business purposes," even if that account was not provided by the employer;

- accessing electronic communications in order to comply with a duty to "monitor or retain employee communications that is established under federal law or by a self regulatory organization"; and

- accessing an account to comply with a court order.

Notably, the new law expressly does not preclude employers from accessing or utilizing information about an employee or applicant that is publicly available or that can be obtained without asking the employee for information or access. The law also does not prohibit an employee or applicant from voluntarily sharing information with an employer in connection with reports of misconduct or investigating misconduct.

Recommended Actions for Employers

- New York employers should carefully review their policies and procedures to ensure that they address the lawful circumstances in which the employer may access employees' personal accounts or electronic communications.

- Employers should ensure that all human resources professionals, hiring managers and those employees conducting internal investigations are made aware of such policies and procedures.

- Employers should take steps to mitigate the risk of inadvertently accessing purely personal accounts or communications of employees by establishing clear protocols prior to any internal investigation or review.

- Employers should take steps to document in writing the voluntary nature of any disclosures of personal account information made in connection with any investigation of misconduct.

* * *

Please do not hesitate to contact us with any questions.

Helen V. Cantwell
Partner, New York
+1 212 909 6312
hcantwell@debevoise.com

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandra@debevoise.com

Jyotin Hamid
Partner, New York
+1 212 909 1031
jhamid@debevoise.com

Arian M. June
Partner, Washington, D.C.
+1 202 383 8053
ajune@debevoise.com

Tricia Bozyk Sherno
Counsel, New York
+1 212 909 6717
tbsherno@debevoise.com

Johanna N. Skrzypczyk
Counsel, New York
+1 212 909 6291
jnskrzypczyk@debevoise.com

Andrew Stamboulidis
Associate, New York
+1 212 909 6833
astamboulidis@debevoise.com