# BYOD Policies: A Great Idea When Properly Executed

C. Alex Retzloff

WILLCOX SAVAGE

In today's highly connected, tech-obsessed world, personal electronic devices ("devices"), including tablet computers and mobile phones, are seemingly ubiquitous. Increasingly, employers are capitalizing on this phenomenon by adopting so-called Bring Your Own Device ("BYOD") policies that permit, encourage, or even require employees to use their own private devices for business purposes in lieu of employer-provided devices. Many employers that have adopted BYOD policies praise them as a means reducing costs while simultaneously increasing employee convenience, flexibility, and productivity. Others, however, view BYOD policies differently. To these employers, BYOD policies represent a significant, unnecessary risk that they cannot justify voluntarily assuming, notwithstanding their other advantages. But as is often the case, neither side is wholly right or wrong. Prudent employers should, therefore, consider both the advantages and disadvantages of BYOD policies before they decide whether or not to embrace them. Furthermore, those that choose to embrace BYOD policies should take certain, deliberate steps to maximize their benefit and minimize their risk.

As the employers that have already adopted BYOD policies of their own are quick to point out, there are significant advantages in allowing employees to use private devices to conduct company business. These advantages can include reduced costs for providing, maintaining, replacing devices and training employees how best to use them; increased convenience and flexibility for employees; and increased productivity, access to company information, and digital business operations.

But the practical disadvantages of BYOD policies can also be significant. Many employers have found that allowing employees to use their own devices for business purposes creates or exacerbates a host of problems, including, but not limited to, reduced control over data, devices, and the use thereof; increased information security vulnerability; and added strain on information technology support staff who must support a wide array of new or different devices.

Even more concerning than the practical disadvantages of BYOD policies are the potential legal disadvantages. Most of these disadvantages primarily arise under federal law, but state law analogues should also be considered. Whether they arise under federal or state law, these disadvantages can largely be divided into two categories: those concerning pay and those concerning privacy.

**Legal Issues Related to Pay**

The pay-related disadvantages typically arise under overtime and minimum wage laws like the federal Fair Labor Standards Act ("FLSA"). Since BYOD policies enable employees to work remotely during abnormal hours, they blur the line between working and non-working hours. If non-exempt employees use their private devices to access work-related emails, make work-related calls, or "log in" to perform even mundane work-related tasks outside of normal business hours, that would likely qualify as compensable hourly work. And if the employees fail to accurately record this time, or if the employees accurately record the time, but these additional hours push their weekly hours above the 40-hour cap, their employers could be liable for unpaid overtime wage claims.

**Privacy Concerns**

Unlike the pay-related disadvantages, the privacy-related disadvantages to BYOD policies arise under a variety of laws. Where BYOD policies grant employers access to their employees' private devices, they must

be careful not to surveil or access, even accidentally, their employees' personal emails, texts, and other electronic data and communications. Employers who fail to exercise caution risk violating the federal Computer Fraud and Abuse Act ("CFAA"), which criminalizes certain unauthorized access of another's computer, or the federal Stored Communications Act ("SCA"), which protects the privacy of wire and electronic communications while in electronic storage, including emails stored on a server. They also risk violating the Genetic Information Nondiscrimination Act ("GINA") or the Americans with Disabilities Act ("ADA") by viewing protected personal information stored on an employee's private device. Additionally, they open themselves up to liability under the National Labor Relations Act ("NLRA"), as monitoring their employees' communications or activity or accessing their location through their private devices' location software may directly infringe on their employees' right to engage in protected concerted activity under the NLRA or otherwise chill their employees' exercise of that right. Similar concerns arise under the state law analogues to these federal privacy laws.

**Best Practices**

As mentioned above, employers would be wise to consider both the advantages and disadvantages of BYOD policies before adopting them. For some, the disadvantages will outweigh the advantages and cut against adoption. But for others, the converse will be true.

Employers that, after careful and deliberate consideration, determine that the advantages of BYOD policies outweigh their disadvantages can and should take certain, deliberate steps to ensure that they maximize the benefit of such policies while minimizing their risk. These steps include:

- Prohibiting all off-the-clock work and instructing non-exempt employees to record all time worked;
- Developing policies and procedures for non-exempt employees to easily report off-the-clock work so that these employees will be properly compensated for all hours worked;
- Including statements in their BYOD policies making clear that time spent by non-exempt employees responding to emails and answering telephone calls during non-business hours should be considered "hours worked";
- Prohibiting or limiting non-exempt employees from responding to emails or telephone calls during non-business hours;
- Requiring prior written authorization to work remotely or via mobile device;
- Training managers to minimize sending emails to or calling non-exempt employees during non-business hours to mitigate the risk of off-the-clock work;
- Training managers to indicate in their communications whether an immediate response is required or whether it can wait until regular business hours;
- Implementing internal policies and procedures to limit the employers' access to private employee communications;
- Including provisions in their BYOD policies that limit employee expectations of privacy;
- Requiring employees to give their employers affirmative consent to access their private data, monitor their activity, and manage their devices;
- Inserting genetic and medical information waivers in their BYOD policies, employee handbooks, or both;
- Defining employee and device eligibility to participate in the BYOD program;
- Defining appropriate use and misuse of devices and any employer-provided software installed on them;
- Mandating minimum security requirements for private devices used for business purposes;
- Requiring employees to concede a certain degree of device management authority to their employers through mobile device management ("MDM") software;
- Defining cost and reimbursement terms for each device and related device services and having employees affirmatively consent to any deductions made to reimburse the employers for the cost of a private device;
- Including disclaimers of liability for lost, stolen, or damaged devices and data; and
- Dictating processes for preserving, returning, or destroying employer data, customer contacts, financial information, intellectual property, and other employer digital assets when the employment relationship ends.

**C. Alex Retzloff**
Willcox Savage
440 Monticello Avenue, Suite 2200
Norfolk, Virginia 23510
cretzloff@wilsav.com