FERBER LAW
A PROFESSIONAL CORPORATION

MICHELLE R. FERBER
mferber@ferberlaw.com

SMARTPHONES – DUMB PROBLEMS FOR EMPLOYERS. DOL SIGNALING POSSIBLE RULES REGARDING MOBILE DEVICE USAGE.

For some time employers have been navigating the myriad of legal issues pertaining to use of smartphones and other mobile devices by employees. The ever growing use of mobile devices by employees for work purposes has led to a number of compliance concerns for employers from privacy and data security, to expense reimbursement – all of which remain in various stages of uncertainty. The most recent issue to hit the federal agenda – non-exempt compensation, is equally uncertain.

This month, the Department of Labor announced its intent to request information in July or August 2016 from stakeholders regarding "the impact of the use of electronic devices by nonexempt employees on hours worked issues." It is anticipated that the DOL will gather information to determine how, and how frequently, non-exempt employees are using mobile devices for work, and how, if at all, employers are tracking and compensating employees for this. This move by the DOL is not surprising, and absent a party change in the White House, will likely result in the DOL promulgating rules regulating use of mobile devices by non-exempt employees including rules about when such time should be tracked and paid.

The issue is simple on its face: non-exempt (hourly) employees must be paid for all time worked. This is relatively straightforward when someone is physically present on a job site or in an office or even when work occurs remotely but during the workday. It gets abundantly more complicated outside of scheduled work hours when employees are using mobile devices or other remote access tools (sometimes even without employer visibility) for work-related tasks.

To illustrate how complicated it can become, consider the following example. A supervisor sends a non-exempt subordinate an email about a work-related issue in the evening, the employee reads and quickly responds to the email from her couch while watching TV; is that work? If so, how is an employer expected to capture this time? What if the supervisor didn't expect a response that evening? What if the employee received 10 emails that same night? Or, what if the employee only receives one or two short emails but receives the same volume nightly? At what point is work de minimus (a legal concept recognized under federal law which means it is not material enough to require payment) and at what point is it not? Does it matter if the emails come at 7:00 pm vs 10:00 pm, or on a workday vs a non-workday? What if the employee is required to accept text messages so that the employer can make last minute schedule changes; is that ok? Not so simple, right?

So what to do? Although we don't know yet whether the DOL will promulgate rules, it is likely. Moreover, the compensation issues exist under federal law (and some state laws, including California) even absent rules by the DOL. Thus, the federal attention to this issue is just a good reminder that employers must exercise diligence regarding use of mobile devices and other remote access tools, especially by non-exempt employees.

If you are not doing so already, some things to consider include the following:

1. Review your timekeeping policy and ensure it prohibits "off the clock work" and requires employees to report any time spent working even if offsite or outside regular work hours. Also, make non-exempt employees certify that their time records are accurate.

2. Make sure there is an effective way for employees to record after hours or offsite work. For example, if you use physical time clocks you must come up with an alternate way for employees to "clock in" for remote time. Perhaps you allow manual time slips for remote time or, if it occurs frequently, consider converting to a virtual time clock which allows employees to "clock in" remotely.

3. Consider whether and to what extent non-exempt employees need remote access. Given the complications, the more you can limit non-exempt, after hour, remote work, the better from a wage and hour perspective. At a minimum, safeguards should be established (like supervisor approval for remote access from mobile devices or otherwise) such that employers have visibility to which non-exempt employees have remote access and can better monitor off-hour work and avoid surprise claims. Another safeguard to consider is what non-exempt employees can access remotely and what they cannot. For example, maybe non-exempt associates can access schedules or time off requests from mobile devices, but not email?

4. Have a policy requiring supervisors to limit requests made (phone calls/emails) to non-exempt employees during non-work time. For example, encourage supervisors not to send emails to employees outside normal work hours or on vacation or sick days. Or, if emails outside of work time are a must, consider asking supervisors to spell out when a response is requested so it is clear whether remote work is expected. This is particularly important for vacation and sick days. Even if employers have remote access to employees it should limit interruptions on non-workdays.

5. Ensure that your break policies make clear that all work, including use of mobile devices for work purposes, during meal and rest periods is prohibited.

6. California employers (and employers in other states with expense requirements) must reimburse employees for related expenses if use of a mobile device or home internet is required for work. This is true even if the employee would otherwise have these services in the absence of the business need.

7. To the extent employees are allowed to use personal mobile devices, consider implementing a Bring Your Own Device policy. BYOD policies outline rules for employees who use their own devices to access company data, such as email and address how the employer will protect sensitive business data, especially when the employee leaves or if the device is lost or stolen. Such policies typically remind employees that you own the business data, limit privacy interests in such data, prohibit employees from sharing confidential, proprietary, or trade secret information, and require employees to keep their devices password-protected.

Article provided by Ferber Law CTA's Premier Circle Club & Legal Partner. For more information about the Legal Resource Center and Ferber Law, visit http://www.caltrux.org/legal-resource-center.html. The views expressed in this article reflect

the views of the author and do not necessarily reflect the views of the California Trucking Association.