New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 260—NO. 26
TUESDAY, AUGUST 7, 2018

FEDERAL E-DISCOVERY

Commentary Provides Guidance On BYOD Discovery

By **Christopher Boehning**
And **Daniel J. Toal**

Two years ago in this space we observed that personal devices were becoming part of the new discovery normal. Such devices, often managed by organizations as part of a "Bring Your Own Device" (BYOD) program, were—and are—increasingly used for work purposes and, thus, ever more likely to contain electronically stored information (ESI) potentially relevant to a litigation or investigation. In 2016, scant direction existed for organizations looking to structure a BYOD program with e-discovery requirements in mind, and there was even less guidance for courts confronted with requests for discovery of ESI on such devices.

SHUTTERSTOCK

That has changed thanks to a new publication from The Sedona Conference (Sedona), the leading think tank on issues relating to law and best practices on the discovery of ESI. Sedona has evolved the discussion of discovery of ESI from personal devices used for work with its publication, "The Sedona Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations" (the Commentary). The Commentary provides important guidance to organizations, practitioners, and courts, stressing the concept that personal devices used for work can be excluded from both preservation and discovery if an organization can reasonably conclude such devices do not contain ESI that is both relevant and unique.

The BYOD Commentary

As with many of Sedona's publications, the Commentary is structured as a set of principles, with comments to each principle and analysis in the context of each comment. There are five principles, the first two of which are designed to guide organizations

CHRISTOPHER BOEHNING *and* DANIEL J. TOAL *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison.* ROSS M. GOTLER, *e-discovery counsel, and* LIDIA M. KEKIS, *e-discovery attorney at the firm, assisted in the preparation of this article.*

in determining when and how to develop and implement a BYOD program. Principles 3, 4, and 5 focus on discovery of ESI from personal devices used for work.

- 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, BYOD.
- 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 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 for discovery.

Principle 3 introduces a cornerstone of the Commentary, the notion that personally-owned devices that contain "unique, relevant ESI" are appropriately considered as sources for discovery. The Commentary notes that "[w]hether and how that device may become an appropriate data source for discovery in litigation is subject to numerous considerations, including the way ESI is stored on a BYOD device; whether that ESI is duplicative of other ESI on the organization's systems; and how effectively segregated that ESI is from the user's personal information." It provides a framework for counsel to conduct due diligence in making such determinations, including:

In 2016, scant direction existed for organizations looking to structure a "Bring Your Own Device" program with e-discovery requirements in mind, and there was even less guidance for courts confronted with requests for discovery of ESI on such devices. That has changed thanks to a new publication from The Sedona Conference, the leading think tank on issues relating to law and best practices on the discovery of ESI.

- If the ESI is within the employer's possession, custody or control—a complex determination that may vary across circuits.
- Whether the ESI is both relevant and unique, or, if instead there is other ESI that is more readily available from other sources.
- Whether the discovery of the ESI is proportional to the needs of the case, especially in light of the 2015 amendments to the Federal Rules of Civil Procedure.

The impact on an employee's privacy interests, including balancing data privacy protections with discovery obligations.

An appropriate due diligence effort, notes the Commentary, is the basis for defensible representations to the court and to opposing counsel regarding the discoverability of such devices.

Principle 4 then guides potential future litigants in shaping their BYOD policies and practices to minimize the storage of unique, relevant ESI on employee-owned devices and to facilitate the collection of such ESI if needed. The Commentary encourages organizations to proactively manage the devices, stating that "[p]roactive BYOD management can reduce discovery costs by limiting or excluding unique ESI from the BYOD device (where practical), and striving to ensure that all organization ESI transmitted, received, or stored on the BYOD device is also captured and retained on the organization's network servers or other centralized storage locations under the organization's control, where preservation and search functions can be addressed in a targeted and efficient manner."

The final principle, Principle 5, has perhaps the potential for the most

impact on e-discovery practice. The inverse of Principle 3, Principle 5 explicitly states that "[e]mployee-owned devices that do not contain unique, relevant ESI need not be considered sources for discovery." Organizations that follow the guidance in the Commentary that precedes Principle 5 would be in a position to reasonably assert that employee-owned devices that are part of their proactively managed BYOD program can be excluded from discovery-related preservation and collection. As stated in the Commentary, "efforts related to discovery of BYOD devices should target the unique, relevant ESI on such devices. It is now well-accepted that discovery of relevant information is limited in scope to exclude duplicate copies of otherwise responsive ESI, as long as none of the copies have independent value. Thus, if there is a reasonable basis to believe that personally-owned devices do not contain unique, relevant information, the organization should not be required to preserve or collect ESI from those devices."

The Commentary notes that the existence of such a reasonable basis can be demonstrated in various ways, including:

- The use of custodian interviews and inquiries to confirm that all relevant communications are in email messages that are preserved and available on the organization's central server, eliminating the need for copying BYOD devices.

- Ensuring that the BYOD policy incorporates "technology controls reasonably designed, with due care and in good faith," that block the ability to store unique, relevant ESI on BYOD devices. In such instances, preservation and collection efforts should, instead, target the most accessible copies of the ESI from other sources like active email files or archives.

Even with strong policies and practices in place and despite an organization's reasonable efforts, there is always the possibility that, limited "instances of unique, relevant ESI" may reside on an employee-owned BYOD device. An example would be an email attachment that was downloaded to the device that no longer exists in the organization's email systems (perhaps due to retention policies in place prior to a legal hold). Citing the support of many courts for the standard of discovery to be reasonableness, not perfection, the Commentary provides guidance in such a situation, explaining that "[t]he mere possibility or existence of such ESI, in the absence of a compelling need or showing, should not require an organization to take additional steps to preserve and collect ESI on BYOD devices."

Conclusion

The BYOD Commentary brings much needed guidance to an aspect of e-discovery practice that has long vexed parties and has often led to significant expenditures on preservation, collection, and processing—with minimal return. With its emphasis on encouraging proactive management of BYOD programs and on reasonable discovery practices that target unique, relevant ESI, the Commentary has the potential to impact discovery-related decision making in organizations that often wrestle with such issues.