PRIVACY, SECURITY, AND PRACTICAL CONSIDERATIONS FOR DEVELOPING OR ENHANCING A BYOD PROGRAM

By: James A. Sherer, Melinda L. McLellan, & Emily R. Fedeles[1]

The development and implementation of a "bring your own device" (or "BYOD") program presents a host of administrative and technical challenges, especially for multinational organizations that regularly transfer data across borders. Unsurprisingly, designing a BYOD program does not lend itself to easy answers or "cookie cutter" approaches, and there is no one-size-fits-all solution or set list of "do's and don'ts" that will apply in all cases. There are, however, certain principles and considerations that can help guide data privacy professionals as they draft or revise BYOD policies and procedures. In this article, we provide a list of relevant questions and issues to consider when creating or revamping a corporate BYOD program, including some finer points that may enhance even mature, well-functioning BYOD practices.

In most cases, taking an organization-oriented approach to the program development process will yield the best results. The effort should involve all relevant stakeholders: typically, senior management, the IT Department, the Legal Department, Human Resources, and others (as appropriate). Subsequent discussions should explore which path or paths to legal compliance would best serve the organization's business needs. Once compliance and business goals have been established, the considerations listed below may be used as a framework for the design and implementation of specific policies and procedures. Given rapidly-evolving BYOD technology and the constantly shifting legal landscape, regularly-scheduled reviews for purposes of adjusting and updating policies should be built into the backbone of any BYOD program.

[1] James A. Sherer and Melinda L. McLellan are Counsel in the New York office of Baker & Hostetler LLP. Emily R. Fedeles is an Associate in Shook, Hardy & Bacon's Geneva, Switzerland office. The views expressed herein are solely those of the authors, should not be attributed to their places of employment, colleagues, or clients, and do not constitute solicitation or the provision of legal advice.

Considerations Pertaining to the Device Itself

- Which mobile devices will the organization support?
    - If a wide variety of devices (and versions of devices) will be supported, how will the organization provide consistent user experiences?
    - Will the device selection be driven by user preferences, organizational mandate, or a compromise?
- Which Mobile Device Management Solutions ("MDMs") would best suit the organization's security needs?
- Would the organization be better served by a corporate-owned, personally enabled ("COPE") model, a corporate-owned, business-only ("COBO") model, or a hybrid strategy?
- Would export controls apply to certain devices, operating systems, applications, or business information?
- Will the organization pay for the devices and their usage directly?
    - If so, will the organization be the "customer" for the purposes of the provider relationship?
    - What employee privacy issues may arise in this scenario?
    - Will employees be reimbursed for device purchases?
    - How will the reimbursement process work?
- What procedures should the organization put in place to manage employee separation and device decommissioning/disposal?
- What procedures should the organization put in place to mitigate potential damage when a BYOD device is lost or stolen?
- How will the organization ensure that all company data is securely removed prior to an employee trading in the device?
- If an employee is terminated or otherwise separates from the company on bad terms, what heightened security measures will be needed to protect company data on the employee's device?
- How will the organization recover company data if an employee inadvertently (or intentionally) deletes the data from a BYOD device?

Considerations Regarding Device Usage

- Who within the organization will be allowed to participate in the BYOD program?
- Will the scope of employee participation differ depending on job functions?
- Will the organization pay for (or reimburse) data plan charges?
    - If so, which party will be considered the "customer" in the relationship with the service provider?
    - Will standard charges be treated differently from overages, roaming charges, international charges, or other such expenses?
- Does applicable law require consideration of overtime and other wage-and-hour restrictions with respect to BYOD use outside of normal working hours?
- If the organization needs to collect information off of the device (either for business purposes, or to comply with law or legal process), what additional considerations arise?
    - Is the organization required to segregate certain information prior to, or following, collection?
    - Must the organization certify destruction of the information following the relevant period of inquiry?
- To what extent will the organization seek to segregate business data from personal data on the device—and what if such segregation is not technologically feasible?
- To what extent, if any, will the organization attempt to restrict third-party use of the device (e.g., casual use by a spouse or child)?
- Will the organization need to restrict the use of BYOD for certain types of *work* activity, for example, when legal holds create preservation and collection burdens?
- What procedures will the organization put in place to protect organizational data if an employee must replace a device from a remote location, without organizational support?

Policy Development Strategy

- When operations vary widely within the organization, is a single, organization-wide policy appropriate?
- Does a traditional, top-down approach make sense for the organization?
- Generally, a consistently-enforced, well-structured BYOD policy may help shield the organization from potential liability, but would the organization benefit from a less structured approach?
    - For example, would developing policies on the business-unit level allow for beneficial flexibility?
- How will the organization handle BYOD policy violations?
- How will the organization address border crossing security issues with respect to BYOD devices?
    - Policies should address threats to data security posed by foreign jurisdictions as well as the possibility of employee devices being searched at the U.S. border by U.S. authorities.
- What risks and benefits are associated with implementing a "business use only" policy with respect to BYOD?
    - Would such an approach make sense vis-à-vis the company's culture?
- How should the organization inform employees of applicable policies and verify acknowledgement and understanding of such policies (e.g., annual re-affirmation, reminder pop-ups presented *on* the device)?
- Which law(s) will apply in various scenarios, and how should potentially overlapping jurisdiction inform policy development?
- How will the organization apply multiple jurisdictions' laws or regulations consistently?
    - Consistency is perhaps the best defense when the law is uncertain: develop policies that hew as closely as possible to the ostensibly applicable laws, and then enforce those policies across the board.

- How will the organization integrate BYOD considerations into other organizational policies (e.g., workplace safety and discrimination policies, acceptable use policies, and records management policies)?

Privacy Concerns and Other Legal Considerations

- Who within the organization is responsible for monitoring legal developments that may impact BYOD practices?
- How will the organization consider and apply forthcoming revisions to the EU Data Protection Regulation?
- Should the organization obtain advice from foreign local counsel before proceeding with a BYOD program in certain jurisdictions?
- How will the organization provide notice of its monitoring practices, and offer choices with respect to monitoring where required?
    - In the U.S., organizations may expose themselves to liability for unfair or deceptive trade practices if their disclosures are inaccurate or misleading.
    - In the EU, it may not be possible to obtain valid consent in the employment context.
- What additional privacy concerns may arise when the organization issues legal holds applicable to BYOD devices?