# ISO: Digital Help
# More Online, June 2017

**Managing the Risks of Employee Cellphone Use**
**By** Jessica Summers, Esq.
Paley Rothman, Bethesda, Maryland
**** SAF members can get FREE legal advice on quick questions from Paley-Rothman, anytime. Call Paula A. Calimafde at (301) 951-9325 and be sure to mention you are an SAF member*

Cellphones have become a ubiquitous yet useful part of modern life. However, for employers, cellphone use by employees poses significant risks. By effectively identifying and managing these issues, employers can drastically reduce the likelihood of costly claims or damaging losses.

Wage and Hour Issues

***Do you know if and when your employees answer phone calls, check emails or do other work outside the workplace? Are your employees paid for this time?***

For many employers, the answer to one or both of these questions is no. Depending on the employee, this can be a big (and expensive) problem known as "off-the-clock work."

The fact that cellphones and other remote access technology gives many employees the ability to perform work from anywhere can be great for business efficiency and production but can also mean that employers don't always know, or have record of, when or how much an employee is working.

Under the federal Fair Labor Standards Act (FLSA), non-exempt employees must be paid at least the applicable minimum wage for all hours that they work. This includes time that an employee spends managing emails, answering calls or doing other work outside the workplace.

For non-exempt employees that are paid a salary rather than by the hour, of-the-clock work is still an issue because all non-exempt employees, including those on salary, must be paid overtime for hours worked over 40 hours in a workweek (or over 8 hours in a day in some states). If the employer does not know how much time the employee has spent working outside the office, the employer cannot accurately calculate how much overtime it must pay the employee. These same concerns do not exist for FLSA exempt employees who are paid a straight salary for all hours worked and who are not eligible for overtime.

Off-the-clock work is particularly challenging because of the absence of clear rules on the topic. For example, it is an open question as to when an employee crosses the line from de minimus

checking of an email account to doing compensable work. During the Obama Administration, the Department of Labor was preparing to gather information about the use of technology in the workplace. The expectation was that this would lead to new regulations on the interplay between the FLSA and new technologies. However, with the change of administration and party control, it is unclear whether this issue will still be a priority for the DOL.

While awaiting any further rules or guidance on the topic, there are a number of steps that employers can take to mitigate the risk of wage and hour claims arising from employees performing work outside the workplace.

- A straight forward, but sometimes unfeasible, move is to eliminate outside access for some or all non-exempt employees. In other words, unless non-exempt employees really need to have access to company email, documents or systems outside of the workplace, don't give them remote access or allow them to download company email on their mobile devices.

- Implementing clear written policies is another way to manage outside work and prevent of-the-clock work. For example, some employers have a policy that non-exempt employees may not do any work outside the office (including checking email) unless they have received advance approval to do so. Under such a policy, if the employee does unapproved work outside the workplace, the employee will still need to be credited and paid for that time but the employer can discipline the employee for violating the policy. At minimum, all employers should have a clear policy requiring employees to report any and all time spent working outside the workplace.

- Even if employees haven't been given access to remote technology or have been instructed not to work remotely, there is still the opportunity for off-the-clock work to occur. For example, the employee might receive a work related phone call or bring a hard-copy document home to work on. In light of this, it is critical that employers have a timekeeping system that allows employees to report any and all outside work time. A traditional system where employees punch in when they arrive and out for breaks and at the end of the day, will need to be supplemented to ensure offsite work is captured.

- When utilizing any of the above approaches, proper training of supervisors or managers is very important. All supervisors and managers should have a clear understanding as to the company's rules about outside work by non-exempt employees and should be held accountable for following and enforcing the rules. Supervisors or managers who ask or expect employees to work outside the office when company policy prohibits it or who dissuade employees from reporting outside work will undermine the steps that the company has taken to protect itself.

- Since the major concerns with off-the-clock work relate to non-exempt employees (because of the hourly pay and overtime issues), employers should conduct an wage and hour audit to make sure all of their employees are properly classified as exempt versus non-exempt.

Protecting Company Information

Another concern posed by employees with cellphones is the risk that the employees will intentionally or inadvertently use their phones to improperly copy or disclose confidential company information. The potential for problems becomes greater when employees are permitted to access company emails or systems using their personal devices.

The bad news is, short of completely banning cellphones from the workplace and preventing any access from personal devices, there is no way for employers to completely eliminate the threat that employee cellphones pose to confidential information. However, the good news is that the threat can be substantially reduced by taking a few relatively simple actions.

- First and foremost, any employee that is going to have access to confidential company information should be required to sign a non-disclosure agreement as a condition of employment. Having a non-disclosure agreement signed by the employee, rather than simply having a policy telling employees not to disclose confidential information, gives the employer more legal options in the event of an actual, or threatened, violation. Employers are well advised to consult with an attorney in preparing a non-disclosure agreement to use for employees. There are certain provisions that cannot be legally included in a non-disclosure agreement, such as a provision preventing an employee from disclosing his or her wages or work conditions. On the other hand, there are certain provisions that should be included, such as the language required for employers to gain the additional protections under federal Defend Trade Secrets Act.

- If employees are permitted to access company emails or systems from their personal devices, employers should make sure that there are clear expectations and policies governing such use. As a condition of being permitted remote access, employees should, at minimum, agree and acknowledge that they will produce any devices used for remote access when requested by the company and that the company has the right to inspect for, and remove, any company confidential information at its discretion. Employees should also be required to implement proper security controls (such as a

password) on all devices that they use for remote access to ensure that company information can't be accessed in the event that the device is lost or stolen.

- IT departments or outside technology consultants can also be an important resource for employers in protecting company information. Particularly where employees have remote access to company systems, employers should consult with their technology specialists to determine what systems they can use to detect or track remote downloads, file transfers or other activities. Having this information can allow employers to identify unusual patterns of activity or determine what an employee, or former employee, may have accessed or transferred to their personal device.

- Finally, when an employee is being terminated, the employer should make sure that all of the employee's access points to company systems are disabled during the termination meeting or as soon thereafter as possible. This should include disabling the employee's login credentials for any company email accounts or systems that he or she might have remote access to.

Cellphones While Driving

At this point, it should come as no surprise that research clearly shows that the use of cellphones increases the risk of accidents while driving. What may shock some employers is that the company might be held responsible for cellphone-related accidents caused by their employees. For example, just a few years ago, Coca Cola learned this lesson when it was hit with a $21 million judgment in a suit brought by a woman injured in an accident caused by a Coca Cola driver who was using a hands-free headset to take a business call at the time of the accident.

The biggest risks exists with employees who drive as part of their job. However, there have also been instances of employers being sued where the employee was driving their own vehicle for their own purposes but was on a business call.

The best protection for employers against these types of claims is a clear policy governing employee cellphone use while driving. In fact, one of Coca Cola's biggest problems in its case was that the company's policy largely left it up to the employee to determine what was appropriate. For maximum protection, employees should be prohibited from being on the phone (even hands-free) when they are driving for company business or when they are driving for any other purpose and the call is work-related. For some employers, such a policy might not be feasible for any number of reasons. In such case, the primary goals for the employer crafting a policy on cellphone use while driving should be to make sure that the policy is clear and unambiguous and as restrictive as possible in light of the business needs and concerns.

Once a policy has been put in place, employers should make sure that the policy is actually being enforced. As with the other types of cellphone use policies, it is critical to ensure that managers and supervisors understand the parameters of the policy and are not doing anything to motivate employees to violate the policy.

Even with a clear and restrictive policy in place, there is always still the chance of accidents occurring. Employers should not assume that their general liability insurance will cover all types of incidents involving employees and should consult with their broker to determine if, and to what extent, the company would be covered in the event that an employee is involved in an accident while driving for business or in their own vehicle while on a business call. If the coverage under the general liability insurance is limited, there may be riders or other options that the employer can explore to expand their protection.

## Conclusion

As technology continues to change, so do the issues surrounding employee cellphone use. While the three items discussed above are presently the biggest concerns in this context, they are not the only ones that could arise. Cellphones in the workplace can be used by employees to violate any number of employer policies (such as harassment) or the law (such as unlawful video or audio recordings). However, employers need to be careful that, in restricting how employees can use their cellphones, they are not infringing upon employees' rights under the National Labor Relations Act to discuss, or engage on, the terms and conditions of their employment. Carefully crafted and enforced policies can go a long way to making sure that employers and employees are on the same page when it comes to cellphone use and that employers are protected to the maximum extent permitted by law.

*The explanations and discussions of legal principles herein are intended to be used for informational purposes and are not to be relied upon as legal advice. Situations may vary and nothing included herein is intended by the author to be used as the principal basis for specific action without first obtaining the review and advice of an attorney.*