Is your Company BYOD or COPE?

By **Benjamin Fink**

In today's world, there are a myriad of personal electronic devices we have to choose from for our calls, emails, texts and other forms of communication. As individuals, we all have personal preferences and want the widest possible selection when deciding which device to use; however, as employers, we need to be mindful of how this issue can impact our ability to protect our confidential information and trade secrets. Whether the employer owns a device, or whether the employee owns the device can have critical implications when an employee leaves one company to join another, particularly when the other is a competitor.

Companies generally fall into two categories with respect to electronic devices used for business purposes. The first is BYOD – often referred to as "Bring Your Own Device." The second is COPE – "Company-Owned, Personally Enabled" devices.

The BYOD scenario provides employees with the widest latitude to satisfy their personal preferences; however, it also requires the company's IT department to support a wide variety of personal devices. Perhaps more importantly, in the BYOD scenario, employers are putting their confidential information or trade secrets at risk if they don't implement clear policies for how information may be used and stored on the employee's devices or implement measures to secure the information when the employee departs. At a minimum, the company must tailor its technology use policies to ensure that employees are put on notice that any information residing on their personal devices at the end of their employment is required to be returned and deleted from the device. Employers may also want to consider requiring employees to create a secure area for work data and activity on the employee's personal device. This will allow the employer to more easily secure that data and information when the employee departs from the company.

In the COPE scenario, it is much easier for the employer to maintain control over information stored or accessed from the device. However, given the myriad of choices available, employees may not like the COPE approach, unless the employer offers a fairly wide variety of devices from which employees can choose. Employees also may not like this approach because most employees will want to be able to use their devices for personal activities in addition to conducting business (e.g., text messaging, Facebook, Twitter, etc.). Given these competing interests, companies that use the COPE approach may wish to develop a policy which allows employees to install apps, music, video and other things on the device; however, the employer must consider how it is going to deal with the employee's personal data, apps and other things on the device when the employee leaves and how the company's technology use policies will apply to personal use of the device.

This article only scratches the surface of the various issues that an employer must address with respect to personal technology devices. It is important for companies to address these issues and develop policies that will best position them to protect data and other confidential types of information when an employee departs. Failing to do so could result in the loss of the ability to protect the information from being disclosed to or used by a competitor when an employee departs.

Benjamin I. Fink is a shareholder in Berman Fink Van Horn P.C. where he focuses his practices on trade secret, non-compete and other competition-related disputes.