Ava Baratz

CYSE 425W

February 4th, 2024

Policy Analysis Paper 2

Bring Your Own Device (BYOD) enables employees to use their personal devices to perform functional tasks within their position. BYOD has become increasingly popular as society continues to increase its dependence on personal devices. Implementing BYOD offers an organization many benefits, including reduced operational overhead costs, increased employee productivity, and improved employee interactions. Although BYOD offers favorable advantages over corporate-issued mobile phone management, policymakers must consider the significant political implications of BYOD, including 4th amendment conflicts, privacy concerns, and ownership conflicts.

One of the most significant political ramifications of an organization's BYOD policy is the conflict with the 4th amendment. A BYOD policy often blurs the line between privacy between individuals and organizations (Smith, 2017). The 4th amendment protects individuals from unreasonable search and seizure without a warrant and a trial (Utter, 2015). Regarding smartphones, if an organization does not establish a policy that explicitly allows forensic investigators to consent to search phones, the investigator will be unable to search any personal devices. This could complicate forensic investigations within an organization. Suppose a security incident occurs and evidence is present on a device enrolled in a corporate BYOD program. In that case, a policymaker must consider explicitly written consent to mobile device searches by forensic investigators. If policymakers do not include this statement in their BYOD policy, they will immensely reduce forensic investigation findings. Successful policymakers will include

explicit statements that consider the implications of privacy concerns if there a forensic investigation must be conducted on a device enrolled in BYOD to make employees aware of legal procedures.

In addition to 4th amendment implications, BYOD policies create unclear boundaries between corporate and personal data. Often, BYOD creates a "unique set of challenges for IT professionals." (Degirmenci et al., 2023). The Electronics Communication Privacy Act aims to establish protection around personal device communications from unauthorized search and seizure (Utter, 2015). While a mobile device uses a service provider, its electronic communications are protected from viewing or alteration by a third party (Utter, 2015). However, a digital forensic investigator can submit a formal request to the service provider to obtain information from a third party. Although this law is enacted further to protect the privacy of user mobile device communications, digital forensic investigators can breach other parties' rights to complete forensic investigations (Utter, 2015). This is a significant consideration policymakers must acknowledge and inform BYOD users in the case of a possible forensic investigation within the organization.

Lastly, policymakers must consider establishing clear boundaries regarding BYOD ownership. If an employee is terminated within an organization, there must be explicit procedures for data ownership (Degirmenci et al., 2023). If an organization does not establish these procedures, there may be potential lawsuits against the company for invading personal privacy (Smith, 2017). An organization must state that it owns all corporate data on a device enrolled in BYOD. In addition, an organization must establish media sanitizing procedures for obtaining strictly company data and exclude the gathering of any personal data. An organization must also establish a policy for data retention that states how long the company will store the

corporate data gathered on the BYOD device. An organization must establish the required time frame on how long to store corporate data and establish a method for secure data archiving in case an organization must investigate the corporate data gathered on a device enrolled in BYOD.

References

Degirmenci, K., Breitner, M. H., Nolte, F., & Passlick, J. (2023). Legal and Privacy Concerns of BYOD Adoption. *Journal of Computer Information Systems*, 1–12. https://doi.org/10.1080/08874417.2023.2259346

Smith, W. P. (2017). "Can we borrow your phone? Employee privacy in the BYOD era". *Journal of Information, Communication & Ethics in Society, 15*(4), 397-411. https://doi.org/10.1108/JICES-09-2015-0027

Utter, C. (2015). The "Bring Your Own Device" conundrum for organizations and investigators: An examination of the policy and legal concerns in light of investigatory challenges. *Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2015.1202