Protecting Workplace Privacy In The New Age Of Social Media

By **Christina Wabiszewski and Kimberly Henrickson** (March 30, 2023)

Christina Wabiszewski

Kimberly Henrickson

The newest and hottest forms of social media — TikTok and BeReal — pose similar risks to an employer's workplace as did the older forms, like Snapchat, Instagram and Facebook.

Namely, that employees can unintentionally, or intentionally, expose confidential or private information to their followers.

While TikTok Inc.'s CEO Shou Zi Chew last week during a day-long congressional hearing repeatedly denied his company's app shares data or has connections with the Chinese Communist Party and argued the platform ensured safety for its 150 million American users, Congress and U.S. intelligence sources have expressed little confidence in these assertions.

Moreover, unique to TikTok and BeReal is their position to incentivize users to share workplace content.

One popular TikTok trend over the last few years has been "a day in my life" content, in which users show curated snippets of otherwise average days.

Many videos prominently feature the workplace, showing laptop screens, colleagues and offices. During the recent bout of technology industry layoffs, many users posted videos of the days they were laid off, exposing the difference between workplace reality and the romanticized posts that are far more typical.[1]

Comparatively, BeReal limits users to one post per day, with a notification going off at a different time every day, prompting users to post two simultaneously taken photos from the front and back cameras on their phones.[2]

Due to BeReal's emphasis on immediacy, when the notification goes off during the workday, many times BeReal shots feature an image of an employee on the back view, and, most concerning, their computer screen on the front.

The rise of TikTok and BeReal merits a reminder to employers to ensure that their social media policies protect both their and their employee's confidential and private information, while taking into account key legal risks brought to light by these platforms and issues surrounding the enforceability of these policies.

Being Real About Social Media and the NLRB

If an employer institutes a policy prohibiting employees from featuring their workplace or work materials in TikToks and BeReals, the employer must be able to justify the policy under the latest National Labor Relations Board case law.

In their 2017 The Boeing Company decision, the NLRB determined that when evaluating employer policies that could reasonably be interpreted to interfere with employee rights under the National Labor Relations Act, it would look at the nature and extent of the

potential impact on NLRA rights and the employer's legitimate justifications associated with the rule.[3]

More recently, applying their 2021 decision in Medic Ambulance Service Inc., the NRLB upheld an employer's policy prohibiting employees on social media from engaging in inappropriate communications, disclosing confidential information, using the employer's name to denigrate or disparage causes or people, and posting photos of coworkers.[4]

That decision explained that the nondisclosure in the social media policy requirements at hand met the Boeing factors because it referenced copyrighted or trademarked information and trade secrets rather than information traditionally associated with Section 7 rights like employees' contact information, wages, or other terms and conditions of employment.

Similarly, the prohibition on posting photos of coworkers without their consent and from posting pictures of company-owned equipment without prior written permission clearly was permissible because it was linked to protecting the company's confidentiality interests and employees' privacy interests.

However, as the current NLRB general counsel Jennifer A. Abruzzo noted in a 2021 memo, the NLRB is expected to continue striking down employer-protective rulings that were instituted during the Trump administration and more generally narrow employer protections.[5]

Thus, it is likely that even narrowly tailored social media policies can be viewed as violative of the NLRA in the future.

The board's recent decision in McLaren Macomb,[6] which prohibited, among other things, confidentiality and nondisparagement clauses in severance agreements, is a timely reminder of the Biden board's renewed emphasis on employee rights.

In light of these rulings and possible changes to board law in the near term, key considerations for drafting enforceable social media policies applying to unionized workforces include:

- Avoid broad-stroke prohibitions that could be interpreted to restrict Section 7 activities, such as prohibitions on discussions of wages and benefits with coworkers, as well as discussions about improving the terms and conditions of employment.

- Focus instead on prohibiting employees from taking photos of valuable and confidential information. Spell out the explicit business reasons why social media recordings by an employee are damaging to the business and, therefore, prohibited.

- Include a National Labor Relations Act savings clause that provides the policies do not impede and are not intended to impede employees' Section 7 rights.

No Such Thing As Private Settings When It Comes to Employee Privacy

Employers should also consider whether apps like BeReal and TikTok expose them to heightened legal risks under state biometric privacy laws, such as the Illinois Biometric Information Privacy Act.

Recently, in Cothron v. White Castle System Inc. in February, the Illinois Supreme Court held that claims under BIPA accrue on every scan or collection of biometric information and allowed per-scan damages to employees, meaning employers face huge liability exposure for continuous violations of the act.[7]

Additionally, in a 2022 case, Ronquillo v. Doctor's Associates LLC, the U.S. District Court for the Northern District of Illinois held that BIPA applies even to third parties that collect biometric information under the act.[8]

TikTok's privacy policy specifically provides that it collects biometric info, including "biometric identifiers and biometric information as defined under U.S. laws, such as face-prints and voiceprints."

Although TikTok has recently settled a class action for violating BIPA, courts have not considered BIPA in light of an employer's obligations to employees using TikTok over its systems.

Given the ever-increasing list of pro-plaintiff decisions under BIPA, risk of liability is very real for employers that permit employees to use these apps over employer systems and devices or require employees to use company-sponsored accounts.

While federal and state government entities are drawing attention to the security risks these apps pose, private employers lag behind.

Key considerations for drafting social media policies targeted at restricting risk for privacy law violations may include:

- Prohibiting the use of social media apps that collect biometric information on company systems and devices — such a measure has the added benefit of protecting company confidential information and trade secrets from an unintentional disclosure.

- If TikTok and BeReal are essential components, for example, of your business' marketing and public relations outreach programs, consider requiring BIPA-compliant written consent from or notification to employees who use the company's accounts on these platforms.[9]

Conclusion

Just like the apps themselves, the law on social media use, employee privacy and confidentiality is in constant flux these days.

Narrowly and carefully drafting social media policies that anticipate further developments in all these arenas is critical to protecting an employer's legitimate business interests.

Employers who have not recently reviewed their social media policies to ensure legal compliance should consider doing so.

Christina Wabiszewski and Kimberly Henrickson are associates at Foley & Lardner LLP.

[1] https://www.nytimes.com/2023/03/01/magazine/what-does-workplace-tiktok-look-like-during-layoffs-it-gets-weird.html.

[2] https://www.nytimes.com/2022/05/10/style/bereal-app-social-media.html.

[3] https://apps.nlrb.gov/link/document.aspx/09031d458263fae2.

[4] https://apps.nlrb.gov/link/document.aspx/09031d45833291e3.

[5] https://apps.nlrb.gov/link/document.aspx/09031d4583506e0c.

[6] https://www.foley.com/en/insights/publications/2023/02/strictly-confidential-labor-board-flip-flops-again.

[7] https://www.foley.com/en/insights/publications/2023/02/bipa-potential-billion-dollar-exposure-illinois.

[8] https://casetext.com/case/ronquillo-v-doctors-assocs.

[9] More information on drafting BIPA compliant policies was recently addressed here: https://www.foley.com/en/insights/publications/2022/12/biometric-information-adopt-biometric-policy-now.