2025| VOL. 42 | NO. 1

Inside

A publication of the Corporate Counsel Section of the New York State Bar Association

Your Personal Cell Phone and Discovery: Bring Your Own Device (BYOD) Policy Considerations

By Arnold Blair

The proliferation of cell phones into the daily lives of almost every person on the planet has changed how we all communicate both personally and professionally. Allowing employees to use their own cell phones for work can save a company money, help employees to stay connected, and increase productivity. On the other hand, personal devices can put company information at risk and create potential legal issues during data collections. Some of the concerns with employees using personal cell phones for work are data security, risk of confidential information being lost or stolen, and privacy breaches. Specifically, some of the issues that can arise during data collections include access to devices for collection and adequate preservation during a legal proceeding.

With the increasing use of personal cell phones for work purposes, some companies have developed what are known as Bring Your Own Device (BYOD) policies. These are policies that address the concerns mentioned above. The purpose of a BYOD policy is to set expectations for employees regarding privacy and data security. For this reason, explicit BYOD policies are essential. BYOD policies can set the foundation for a company to identify and collect data from employees' personal devices while addressing employee concerns about privacy and personal data.

These BYOD policies can also help balance competing interests and set out rules regarding a company's right to access information on an employee's personal phone. Nowadays, electronic communications include not only emails, but texts, communications sent through messaging apps (including ephemeral messages), and social media posts. A company can define what communications methods are authorized for work in a BYOD policy. It also can spell out that a company has the right to place a cell phone under a document preservation order and collect and produce data relevant to a legal proceeding. Stating the acceptable means of communication for personal cell phones used for work purposes is paramount.

BYOD policies are also important because failure to effectively monitor employees' communications on personal cell phones can lead to penalties as well. Consider the high-profile settlements where companies have been fined because their employees used non-company channels for work-related communications. These settlements show that companies need to take employees' communications and preservation seriously. BYOD policies that clearly define expectations are one step to addressing modern workplace communication concerns.

Good discovery practices are another focus of BYOD policies. When it comes to discovery, a company has a legal obligation to review data in its possession, custody, and control. This fact presents a challenge to companies that allow employees to use their personal cell phones for work. By allowing employees to do so, companies sometimes gain possession, custody, or control of the data on employees' cell phones. Regarding discovery in legal matters, courts have held that employee use of personal devices does not negate this obligation to search for data on personal cell phones when it is in a company's possession, custody, or control.

Ensuring that employees use personal cell phones for work in an appropriate manner clearly has important implications for discovery. The manner in which business communication is conducted via a personal cell phone can affect whether a company can comply with document requests and other discovery obligations. For effective discovery, a company needs to balance its abilities to protect any confidential information, adhere to legal regulations, ensure personal information is protected, and encourage employee efficiency.

Structuring BYOD Policies

There are a few important things to keep in mind when creating a BYOD policy. Those include making it clear who owns the data on personal cell phones, what methods of communications are permissible for work-related communications, and how privacy issues will be handled.

First, a BYOD policy should have language that clearly outlines which data belongs to whom, i.e., the employee or the employer. Typically, the business entity, company, or organization will have control over the work-related data with the right to manage and keep it secure. Although the employee still owns the actual device, the company can still be responsible for reviewing any material on the device that is subject to discovery.

Second, in a BYOD policy, a company should spell out in detail the communication methods that an employee is permitted to use on a personal cell phone for work-related activities. Given the continued proliferation of new ways

to communicate, it is important to limit those methods of communication to apps that have been vetted and approved by an IT department or someone with knowledge of such issues. This ensures that company communications not only are protected but also retrievable if the need arises through discovery. A BYOD policy can set forth guidelines for these protections.

Third, a BYOD policy can clarify privacy issues related to employees' use of personal cell phones. Whenever a personal cell phone is potentially subject to discovery, the issue of privacy inevitably arises. Handing over a personal cell phone can make some employees uncomfortable. A well-crafted BYOD policy can alleviate that fear by establishing an employee's expectations of privacy and provide a roadmap on where potentially relevant communications may reside.

Conclusion

Successful BYOD policies balance employee expectations of privacy with a company's obligation to comply with legal requests and discovery obligations. For example, they can facilitate targeted document collections from personal cell phones used for work, while keeping personal, non-relevant data outside the scope of a collection. They can also allow a company to control who has access to sensitive information, lessen any potential vulnerabilities that can compromise data, and assure employees that their personal information and privacy is being protected.

Arnold Blair is discovery counsel at MoloLamken LLP. He is highly experienced with discovery, with a focus on practical and defensible solutions in connection with high-stakes government investigations and litigation. He is experienced in managing all aspects of eDiscovery and assisting case teams with strategies to achieve desired goals and outcomes.