jackson|lewis

"Bring Your Own Device" (BYOD) Issues Outline

For a variety of reasons, including significant cost savings and employee relations, businesses have been considering or have already transitioned to a "bring your own device" ("BYOD") platform. In short, BYOD refers to arrangements where employees are permitted to connect their own personal devices to the employer's networks and systems to complete job tasks either in the office or working remotely. Moving in this direction has many benefits, but also creates a number of business and legal risks. Adopting BYOD also may result in some unintended consequences that may not be problematic for your organization, but are issues you want to be aware of when deciding whether to make the switch.

We prepared the following outline to highlight key issues and policy considerations for companies considering moving to or continuing a BYOD program. This outline is not exhaustive, nor is it industry specific, but we think it provides a good starting point, a "cheat sheet" or checklist if you will, for issues you should be thinking about. If you have any questions regarding these issues, please contact a member of our Privacy, Social Media, and Information Management Practice Group, or the Jackson Lewis attorney with whom you normally work.

Key Issues to Consider:

Compliance risks. Whether a business is "compliant" concerning BYOD will depend on a number of factors including industry, location, classes of data maintained on the device, governing regulatory agencies, professional/industry standards, contracts with business partners and other issues. More specifically, these include:

- *HIPAA and state data security requirements* – Even with new developments in device management software applications, the ability to manage and secure important company data and personal information is made more difficult with BYOD. The tightening of requirements to safeguard personal data under various federal and state laws (e.g., HIPAA, GLBA, and state mandates in CA, MA, CT, TX, NY, OR, MD, and others) and to quickly react to data breaches enhance this concern. Problems can arise in a variety of ways, such as the rogue employee who refuses to return the device, a challenge to whether a trade secret had been appropriately safeguarded, or a diligent employee who happens to inadvertently use an unsecure wireless network.

- *e-Discovery* - When involved in a litigation, having ready access to information required in the course of the discovery phase of the case can be made more complicated when some of that information may be stored on an employee's personal device.

- *Wage and hour* – BYOD and personal communication devices can further blur the lines between personal and work time, raising the issue of whether time is compensable. Consider, for example, the employee on an employer-approved leave who spends hours each day responding to work-related emails.

- *International data privacy requirements* – BYOD needs to be considered even more carefully when implemented on a global scale. Cross border transmissions of personal data and different employment standards from country to country can raise thorny issues for multinational companies.

- *Garden variety workplace law issues* – Workplace harassment, discrimination, and privacy risks are not avoided because suspect activities happen on an employee's device, rather than the company's device. For example, businesses that engage in monitoring employees' locations and communications may need to think more carefully about the nature, scope and notification requirements concerning that kind of monitoring activity. An awkward employee relations issue (as well as an e-discovery risk) is the ability to "wipe" a device in the event of a security risk to the information on the device, or other circumstances affecting the device. Businesses will need to explore this option carefully with regard the selection of their BYOD device management vendor/solution, their own IT capabilities, as well as communicating the "wipe" possibility to employees.

- *Labor* – A company considering BYOD for a group of employees represented by a bargaining group likely will need to bargain with the union on whether it can implement such a program.

- *Record retention and destruction requirements* – One of the concerns in a BYOD context is triggered when an employee changes his or her device. Tossing the device in the trash, even if in an environmentally friendly way, may not be consistent with the federal or state data disposal laws requiring personal information be appropriately destroyed.

Business Issues.

- Will all employees be eligible for BYOD? Can we have a mixture of company owned devices and BYOD?
- What devices are permitted? Will/should the IT department be able to service employees? How do we determine whether to adopt new devices?
- How do we ensure devices are appropriately updated, secured?
- When does the company have to reimburse the employee for the cost of the device because it is necessary to perform the employee's duties? See CA and other states.
- What device management vendor should we use? What are some of the critical services agreement provisions?
- How will BYOD affect our ability to manage employee workload and performance?
- Are our clients OK with our employees using BYOD?
- Are our trade secrets protected?

Sample Policy Elements:

Eligibility and Program Parameters.

- Defining employees/departments eligible to participate in BYOD
- Defining eligible devices
- Address permissible personal v. business use
- Employee agreement requirement, acknowledgement, consideration, etc.
- Access and use limitations
- Applicability of other employment/workplace policies

Reimbursement.

- Personal v. business use
- Tax compliance
- Conditions for reimbursement
  - Device purchase and/or replacement
  - Data plan limitations (e.g. maximum reimbursable amount)
  - Substantiation of expenses

Security.

- Prohibited activities
  - "Jail Breaking" or "Rooting"
  - Modifications to device hardware or operating software beyond routine updates
  - Unsecured networks, WiFi
- Utilization of technology consistent with an enterprise-wide written information security program, global privacy compliance, and business partner/client agreements
- Process and timing for reporting loss, theft, new device, unauthorized access, and cessation of employment
  - Remote wipe (failed log-in, lost device, other)
  - Back-up reminder/notice
  - Update, patch reminders
- Password and/or encryption requirements

Monitoring.

- Address employees' expectations of privacy
  - Reserve the right to monitor - communications, location and activity
  - Voluntary acceptance of program
  - Explicit/implied consent
  - Notice/posting requirement (e.g., DE and CT – bulletin board, log-in screen, handbook)
  - Consistency in content and application of policies

End-User (employee) Support.

- Define what devices are supported
- Define types of support provided (e.g., applications, device, scenarios, "self-service")
- How to request support
- Train support staff concerning access and handling of data in the course of providing support

Policy Violations.

- Be clear and consistent on consequences
- Business partner and other notifications
- Breach risks

Additional Policy Considerations.

- Guidelines on device configuration
- Safety (e.g. vehicle use)
- Data breach response program (required under HIPAA and in certain states)
- Develop process for litigation preservation, data deletion, device and security updates at all relevant times including commencement of certain leaves of absence and termination
- Training

4846-1172-3028, v. 1