LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
THURSDAY, MARCH 7, 2024

BYOD: Internal investigations and employee personal devices

By Winston Y. Chan and Nicole Waddick

This art was created with the assistance of Shutterstock AI tools

In March 2023, the U.S. Department of Justice (DOJ) announced new guidance regarding its consideration of company device policies in its Evaluation of Corporate Compliance Programs (ECCP). The new guidance, which directs prosecutors to consider companies' device policies in their investigations and charging decisions, necessarily shapes how companies and their counsel understand compliance and effective internal investigations. To ensure effective compliance systems, it is critical for companies and their counsel to understand when and how they may access employee devices, what is entailed in an effective device policy, and what options exist to examine employees' business communications in the event that company device policies do not set out a clear process for doing so.

The law - when can companies access employee devices?

The law on access to employee devices delineates between employer- and employee-provided devices. While the exact contours of the law vary between jurisdictions, employers are generally free to search and review employer-provided devices. *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010); *Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026 (N.D. Cal. 2014). For the purposes of internal investigations, this means that companies may generally search and image employer-provided devices to identify potential concerns relating to misconduct. *See e.g., Sunbelt Rentals*, F. Supp. 3; California Office of the Attorney General, *Work-place Privacy*, https://oag.ca.gov/privacy/workplace-privacy.

On the other hand, employee-owned or personal devices do not necessarily afford companies such access. While the exact state laws vary, employers cannot review or access employee devices, absent an agreement to the contrary. *See e.g.*, Cal. Penal Code § 502. Searching employees' personal devices is also fraught with liability given the risk that the employer might access private and personal information, such as health information.

Given this legal context, where companies have elected to allow employees to use their personal devices for business communications, an effective "Bring Your Own Device" (BYOD) policy is essential to ensuring that companies retain the ability to review employees' business communications for compliance purposes. While the exact form of a BYOD policy will vary based on a company's operations and risk profile, generally an effective BYOD policy will require employees to provide clear and informed consent for employers to review relevant business communications.

Where there is no BYOD policy in place that establishes prior consent for the review of business communications, employees will likely have to consent to the review of their phone at the outset of an investigation. This situation can raise significant practical difficulties amid often time-sensitive investigations. Employees, even those not involved in any misconduct, may understandably be reluctant to provide access to their device in the face of uncertain employment and legal consequences.

The challenge - what to do when access to employee devices requires specific consent

As an initial matter, in the absence of an applicable BYOD policy, company counsel should attempt to obtain specific consent by clearly discussing with the employee the benefits of permitting a review of their personal device. This is particularly so because addressing the particular allegation at issue will redound to the employee's benefit, and a full and transparent investigation is the quickest route to that result–especially if company counsel can leverage the internal investigation to forestall a full-blown government enforcement action or private lawsuit.

However, if the employee still does not consent to the blanket review of their personal device, counsel may be left to pursue creative compromises. One potential strategy is to arrange a physical inspection of the employee's device: if the employee is not willing to have their personal device imaged, company counsel can consider conducting a review of relevant messaging apps while the employee is present, allowing the employee the opportunity to consent to the review of specified communications. While a physical inspection cannot afford as much information access as wholesale imaging of a device, a narrower approach may still be reasonably sufficient to identify relevant work communications while still providing the employee with requisite comfort that irrelevant personal matters will not be exposed. This approach is especially manageable if the investigation involves discrete time periods, actors, and topics, such that word-and person-based searches directly within a messaging application would be practicable. Moreover, at a minimum, this approach may yield leads that advance the investigation, as well as information that can be used during a preliminary interview of the employee, who in turn may later be more comfortable consenting to additional searches of their personal device.

In the absence of an employee's specific consent, employers without applicable BYOD policies are left with limited options. Employers may generally insist that employees cooperate with an internal investigation and impose disciplinary measures on employees who refuse, provided that the requests for cooperation are reasonable. *See e.g., Gilman v. Marsh & McLennan Companies, Inc.*, 826 F.3d 69 (2d Cir. 2016). However, there is a substantial risk that some courts will find that an employer's request to review an employee's personal device to be unreasonable, and perhaps even coercive. If so, the employer may be subject to wrongful termination or breach of contract claims, depending on the specific state laws and employment arrangements. Additionally, imposing such discipline solely for failing to share the contents of their personal devices may give rise to a claim that the employer improperly retaliated against the employee for their assertion of their right to privacy under federal or state law. *See e.g.*, Cal. Civ. Code § 1798.125.

The takeaways

As should be clear, there is no substitute for preparation when it comes to systems for reviewing employee business communications. The best way to ensure that companies can monitor and review employees' business communications for compliance purposes is to ensure either that all business communications take place on employer-provided devices, or to have an effective BYOD policy that mandates an advanced blanket waiver as to personal devices. In the absence of such frameworks, employers will often be left to pursue creative compromises such as the physical inspection approach described above.

Winston Y. Chan *is a partner and co-chair of the White Collar Defense and Investigations practice group, and* **Nicole Waddick** *is an associate attorney at Gibson, Dunn & Crutcher LLP.*