POLSINELLI®

Commercial Litigation

April 2018

New Guidance on Employee-Owned Device Discovery

By Amy D. Fitts, Caitlin J. Morgan, and Ashley N. Gould

As technology continues to evolve, organizations are increasingly facing challenges concerning whether, and to what extent, they allow employees to utilize their own devices for work purposes. When employees use their own personal, privately-owned devices to access, manage, and store organization information, organizations are frequently asked to produce information from those devices in litigation, which can impose significant costs on the employer. Whether such information is within the employer's possession, custody, or control and whether that information is more readily available from other sources are frequent sources of disagreement.

Recently, the Sedona Conference, a non-profit legal research and educational institute that is often cited by courts, weighed in on so-called "Bring Your Own Device" or "BYOD" policies and some of the discoverability issues involved with employee-owned devices. **Although the Sedona Conference's guidelines are unlikely to resolve many of the day-to-day disputes over BYOD discovery issues, they do shed light on the need for employers to take discoverability issues into account when setting BYOD policies.**

The Sedona Conference: Five Principles

To provide guidance on this issue, the Sedona Conference recently released "Commentary on BYOD: Principles and Guidelines for Developing Policies and Meeting Discovery Obligations."[1] This commentary contains five principles regarding the considerations that organizations should address when determining whether to permit the use of employee-owned devices. For organizations that choose to allow or require their employees to use their own devices, the principles also provide a list of precautions and actions organizations should take to ensure they comply with their legal and discovery obligations. The five principles are:

[1] The Sedona Conference Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations, (January 2018), available at http://www.thesedonaconference.org.

Authors:

Amy D. Fitts
Shareholder
816.218.1255
afitts@polsinelli.com

Caitlin J. Morgan
Associate
214.661.5513
cmorgan@polsinelli.com

Ashley N. Gould
Associate
214.754.5716
agould@polsinelli.com

Principle 1: Organizations should consider their business needs and objectives, their legal rights and obligations, and the rights and expectations of their employees when deciding whether to allow, or even require, BYODs.

Principle 2: An organization's BYOD program should help achieve its business objectives while also protecting both business and personal information from unauthorized access, disclosure, and use.

Principle 3: Employee-owned devices that contain unique, relevant electronically stored information ("ESI") should be considered sources for discovery.

Principle 4: An organization's BYOD policy and practices should minimize the storage of—and facilitate the preservation and collection of—unique, relevant ESI from BYOD devices.

Principle 5: Employee-owned devices that do not contain unique, relevant ESI need not be considered sources of discovery.[2]

Based on these principles, the Sedona Conference suggests that organizations should first assess the pros and cons of permitting their employees to use BYOD devices.[3] In making this determination, organizations may want to consider their size, cost concerns, privacy concerns, and legal factors that would affect the organization's ability to access organization data on the BYOD devices.[4] One of the key legal factors, as the Conference recognized, is whether an organization may access its own information on the employee's private device.[5] This issue alone implicates data protection laws, labor laws, and other laws and policies.[6] Accordingly, organizations should consider that significant legal implications may arise if the organization is required to turn over ESI, but it is unable to access the employee-owned devices that contain the relevant information.[7]

[2] *Id.* at 5.

[3] *See id.* at 6-7.

[4] *Id.*

[5] *Id.* at 7.

[6] *Id.*

[7] *See id*. at 9.

If an organization chooses to allow its employees to use BYOD devices, the Sedona Conference guidance supports the implementation of BYOD protocols.[8] According to the Conference, those protocols should: (i) clearly state the organization's expectations regarding the use of the BYODs and the organization's access to them; (ii) consider the organization's objectives; (ii) protect the organization's business information; (iii) consider the employee's privacy interests; and (iv) consider the employee's protected private information that is stored on the BYOD device.[9]

Additionally, the guidance suggests that organizations should ensure that employee-owned devices are not used to transmit or store unique organization information.[10] In other words, an organization should ensure that all of its data is also contained on, and more readily accessible from, organization sources. For example, organizations should ensure that all organization email is stored on organization servers and not solely on the BYOD devices.[11] In addition, the need for all data relevant to the organization to be stored within the organization, and not just on employee-owned devices, extends to other data sources, such as text messages, which can present additional hurdles for the employer. Complications associated with text messages may include difficulty regulating the use of text messages, the inability to easily store text messages within the organization, privacy concerns of employees who may use their BYOD device to text for both personal and work purposes, and the difficulty and expense of accessing old text messages. Nonetheless, employers can limit these issues by crafting BYOD policies that restrict employees' ability to send work-related texts on BYOD devices and instead require the use of organization-sanctioned texting systems.

Because discovery of BYOD devices is generally subject to a proportionality and reasonableness test, if an organization can demonstrate that an employee's BYOD device only contains information that is largely duplicative of that contained on organization servers, it may reduce the

[8] *Id.* at 11.

[9] *Id.* at 11-16.

[10] *Id*. at 23-24.

[11] See *id.*

likelihood that the organization would be required to produce information stored on BYOD devices.[12] Likewise, BYOD protocols should clarify that the organization does not have possession, custody, or control of information contained on BYOD devices. That being said, because tests for determining possession, custody, and control vary by jurisdiction, so too might the effectiveness of these disclaimers. By implementing thorough and thoughtful BYOD protocols, organizations can limit their exposure to employee-owned device discovery.

Conclusion:

Given the increasing attention being paid to BYOD discovery issues, organizations are best advised to weigh the practical and legal implications carefully when determining whether to allow employees to use their personal devices for work purposes. **If an organization does choose to allow or require its employees to use BYOD devices, it is in the organization's best interest to implement clear policies that set reasonable expectations between the employer and the employee and best position the organization to defend against potentially costly employee-owned device discovery**.

For More Information:

To learn more about how the discoverability of employee-owned devices could impact your business, please contact a Polsinelli Commercial Litigation Attorney.
Or for more information about BYOD policies or to have your existing policies reviewed, please contact a Polsinelli Labor & Employment Attorney.

12 *See id.* at 23-25.

Learn more...

For questions regarding this alert or to learn more about how it may impact your business, please contact one of the authors, a member of our **Commercial Litigation** practice, or your Polsinelli attorney.

To learn more about our **Commercial Litigation practice**, or to contact a member of our Commercial Litigation team, visit http://www.polsinelli.com/services/commercial-litigation or visit our website at polsinelli.com.

About this Publication