Questions Abound About Employee Cellphone Privacy

The answers may surprise you

Mar 22, 2017
By Aliah D. Wright

If your employees are accessing their work e-mail from their personal mobile devices, should they have an expectation of privacy on those devices?

What about when it comes to their Internet search histories?

The answer is that it depends, say workplace legal experts interviewed by the Society for Human Resource Management (SHRM).

Recently, White House Press Secretary Sean Spicer and President Donald Trump's attorneys were trying to crack down on leaks coming from the White House by searching through the mobile phones of White House staffers.

Whether companies are allowed to do that depends on workplace policies and state law—and those laws vary depending on jurisdiction.

Employees may believe that because they're using their own device they can have an expectation of privacy. As *SHRM Online* reported, "86 percent of employees own the smartphone they use on the job." But, experts say, it's up to HR to make sure that employees understand that they may not be able to expect privacy.

This is why employers need specific policies that address company expectations about employee behaviors, including when workers are using their own devices, said Washington, D.C.-based attorney Hope Eastman, co-chair of the employment law practice of Paley Rothman Attorneys at Law, which is headquartered in Bethesda, Md.

"Under most circumstances, it is not illegal for an employer to monitor its employees' e-mail and Internet activity," Eastman said.

"As employees are increasingly using their personal phones for work, employers should [develop] 'bring your own device' (BYOD) policies. The law is in flux as the courts begin to grapple with this issue. Policies should provide that [personal devices used under a BYOD plan]—at least with respect to work communications—can be searched by employers either during employment or at termination."

For the most part, "private employers generally can monitor employee e-mails and keep track of Internet surfing activities that are performed using company devices," said Aaron Tandy, a partner and employment law attorney at Miami-based law firm Pathman Lewis.

(more)

"[Government] employees tend to have more privacy rights than private employees with regard to their own personal devices," Tandy added. "But if private devices are used for public functions or work, then the messages may become discoverable, such as here in Florida where sunshine laws are used to get e-mail and texts between commissioners to determine if any violations occurred. And some public employee jobs are sensitive enough that as part of their employment they have allowed access to their devices."

This is why having a policy is critically important: Employees need to know where the threshold of their privacy lies, experts say.

"A good policy will take into account the concerns of both the company and its employees,"

Eastman said.

"Employee handbooks or a computer use policy should be very specific about using work-related e-mail for personal use," she added. "Most employers expressly state that their computers, and company-owned laptops and mobile phones, including e-mail and text messages, belong to the employer and [that] employees should have no expectation of privacy when using them."

As a general rule, even employees who only use company-provided equipment for work should be told not to use their work e-mail for such personal tasks as finding a job, shopping, scheduling vacations or arranging dates.

U.K. Laws Are Different

According to the U.K. government's website, employers are allowed to check their employees' e-mail and Internet search histories, but only if the employer has previously notified employees of this through an employment policy or in an employment contract.

"In the U.K., workers enjoy a good level of protection when it comes to their own personal privacy, including the means in which their data is collected, stored and used," said Lee Munson, a security researcher at U.K.-based Comparitech, a tech research firm.

"Data protection law does allow employers to monitor them, however, if notice is given [in an] employment contract or a staff handbook. Such monitoring can include the use of computing devices and the e-mail and Internet," Munson said.

However, "should an employer's monitoring go beyond the scope of what has been communicated to an employee, [the employer] may be in breach of the United Kingdom's Data Protection Act, which would give the staff member the option to resign and then bring a claim of unfair or constructive dismissal," he said.

To be safe, employers should have their policy in place before conducting any searches.

(more)

"Without a policy in place, efforts by the employer to inspect or access a personal device that an employee has been using for work purposes can be more complicated and raise concerns related to the employee's reasonable expectation of privacy, as well as possibly federal and state computer fraud and abuse laws," Eastman said.

……