Additional Considerations for Bring Your Own Device

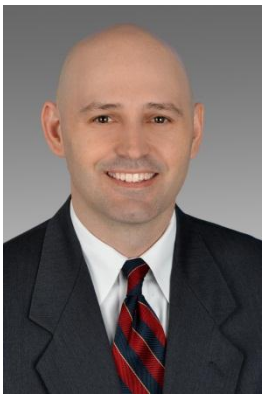
By Brian Von Hatten

A previous blog outlined many of the risks associated with increasingly prevalent bring your own device ("BYOD") policies. While the previous discussion focused on I.T. governance concerns such as security, administration and device management, there are additional legal risks regarding BYOD.

The first is the idea that these devices may, depending on how they are being used, likely require various licensing components to be in compliance. Even though someone else owns the device (the employee), the employer may still need to secure various client access licenses ("CAL") etc. for each device that is connecting to the employer's resources on the backend. This could include access licenses for connections to back-end databases, or vpn clients, etc.

Additionally, there is the possibility for liability depending on how the device is being used. Even though the employer does not own the device, it may still be used to, for example, send text messages while driving. Regardless of who owns the device, if the device is being used while the employee is acting within the scope of her employment, the employer may be exposing itself to liability. Because the employer does not own the device, it most likely does not have the ability to "lock" the device or service provider account and prevent use of text messaging features, as an example.

Given the possible liability that may result from BYOD, employers should carefully consider the potential downsides and benefits of these types of policies to ensure the company is acting in within the scope of its tolerance for risk.



About the author Brian Von Hatten:

Brian represents many large and mid-market organizations on matters related to transactions, software licensing, and disputes. Brian's focus includes substantial attention to complex information technology issues for companies of all sizes.

Get in touch: bvonhatten@scottandscottllp.com | 800.596.6176