Employer E-Discovery Duties Expand in a "BYOD" Environment

Feb 07 2014

Posted By: Mark F. Foley

Practice Area: Information Technology, Data Privacy and Security & Commercial and Business Litigation & Litigation and Risk Management

Companies that allow an employee to Bring Your Own Device ("BYOD") must take extra steps to assure compliance with litigation discovery rules.

Under federal rules and state rules of civil procedure, a company that is a party to litigation or is aware that litigation is reasonably foreseeable has a duty to identify, preserve, and produce relevant information within the company's "possession, custody, or control." Courts have construed "control" to include both the legal right and the practical ability to obtain information from a non-party.

A company's use of a BYOD environment raises many questions about the scope of an employer's e-discovery duties. For example, does the employer have possession, custody, or control of a voicemail concerning employer business left on an employee's personal smartphone through a personal mobile phone account? What about an email sent through the employee's personal email account, social media page, or tweets? Does an opposing party have the right to such social media information or to the metadata pertaining to such communications? What other communications or data storage systems might have to be identified and searched?

There are additional questions about how a search of data created or accessed in a BYOD environment must be conducted. Must the opposing party subpoena the information from the employee or its service providers, or does a request directed to the employer require it to obtain such information from the employee? What if an employee or independent contractor refuses to cooperate? Does the employer have a legal right to demand access to the information? Do privacy laws limit the employer's ability or duty to search personal devices?

The technical specifics of how a company implements its BYOD environment can also affect e-discovery processes. Some companies leave the host operating system open to read and write files in the event the user is without an Internet connection and still needs to work on files "locally." Files modified in or deleted from the host operating system or the virtual operating system may still exist in the other, requiring that both be searched for responsive documents.

The employee's duty to cooperate and the employer's duty in litigation may depend upon the employer's BYOD policies. Such policies vary widely. Some companies address these issues directly. In other cases, a court will try to deduce an employer's custody or control from the circumstances. For example, does the employee's device enable the user to separate work and personal usage, as some Blackberry devices do? Does the company provide technical support for the employee's device? Do company policies allow the employer to access and wipe the device if it is lost or stolen? Does the employer direct the employee to use SMS or other technologies implemented through the employee's device for business purposes?

The court in *Pradaxa (Dabigatran Etexilate) Products Liability Litigation* addressed these issues directly, and came down hard on the side of requiring litigants to identify, protect, and produce such information. In that case, the employer did not take steps to turn off the auto delete function for texts on employee devices, despite a litigation hold, and the employer consequently failed to produce relevant texts during discovery. The court fined the employer for unacceptable conduct of discovery.

Other courts have been more reluctant to find that information on employee devices is within the employer's direct control or custody. Such cases generally rely on the absence of proof that the employees used their devices for work-related purposes. This will rarely be the case in a true BYOD environment.

The best practice is to address the issue proactively. Have employees sign consents allowing employer access to devices, should the need arise. Have clear policies about device use and corporate network connection. Restrict or prohibit the use of non-corporate storage clouds. Update internal litigation hold and e-discovery procedures to assure that employee devices, cloud storage, and service providers are identified and their data preserved when litigation is first foreseeable and appropriately searched and produced as required.

Companies doing business in foreign countries or regulated industries will also have to define these policies and procedures in compliance with applicable laws and regulations such as those pertaining to data privacy, security, and trans border data transfer.

This Update originally appeared in the WTN News column entitled "Digital Lex: Exploring the intersection of law and information technology," at WTNNews.com.
