

# *The Sedona Conference Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*

*The Sedona Conference*



The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complimentary basis to courthouses and public law libraries. Additionally, each issue is available for purchase (\$45; \$30 for Working Group Series members). Send us an email ([info@sedonaconference.org](mailto:info@sedonaconference.org)) or call (1-602-258-4910) to order or for further information. Check our website for further information about our conferences, Working Groups, and publications: [www.thesedonaconference.org](http://www.thesedonaconference.org).

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:

The Sedona Conference,  
301 East Bethany Home Road, Suite C-297, Phoenix, AZ 85012 or  
[info@sedonaconference.org](mailto:info@sedonaconference.org) or call 1-602-258-4910.

The Sedona Conference Journal® designed by MargoBDesignLLC at  
[www.margobdesign.com](http://www.margobdesign.com).

Cite items in this volume to "19 Sedona Conf. J. \_\_\_\_ (2018)."

Copyright 2018, The Sedona Conference.  
All Rights Reserved.

THE SEDONA CONFERENCE COMMENTARY ON BYOD:  
PRINCIPLES AND GUIDANCE FOR DEVELOPING POLICIES  
AND MEETING DISCOVERY OBLIGATIONS

---

*A Project of The Sedona Conference Working Group on  
Electronic Document Retention and Production (WG1)*

*Author:*

The Sedona Conference

*Drafting Team:*

Andrea D'Ambra	Mark Michels
Emily Fedeles	Jessica C. Neufeld
Katelyn Flynn	Matthew Prewitt
Ross Gotler	Lauren E. Schwartzreich
Peter B. Haskel	Ryan Wasell
Heather Kolasinsky	

*Drafting Team Leaders:*

Alitia Faccone	David Moncure
----------------	---------------

*WG1 Steering Committee Liaisons:*

Dean Kuckelman	Ronni D. Solomon
----------------	------------------

*Copy Editor:*

Susan M. McClain

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of The Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers,

---

Copyright 2018, The Sedona Conference.  
All Rights Reserved.

clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the “Sponsors” navigation bar on the homepage of our website.

This publication may be cited as follows:

The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495 (2018).

## PREFACE

Welcome to the final, May 2018, version of The Sedona Conference *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The public comment version of this Commentary was published in January 2018 and stems from the increasing practice of Bring Your Own Device (BYOD), where organizations permit or encourage workers to use their own personal devices to access, create, and manage organization information. After a 60-day public comment period, the editors reviewed the public comments received and, where appropriate, incorporated them into this final version.

BYOD is often accomplished through a BYOD program that includes formal or informal rules and guidelines. This Commentary is designed to help organizations develop and implement workable—and legally defensible—BYOD policies and practices. This Commentary also addresses how creating and storing an organization's information on devices owned by employees impacts the organization's discovery obligations.

On behalf of The Sedona Conference, I want to thank all of the drafting team members for their dedication and contributions to this project. Team members that participated and deserve recognition for their work are: Andrea D'Ambra, Emily Fedeles, Katelyn Flynn, Ross Gotler, Peter B. Haskell, Heather Kolasinsky, Mark Michels, Jessica C. Neufeld, Matthew Prewitt,

Lauren E. Schwartzreich, and Ryan Wasell. The Sedona Conference also thanks Alitia Faccone and David Moncure for serving as the Drafting Team Leaders, and Dean Kuckelman and Ronni D. Solomon for serving as Steering Committee Liaisons.

In addition, we encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent litigation best practices; data security and privacy liability; trade secrets; and other “tipping point” issues in the law. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at <https://thesedonaconference.org/wgs>.

Craig Weinlein  
Executive Director  
The Sedona Conference  
May 2018

**TABLE OF CONTENTS**

I.	INTRODUCTION.....	502
II.	BYOD PRINCIPLES.....	508
III.	COMMENTARIES TO BYOD PRINCIPLES.....	509
	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.....	509
	Comment 1.a. Organizational factors to consider include the organization's workforce, size, and technical support.....	509
	Comment 1.b. Legal factors to consider include limitations on the organization's ability to access data on the device.....	512
	Comment 1.c. Significant legal implications may result if the organization is unable to access its business information on employee-owned devices.....	515
	Comment 1.d. Organizations should consider how they will protect their business information.....	515
	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.....	518
	Comment 2.a. A BYOD policy should be designed to advance the organization's objectives. ....	518
	Comment 2.b. A BYOD policy should clearly state the organization's expectations.....	518
	Comment 2.c. Organizations should consider requiring employees to agree to the terms of the BYOD policy.....	519

Comment 2.d.	The BYOD program should protect the organization's business information. ....	521
Comment 2.e.	The BYOD program should consider employees' privacy interests. ....	525
Comment 2.f.	The BYOD program should consider employees' protected personal information. ....	526
Principle 3:	Employee-owned devices that contain unique, relevant ESI should be considered sources for discovery. ....	528
Comment 3.a.	Factors to determine whether ESI on an employee-owned device is discoverable include: whether the ESI is within the employer's possession, custody, or control; whether the ESI is unique; and whether the discovery of the ESI is proportional to the needs of the case. ....	528
Comment 3.b.	An organization's BYOD program can impact whether the organization has possession, custody, or control over ESI on employee-owned devices, but the legal test may vary widely by jurisdiction. ....	530
Comment 3.c.	Even if ESI on a mobile device is relevant, the ESI is not within the scope of discovery if it can be collected from a more accessible source. ....	532
Comment 3.d.	The concept of proportionality also limits the scope of discovery of ESI on employee-owned devices. ....	534
Comment 3.e.	Organizations should consider their employees' privacy interests before collecting ESI from employee-owned devices. ....	538



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. ....	540
Comment 4.	Organizations should proactively manage employee-owned devices. ....	540
Principle 5:	Employee-owned devices that do not contain unique, relevant ESI need not be considered sources for discovery. ....	542
Comment 5.a.	Responding parties should make reasonable efforts to determine whether mobile devices contain unique, relevant ESI. ....	542
Comment 5.b.	BYOD programs can give organizations a reasonable basis to believe that employee-owned devices do not contain unique, relevant ESI. ....	544
Comment 5.c.	Parties and courts should take reasonable steps to protect business information in cases where the organization is not a party.....	546
APPENDIX A: DEPARTMENTAL COLLABORATION GUIDE.....		548
APPENDIX B: BYOD IN THE INTERNATIONAL CONTEXT .....		555

## I. INTRODUCTION

### A. *The Growth of BYOD*

Mobile computing has obscured the once distinct boundaries between the workplace and private life. Twenty years ago, when an organization hired a new employee, it assigned the employee a desktop computer and a landline phone. Now, either as part of cost-cutting efforts or to accommodate worker preferences, organizations are permitting or encouraging workers to use their own personal devices to access, create, and manage their information—often after hours and outside the office. This practice is commonly referred to as “Bring Your Own Device” or “BYOD,” and is often accomplished through a BYOD program that includes a BYOD policy and practices. Those BYOD programs may *require* employees to use their own devices to conduct the organization’s business. The devices that are owned and used by the employees to access the organization’s emails and documents typically include smartphones and tablet computers, but can also include personal laptops or desktops that access organization information through virtual private networks (VPNs) or other remote access technologies. This Commentary addresses how creating and storing the organization’s information on devices that are owned by the employee impact the organization’s discovery obligations and security goals.

Several factors have driven the rise of BYOD programs in recent years. For example, today’s rapid technological developments in mobile technology motivate workers to purchase their own sophisticated devices rather than wait for their employer’s information technology (IT) upgrade program. And workers purchase those devices with the expectation that they can use them for both personal and business purposes. Also, some organizations have adopted a BYOD policy so they do not have to pay for the devices, but many have found that this just shifted

IT expenditures from device purchases to software intended to protect and manage data on those devices.

Another factor driving BYOD adoption is advances in device security, which has made some organizations more comfortable with permitting access to sensitive data from employees' personal mobile devices. Security measures common to today's mobile devices may greatly reduce the risk that an employee's lost device will expose organization emails or other proprietary data. Mobile device management (MDM) software can be used to require security authentication and to segregate personal information from the organization's data. MDM software also lets organizations remotely wipe the device if it is lost or stolen.

*B. The Scope of These Principles and Commentary*

This Commentary applies specifically to mobile devices that employees "bring" to the workplace. It does not address all of the programs that govern employees' use of mobile computing devices, such as:

- BYOA (Bring Your Own Access—where employees provide their own wireless access to an organization's systems usually through mobile hotspots);
- BYOE (Bring Your Own Encryption—a cloud computing security process where employees use their own encryption software and encryption keys to access a cloud-based organization system);
- BYOI (Bring Your Own Identity—where employees utilize third-party systems (usually social networking sites) as their credentials for accessing organization systems, e.g., "login using Facebook");
- BYON (Bring Your Own Network—where employees create their own personal network instead of utilizing the organization's network); or

- BYOW (Bring Your Own Wearable—where employees utilize wearable technology such as Apple watches to access organization systems or perform certain job functions).

Furthermore, this Commentary does not specifically address programs where the employer provides the mobile device, or programs where employees can select a device from an authorized provider and then get reimbursed by the organization for the cost of either the device or monthly service, or both. However, many of the concepts discussed in this Commentary apply to any program that results in business information being created and stored outside of the office or the organization's servers.

Additionally, although this Commentary focuses on organizations, the discovery obligations for unique, relevant, and proportional electronically stored information (ESI) on mobile devices applies to organizations and individuals alike.

### *C. The Structure and Purpose of this Commentary*

This Commentary begins with five principles related to the use of BYOD programs and continues with commentary for each. The first two principles and related commentary address determining whether a BYOD program is the right choice for an organization, followed by basic information governance requirements for BYOD—security, privacy, accessibility, and disposition—from the perspective of both domestic and global organizations. Against this backdrop, the principles and commentary then turn to preparing for and responding to discovery obligations under the prevailing U.S. approach to discovery.

There is no one-size-fits-all BYOD for every organization. While recognizing that BYOD is not viable for some organizations, this Commentary is cautiously optimistic that careful

planning and implementation can substantially reduce the risks associated with BYOD for many organizations. The principles encourage parties in litigation and investigations to approach BYOD discovery in a manner that both respects and rewards organizations that engage in proactive, responsible BYOD management.

This Commentary embraces a forward-looking approach to BYOD as a permanent trend that is driven by IT's transformation of both the workplace and society as a whole. This Commentary seeks to provide guidance to organizations on developing and implementing an approach to BYOD that meets the specific needs of the organization and addresses security, privacy, accessibility, and litigation. Organizations that responsibly pursue these goals should be able to proceed with confidence that their reasonable efforts will be respected by courts and will not be undermined by disproportionate discovery burdens.

*D. Evaluating Whether to Allow BYOD, and How to Develop a BYOD Program*

Principles 1 and 2 are designed to help guide an organization in deciding: (1) whether to allow (or even require) BYOD; and (2) how to develop and implement a BYOD program. Some organizations may find that BYOD is not suitable at all, while others may decide to adopt BYOD for only a portion of their personnel. This threshold decision should be based on the specific needs and resources of each organization. Among the relevant factors an organization should consider are the:

- impact that a BYOD program would have on the costs and risks of discovery;
- sensitivity of the information that would be accessed or stored on the devices;

- organization's legal obligations to restrict disclosure or use of the data;
- ability of the organization to exercise practical and legal control over the data;
- available technology for maintaining data security;
- receptiveness of BYOD users to usage restrictions; and
- in-house resources for user training and support.

For most organizations, BYOD will require balancing competing considerations of data access, security, privacy, cost, and the impact on discovery. Organizations should balance the privacy interests of individuals and the organization's own business needs and legal obligations. Even where an organization has a clear right to access and use the personal information of its employees, it should carefully consider its legal obligations.

If the organization decides to allow BYOD, it should have a policy that tells its employees what the rules are regarding the access, use, and storage of the organization's data on employee-owned devices. Otherwise, employees are left to guess at what is acceptable, and the organization subjects itself to unnecessary cost and risk.

#### *E. Discovery of ESI from BYOD*

Principles 3 and 5 address discovery obligations, and Principle 4 explains that organizations likely to be subject to those discovery obligations should consider discovery preparedness when creating BYOD programs. This preparedness should include a policy and practices that limit or prevent unique ESI from being stored on the device. As used in this Commentary, "discovery" includes preservation, collection, review, and production of ESI for litigation or government investigations.

More specifically, Principle 3 explains that relevant ESI on employee-owned devices may be subject to discovery—like all other ESI. Parties cannot ignore their discovery obligations merely because the ESI is on a device that is mobile or owned by an employee. Conversely, Principle 5 explains that ESI that is not relevant or not unique is not subject to discovery from employee-owned devices. In addition to relevance, there are three threshold issues that require special consideration when determining whether ESI on employee-owned devices is subject to discovery: (1) whether the organization has possession, custody, or control over the ESI; (2) whether the ESI is unique or duplicative of other ESI that is more readily accessible; and (3) whether discovery of the ESI is proportional.<sup>1</sup> Although these concepts have broader application beyond BYOD, in this Commentary, we address them solely in the context of ESI on employee-owned devices. We also provide examples and circumstances where courts have and have not found ESI to be discoverable.

---

1. Proportionality, and possession, custody, and control, are the subjects of two recent Sedona publications: The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141 (2017); The Sedona Conference, *Commentary on Rule 34 and Rule 45 “Possession, Custody, or Control,”* 17 SEDONA CONF. J. 467 (2016).

## II. BYOD PRINCIPLES

- 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.



### III. COMMENTARIES TO BYOD PRINCIPLES

**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.**

*Comment 1.a. Organizational factors to consider include the organization's workforce, size, and technical support.*

Organizations should consider numerous organizational factors before adopting a BYOD policy, beginning with an assessment of the benefits of BYOD to employees and the organization along with the risks of allowing BYOD. An organization should assess the role of the individual employee within the organization and whether some or all of its employees would benefit from mobile connectivity and access to organization systems beyond the confines of the organization's offices. Some employees may welcome the flexibility and convenience of BYOD, while others may view it as an infringement on work/life balance or an unfair expense imposed by the employer. For many types of workers, mobile access may provide only slight benefit while substantially increasing the risks to the organization. For example, an organization employing cashiers in a retail establishment may find little benefit from giving those cashiers access to the organization's systems when away from their work station (indeed, such access could compromise financial controls). The interests of that organization may be best served by prohibiting BYOD. Conversely, a retail store manager may benefit herself and the organization by being able to access email remotely by mobile device or home computer and quickly respond to emergency situations arising outside normal working hours.

An organization should also assess the types of information that may be accessed by employees who participate in a BYOD program. Some employees may use information that is so highly sensitive that the organization may not want to risk letting them have BYOD access to that information. The organization should consider allowing BYOD for some types of information but prohibiting it for other types of information.

An organization's size and ability to absorb internal IT costs may factor into the decision whether to adopt BYOD. The larger the scale of a business and the more employees who need mobile connectivity, the more attractive a BYOD program may initially appear because the organization can avoid paying for thousands of mobile devices. However, even those organizations that do not pay for mobile devices incur costs associated with BYOD, for example the costs of implementing mobile device management (MDM) software, providing the requisite technical support to assist users in accessing organization systems, and ensuring appropriate security measures are in place.

An organization should also consider the consequential or hidden costs associated with building an infrastructure that can support a BYOD program. In some cases, the risks and the costs may offset or exceed any savings the organization expects to enjoy from adopting the program. For example, organizations that are parties to litigation may incur additional discovery costs to collect, review, and produce ESI from employee personal devices to the extent the information is relevant and unique, a distinction discussed further in Principles 3 and 5. Discovery burdens may be particularly onerous if an organization's operations span a large geographic area, and the unique, relevant ESI contained on the devices necessitate collection or imaging of such devices in multiple locations. The devices may need to be shipped to a vendor or the vendor may need to go onsite. Onsite mobile device acquisition where the devices are

geographically dispersed can be costly, requiring either multiple vendors to cover each location, or the added cost of travel by a single vendor to multiple locations. Shipping devices is no panacea. The loss of use while a device is being shipped for collection—and providing a temporary substitute device—can also increase costs and cause business interruption. These costs and challenges can become compounded when an organization's operations include jurisdictions with strict data privacy regulations.

Companies should also consider whether they have adequate in-house (or outsourced) technical support to assist employees with accessing organization systems through MDM software, or otherwise. The organization's technical or litigation support group should be able to implement appropriate security protocols to protect against intrusion into organization systems through mobile device malware<sup>2</sup> or operating system vulnerabilities.<sup>3</sup>

In the case of litigation or regulatory disclosure requirements (including public records requests for government employers), an organization's litigation support should also be prepared to identify, secure, and work with appropriate service providers, as needed, to facilitate defensible collection of ESI from BYOD devices that contain unique, relevant information.

Various departments within an organization, including Finance, Human Resources (HR), Information Governance (IG),

---

2. See, e.g., Leon Spencer, *16 million mobile devices hit by malware in 2014: Alcatel-Lucent*, ZDNET (Feb. 13, 2015), <http://www.zdnet.com/article/16-million-mobile-devices-hit-by-malware-in-2014-alcatel-lucent>.

3. See, e.g., Don Reisinger, *Most Android phones at risk from simple text hack, researcher says*, CNET (July 27, 2015), <http://www.cnet.com/news/researcher-finds-mother-of-all-android-vulnerabilities>; Jose Pagliery, *The text you never want to get on your iPhone*, CNN MONEY (May 28, 2015), <http://money.cnn.com/2015/05/27/technology/iphone-text-message-hack>.

Information Technology (IT), Legal/Compliance, and Security should work collaboratively to discuss these considerations and develop a BYOD policy, procedures, training, and enforcement programs. *See* Appendix A, *infra*, describing the various roles and questions for stakeholders from these departments.

***Comment 1.b. Legal factors to consider include limitations on the organization's ability to access data on the device.***

Organizations should understand the legal limitations on their ability to access ESI on an employee-owned device, which may vary by jurisdiction. For example, data protection laws, labor laws, and other laws and policies (e.g., Works Council rights, bargaining agreements, and telecommunications laws) can delay or even prohibit employer demands to access ESI that exists on employee personal devices.

How an organization will obtain access to information on the employee-owned device—including whether it will need to take physical possession of the device—should be a central consideration when deciding whether to allow, or even require, BYOD. The ability to access the information may vary from device to device and employee to employee. At the very least, access to information is complicated by the defining characteristic of BYOD—the employer doesn't own or possess the device.<sup>4</sup> An organization should therefore consider that it may not be able to obtain access to the contents of employee-owned devices when a need arises.

Organizations face a wide range of possible obstacles to obtaining information from employee-owned devices, including the following:

---

4. *See infra* Comment 3.b. for a discussion of whether an employer has legal possession, custody, or control over ESI on employee-owned devices.

1. Employees may refuse to hand over the personal device, or refuse to provide passwords needed to access data on the device.
2. Even employees who want to cooperate may be unable to provide complete access, e.g., if portions of devices are locked by device manufacturers.
3. Device backups and related device data may be stored in a computer or system that is separate from the device and inaccessible to the employee or employer.
4. An employee's network or cellular service provider may limit the amount and type of information available to a device user if the user is not the primary subscriber of the account or is otherwise not entitled to information the service provider possesses concerning the device (e.g., call records, location information, text messages, voicemail, etc.).
5. The employee may not actually own the device, or the employee may own it jointly with others who may not consent to employer requests concerning the device (e.g., the phone may be owned by a family member, or the cellular service provider may lease the phone to the employee).

Many organizations attempt to increase their ability to access employee-owned devices by making their employees consent to such access as a precondition to employee participation in a BYOD program. A determination of whether this qualifies as "consent" may vary depending on jurisdiction and the facts at issue in the case, including the access sought by the employer. Questions bearing on this issue include the following:

1. Does the employee have an individualized right to privacy that would prevent or negate an employer's assertion of voluntary consent?
2. Does consent by the employee extend to personal information on the device that is not related to his or her employment?
3. When may an employee withdraw consent?
4. If employee consent is considered a quid pro quo element in an exchange between the employer and employee, is there sufficient consideration given by the employer? If providing continued employment is the consideration given by the employer, does the employee's consent necessarily terminate when the employment relationship ends?
5. Does employee consent extend to ancillary locations to which a device is associated? For example, when an employee synchronizes or backs up a device to a home computer or network, does the consent extend to these ancillary locations? Is the employee authorized to provide consent on behalf of all other users of related ancillary locations? These considerations may be magnified in the BYOD context given that consumer devices are often highly integrated with consumer accounts and storage environments in which third-party providers seek to consolidate functions and information within a technology ecosystem (e.g., Apple, Google, Microsoft, and Amazon all provide devices and services which integrate hardware, operating systems, applications, cloud storage, and other services with a user's various accounts and information).

When evaluating whether to allow or require BYOD, an organization should consider how it will balance the privacy interests of its employees against the organization's needs and obligations. Even where an organization has a legal right to access and use the private information of its employees, it would be wise to do so with care, and upon full consideration of the impact that it will have on its employees. Duties to protect data from misuse or disclosure apply in the BYOD context, not necessarily to a greater degree than in other workplace situations, but with a heightened risk of failure given the mobile nature of devices and the extent of commingling that can occur between employer and employee information.

***Comment 1.c. Significant legal implications may result if the organization is unable to access its business information on employee-owned devices.***

As explained in Comment 3.b., *infra*, whether the organization has the legal right to access ESI on the devices may have a significant impact on whether the organization has a legal obligation to preserve, collect, or produce the ESI in litigation or government investigations. An organization may, in some jurisdictions, reduce the cost and risk of discovery if it does not have a legal right to take the device or access the ESI on the device. However, not having those rights or access can create significant problems for the organization. These problems can include the inability to protect the organization's intellectual property, or get information from personal devices as part of internal investigations.

***Comment 1.d. Organizations should consider how they will protect their business information.***

BYOD programs present significant security challenges. As noted by the National Institute of Standards and Technology (NIST), many organizations have "established boundaries to

separate their trusted internal IT networks(s) from untrusted external networks. When employees consume and generate corporate information on mobile devices, this traditional boundary erodes.”<sup>5</sup> Furthermore, mobile devices, in particular, are a significant source of data breaches.<sup>6</sup> Additional security concerns may arise when users access cloud applications through their devices because malware may be contained in public cloud applications and programs.<sup>7</sup> BYOD devices may also raise heightened security concerns because they co-mingle both personal information and organization information.

Many of the security risks associated with BYOD are inherent in the use of any mobile device with an internet connection. Traditional risks from theft, hacking, and user negligence are ever present on an organization’s non-BYOD devices and networks. BYOD enhances those risks, however, because technical and administrative protections are substantially more difficult

---

5. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [hereinafter NIST], U.S. DEPT. OF COMMERCE, *Mobile Device Security for Enterprises*, Building Block 1, V.2 – Final Draft, at 1 (Sept. 12, 2014), available at [https://nccoe.nist.gov/sites/default/files/nccoe/MobileDeviceBuildingBlock\\_20140912.pdf](https://nccoe.nist.gov/sites/default/files/nccoe/MobileDeviceBuildingBlock_20140912.pdf).

6. Mobile security breaches have affected more than two-thirds (68 percent) of global organizations in the last 12 months. See BRITISH TELECOM, *Art of Connecting: BT Security research on mobile security threats* (October 2014), available at [http://www.globalservices.bt.com/static/assets/pdf/articles/en/bt\\_security\\_research\\_on\\_mobile\\_security\\_threats\\_october\\_2014.pdf](http://www.globalservices.bt.com/static/assets/pdf/articles/en/bt_security_research_on_mobile_security_threats_october_2014.pdf).

7. When asked to identify the trends that most impact their security programs, IT professionals revealed that the malware threat and its associated data breach risk is likely to get worse over the coming years specifically because of the (1) continuing evolution of BYOD practices and (2) increasing adoption of cloud technology, both public and private. See Elden Nelson, Wisegate, *BYOD and cloud are top data breaches and malware risks, survey shows*, CSO (Apr. 6, 2015), <http://www.csoonline.com/article/2906359/data-breach/byod-and-cloud-are-top-data-breaches-and-malware-risks-survey-shows.html>.



to develop and implement in a BYOD environment. For example, the organization's own devices may have controls that restrict access to certain websites, particularly those that may contain malware. However, these access controls may be missing on a BYOD device, thereby enhancing the risk the device will become infected with malware. If the employee connects an infected personal device to the organization's network or sends an infected file from a personal device to an organization's network, the infection could spread to that network and to its data absent protective measures.

Issues also arise when employees view BYOD devices as within their exclusive control and believe they possess unrestricted and unlimited rights to do as they see fit. For example, an employee may more readily use a personal device on an unsecured public Wi-Fi network; share the device with friends and family without any protection for organization data; lose, sell, or trade-in the device without wiping data; or open phishing communications containing malware. For these reasons, BYOD should be subject to at least the same level of security, if not greater security, than employer-issued devices.

An organization should consider the technical sophistication of the work force that may use personal mobile devices for work-related purposes. A more technically-sophisticated work force, such as software developers or engineers, may utilize more advanced applications that may integrate organizational tools with organization data (such as tasking reminder tools, translation tools, or email/calendar clients). This type of usage can drive additional risks with respect to the security of the ESI shared with these applications and may drive an organization to adopt a BYOD policy and IT services which limit the amount of ESI and the manner in which such ESI is shared. Less techni-

cally-sophisticated workers might limit their mobile device usage to social media applications, texting, emailing, voicemail, and taking pictures.

**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.**

*Comment 2.a. A BYOD policy should be designed to advance the organization's objectives.*

Organizations that decide to allow or require BYOD should design and implement a BYOD program that maximizes the benefits that motivated the organization to allow BYOD in the first place, while mitigating the risks and costs of BYOD. The BYOD program should strive to achieve a reasonable balance between improving efficiency and protecting business information and, at the same time, safeguarding personal information. The organization's key objectives in this respect are gains in productivity, reduction in technology and other costs, as well as increased employee satisfaction. Other organizational benefits include increased workplace productivity, and increased flexibility for employees to determine how to fulfill their job responsibilities.

To achieve these objectives, both the organization and its employees should understand their respective responsibilities.

*Comment 2.b. A BYOD policy should clearly state the organization's expectations.*

Organizations should carefully consider all facets of a BYOD program, from deciding to allow or require BYOD, to designing, implementing, and administering the written BYOD policy. The policy should be written in a way so that employees can easily

understand and comply with it, and be coordinated with the organization's acceptable use and information security policies. The BYOD program should also help employees protect their personal data. Key steps toward fulfilling these goals include: ensuring that a policy complies with applicable labor and technology laws; drafting clear technology and personnel rules, and effectively communicating those rules to employees; providing appropriate training to employees to use BYOD devices consistent with policies and to update applications and hardware to keep up with security standards; and ensuring that employees have access to and know how to access the information they will need whenever questions or problems arise.<sup>8</sup> Addressing non-compliance in a timely manner will help employees understand and appreciate the organization's expectations.

***Comment 2.c. Organizations should consider requiring employees to agree to the terms of the BYOD policy.***

Where practical, organizations should clarify their employees' rights and obligations by requiring employees to execute consents, authorizations, or end-user agreements as a condition

---

8. An excellent example of a good reason for an employer to adopt a BYOD policy is presented in *Rajae v. Design Tech Homes, Ltd.*, No. H-13-2517, 2014 WL 5878477 (S.D. Tex. Nov. 11, 2014). There plaintiff claimed that his former employer unlawfully wiped ESI from his iPhone in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the Stored Communications Act component of the Electronic Communications Privacy Act, 18 U.S.C. § 2701. The employer eventually prevailed, but an established BYOD policy that the employee's device, if used in business, would be wiped on termination of employment likely would have avoided litigation entirely. See also Brian Hall, *Texas Federal Court decision illustrates need for BYOD policies*, TECHNOLOGY LAW SOURCE (Nov. 25, 2014), <http://www.technologylaw-source.com/2014/11/articles/information-technology/texas-federal-court-decision-illustrates-need-for-byod-policies>.

for participation in a BYOD program. When drafting and implementing those documents, organizations may want to incorporate the following concepts:

1. Clearly set out the circumstances for, and the types of, information that can be stored on the device, and how that information could be subject to monitoring, access, or deletion by the organization.
2. Address ownership and costs of the device and data, including intellectual property licensing considerations and termination of the employment relationship.
3. Explain that unique, relevant ESI may be subject to discovery. Discourage storing unique ESI on the device. *See Comment 4, infra.*
4. Identify acceptable use restrictions and the consequences for violating an organization's general computing use policies, such as potential loss of privacy rights in some jurisdictions.
5. Identify steps taken by the organization to segregate personal and business information. Employees should be informed about any device management policies and software.
6. Address the potential for litigation, investigation, regulatory disclosures, and other potential disclosure obligations, and the expectation for access to both the device and the ESI stored on it. The organization should carefully consider the implications of insisting on access to the device and data on the device. Additionally, highlight the potential for waiver of privilege if the employee fails to protect the confidentiality of the privileged ESI.

7. Explain security measures that are in place to protect both business and personal information on the device as well as the device itself.
8. Address privacy to be consistent with other organization policies, including information management policies, employee benefit plans, and others specific to the organization.
9. Address the user's obligation to update certain applications or install patches when issued.

***Comment 2.d. The BYOD program should protect the organization's business information.***

To protect business information, an organizer should consider developing security policies, practices, and procedures that address data sensitivity (e.g., business value, legal, regulatory and contractual obligations, etc.) and how employees should handle their devices. These BYOD policies, practices, and procedures should take into consideration the organization's tolerance for assuming security risks, and should also be integrated into an organization's overall security policy.

Experience has repeatedly demonstrated that a strict BYOD security policy that is not integrated into an organization's overall security policies will merely negate the efficiency and other potential benefits of BYOD use and potentially leave the organization's data exposed. It also may incentivize employees to "work around" the BYOD policy.

Security policies may need to be more extensive and intrusive as the sensitivity of the information device increases.<sup>9</sup> The

---

9. For example, NIST has developed a draft guide to demonstrate how to implement security technology for electronic health records. NIST, *SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES, HOW-TO GUIDES FOR SECURITY ENGINEERS*, Public Comment Draft (July 2015), available at

policy should address acceptable device types, access controls, software requirements, the purchase of new devices and disposition of old ones, reporting loss or theft of a device, and post-termination protocols.<sup>10</sup> Security policies should also address cloud access because malware may be contained in public cloud applications and programs. In some cases, organizations may place limitations on taking devices outside of the country if highly sensitive data may be stored on the device.<sup>11</sup>

Most security policies have multilevel security components. These security components may include device encryption, in addition to any other device security features. Other security features may include network access restrictions and device activity monitoring. Security protocols may require device registration on the organization's network.<sup>12</sup> Registration provides for identification of "rogue" devices, device tracking, and access logging, which may be useful in the event of a data breach, investigation, or litigation need. Security policies may also include backup procedures and processes for deploying software security updates, upgrades, and patches.

Security policies may differ depending on whether the organization permits commingling of organizational ESI with per-

---

<https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1c-draft.pdf>.

10. For an in-depth discussion of mobile device security practices, see Murugiah Souppaya & Karen Scarfone, NIST, *GUIDELINES FOR MANAGING THE SECURITY OF MOBILE DEVICES IN THE ENTERPRISE*, Special Publication 800-124 Rev. 1 (June 2013), available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf>.

11. *Id.* at 7.

12. This registration helps prevent unauthorized access to the network by assigning a unique identifier to the device, such as a serial number or the International Mobile Equipment Identity (IMEI) number, which the network then uses to determine if the devices attempting to connect are authorized.

sonal data on the device. Organizations may consider implementing software partitions (sometimes called “containers” or “sandboxes”), which segregate organizational from personal data on the device. Such containers or sandboxes are a standard feature in mobile device management (MDM) software that can be placed on BYOD (as well as organization-owned) devices.

According to NIST, “[c]entralized mobile device management technologies are a growing solution for controlling the use of both organization-issued and personally-owned mobile devices by enterprise users.”<sup>13</sup> These MDM tools use a messaging server’s management capabilities or third-party products.<sup>14</sup> Organizations may find advantages in using these MDM tools for devices to: 1) manage the data on the organizational side of a partition; 2) establish protocols for monitoring software and applications to determine whether there is malware on a device; 3) push software updates and bug fixes to a device, especially security-related updates and bug fixes; 4) permit remote wiping of a device if it is lost, stolen, or the user departs the organization; 5) monitor device activity to identify apps that may be prohibited by policy and identify malware and viruses and remediate them; and 6) provide for cloud-sync blocking.

BYOD security policies that employ MDMs may limit the users’ device choices to those that operate effectively with the MDM. This approach also may require the use of specific containerized applications for all organizational networks and data access. One area of particular concern is restricting device-to-device text messages of organizational data since this transmission may likely circumvent the security controls. The technology is developing too fast, and the range of organizational needs is too great to allow detailed suggestions here—the reader

---

13. See generally Souppaya & Scarfone, *supra* note 10, at 7.

14. *Id.*

should consult appropriate experts in designing and implementing any BYOD security policies.

Organizations should also consider employing a BYOD security policy training program. These programs describe potential security threats, explain the security policy, and identify policy compliance requirements. The training policy could identify training frequency and provide documentation verifying an individual's training compliance.

Similarly, organizations should consider conducting periodic security audits to evaluate the BYOD device security protocols and to evaluate users' security compliance. Such audits are part of a typical risk assessment process and, if violations occur, could include procedures for corrective actions and documentation of corrective actions. In some cases, if a vulnerability or breach is discovered, a disclosure may be required. Organizations should consider developing and implementing an exit protocol when an employee with a BYOD device departs the organization. This policy should be designed to ensure that the former employee no longer possesses or has access to organizational data on their personal device. The policy could also include provisions for the organization to retain data that are subject to discovery requirements (e.g., litigation hold, record retention policy).<sup>15</sup> The exit protocol could identify circumstances where forensic examination of the device may be required prior to the employee's exit.

Organizations should tailor their measures to available resources and the nature of corporate information that may be put at risk. Organizations should be careful about introducing a sophisticated state-of-the art security system that the organization cannot afford to maintain, or that the organization's personnel

---

15. See *supra* Comment 1.b. regarding limitations of these consents, and *infra* Comment 2.f. regarding obligations to protect personal information.



are not trained to use. This may prove to be a greater risk than not employing any security measures at all, because the false sense of security it will engender may encourage risky behavior by BYOD users.

Organizations that have only limited resources for BYOD security measures can still substantially enhance security through administrative safeguards. Administrative safeguards may include warning the people who are providing information to the organization that the information may be vulnerable on the employee-owned devices.<sup>16</sup> Organizations may also prohibit storing some types of data (e.g., client data) on employee-owned devices, or they may require a short retention period for some types of data. User training can also be an important part of an effective security plan.

Investment in data security measures should reflect the value of information to be secured. Organizations that do not have sensitive client data, or other protected data on BYOD devices, may find that the risk of disclosure of business information on such devices is low and thereby forgo investment of state-of-the-art data security measures.

*Comment 2.e. The BYOD program should consider employees' privacy interests.*

Developing an organization's BYOD security policies involves weighing the organization's need for security against employees' privacy interests. An organization may have to decide whether to incur the additional expense and burden of monitoring device usage. Monitoring would likely be needed to create differing levels of security depending on factors, such as

---

16. The warning may be analogous to the boilerplate footers that many law firms provide in their email signature lines.

an employee's access to sensitive information, or the sensitivity of specific information.

Technology tools that minimize the commingling of personal and organization data are becoming more common-place, effective, and less expensive. Available measures include encryption, virtual and hardware partitioning of portable devices, and making an organization's data portion of a device akin to a terminal, so that the organization data will continue to reside only on the organization's servers even though the employee can view and create the data through the personal device. Consultation with technology experts is essential for designing appropriate BYOD security measures.

*Comment 2.f. The BYOD program should consider employees' protected personal information.*

Organizations with obligations to protect personal information of users, employees, or customers, should understand those obligations and implement appropriate safeguards. Various laws mandate the protection of health, financial, and other private information, for example the Health Insurance Portability and Accountability Act (HIPAA), which requires covered entities to comply with the rule's requirements to protect and secure individually identifiable health information. Similar rules requiring the protection of categories of sensitive information from misuse or disclosure can be found in many states and worldwide.

Employees often store protected "personal" data on their personal devices. For example, employees may store their health information on a BYOD device in a health tracking app or other app that syncs with an account associated with the owner's medical provider. Employees may also store their social security number or banking information on their devices via a

personal profile or password manager app or a banking provider's app. Some organizations may choose to restrict the user's ability to download certain apps that may contain sensitive personal content, though doing so may intrude on the positive aspects of BYOD programs that an organization's employees enjoy.

Organizations should additionally factor into their BYOD protocols and policy the likelihood that personal information of third parties may become stored on the BYOD devices in the normal course of business. An employee may have personally identifiable information about customers, relatives, friends, social network "friends," and others. The presence of such information may present special compliance risks for the organization. For example, it would be inordinately difficult to prove that the non-employee consented to any organization access to or use of the non-employee's information.

Federal, state, and foreign data protection laws may protect the personal information of a device's owner. For example, under the Electronic Communications Privacy Act (ECPA), personal communications made via BYOD devices may not be accessed without valid authorization. Similarly, any disputes about ownership of the device or the data stored on it may complicate questions about who has standing to provide "authorization" to access the device and implicate protections afforded under the Computer Fraud and Abuse Act (CFAA). Similarly, evolving individual state laws may also create protections for personal information such as social media content stored on devices used by employees.

**Principle 3: Employee-owned devices that contain unique, relevant ESI should be considered sources for discovery.**

*Comment 3.a. Factors to determine whether ESI on an employee-owned device is discoverable include: whether the ESI is within the employer's possession, custody, or control; whether the ESI is unique; and whether the discovery of the ESI is proportional to the needs of the case.*

It should come as no surprise that ESI that falls within the scope of discovery is often stored on mobile devices.<sup>17</sup> Organizations cannot ignore their discovery obligations merely because a device containing unique, relevant ESI is also used for personal purposes.<sup>18</sup> That said, several courts have noted “significant concerns regarding the intrusiveness of the request and the privacy rights of the individuals to be affected.”<sup>19</sup> Whether

---

17. See FED. R. CIV. P. 26(b)(1), 26(b)(2)(B)–(C); see also *Ewald v. Royal Norwegian Embassy*, No. 11-CV-2116, 2013 WL 6094600, at \*10 (D. Minn. Nov. 20, 2013) (quoting the Magistrate Judge in the case: “It is not a surprise to any of the parties in this case that there were tablets, text messages, cell phones, and laptops involved. All of these devices were known prior to the initiation of litigation, and it is common knowledge that ESI is contained on all of these devices.”).

18. E.g., *Alter v. Rocky Point School Dist.*, No. 13-1100 (JS)(AKT), 2014 WL 4966119 (E.D.N.Y. Sept. 30, 2014) (“to the extent school district employees had documents related to this matter, that information should have been preserved on whatever devices contained the information (e.g., laptops, cell-phones, any personal digital devices capable of ESI storage.)”); *H.J. Heinz Co. v. Starr Surplus Lines Ins. Co.*, No. 2:15-cv-00631-AJS, 2015 WL 12792025 (W.D. Pa. Jul. 31, 2015).

19. *Kickapoo Tribe of Indians of Kickapoo Reservation in Kan. v. Nemaha Brown Watershed Joint Dist.* No. 7, 294 F.R.D. 610, 619 (D. Kan. 2013); see also *Bakhit v. Safety Marking, Inc.*, No. 3:13CV1049 (JCH), 2014 WL 2916490, at \*3 (quoting *Riley v. California*, 134 S. Ct. 2473, 2478–79 (2014) (regarding the

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.

BYOD devices and apps can pose unique discovery challenges as the technology behind them is evolving and discovery tools may not yet exist or be mature enough to handle this type of ESI efficiently and effectively. Counsel has the responsibility to conduct adequate BYOD discovery process due diligence. This due diligence will be the basis for a defensible process and counsel's representations to the court and opposing counsel regarding the discovery process. This is one area where counsel should consider engaging experts with the appropriate technical knowledge, competence, and experience.<sup>20</sup>

An organization's duty to preserve or produce such content will often depend on whether the employer is deemed to have possession, custody, or control of either the ESI or the device, or both, under Rule 34 of the Federal Rules of Civil Procedure (or its state equivalent), and whether the ESI is both relevant and unique (or if instead there is other ESI that is more readily available from other sources), and whether the requested discovery is proportional to the needs of the case. We discuss each of these issues in turn.

---

implication of the individual defendants' privacy interests and the qualitative impact of the volume and variety of data that can be stored on a modern-day cell phone)).

20. See *The Sedona Conference, Commentary on Defense of Process: Principles and Guidelines for Developing and Implementing a Sound E-Discovery Process*, Principle 2, THE SEDONA CONFERENCE (Sept. 2016 Public Comment Version), <https://thesedonaconference.org/publication/sedona-conference-commentary-defense-process-public-comment-version-september-2016>.

**Comment 3.b.** *An organization's BYOD program can impact whether the organization has possession, custody, or control over ESI on employee-owned devices, but the legal test may vary widely by jurisdiction.*

Three different legal standards have developed and been applied in the federal courts to determine whether discovery is in the possession, custody, or control of a responding party generally: the legal right standard, the legal right plus notification standard, and the practical ability standard. A far more detailed examination of these three standards can be found in The Sedona Conference *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* but generally speaking, the legal right standard evaluates a party's control based on their legal right to obtain the documents or ESI in question.<sup>21</sup> The legal right plus notification standard builds on the previous standard by further obligating responding parties who do not have a legal right to the ESI to notify the requesting party of the third parties who have possession, custody, or control of the information requested.<sup>22</sup> Finally, the practical ability standard evaluates control based on whether the responding party has the practical ability to obtain the documents and ESI, regardless of whether or not it has the legal right to do so.<sup>23</sup>

The *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control"* advocates for universal adoption of the legal right standard.<sup>24</sup> The Sedona Conference believes this is particularly

---

21. *The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control," supra note 1, at 482–518.*

22. *Id.*

23. *Id.*; see also *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007).

24. *The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control," supra note 1 at 537–45.*

true in the case of BYOD, where it is often unclear whether the organization has the “practical ability” to demand the device from its employees. Under any of these tests, organizations should not be compelled to terminate or threaten employees who refuse to turn over their devices for preservation or collection. It should be emphasized, however, that, at present, the legal right standard has not been unanimously adopted by all federal courts and therefore it is crucial to consider the standard applied in the applicable jurisdiction.

In the BYOD context, the concept of “control” can be particularly murky and ripe for disputes due to the overlap of personal and business information on the device, as well as the physical possession and ownership of the device by the employee, who may be an uninterested third party to the litigation. There is limited case law on possession, custody, or control in the BYOD context although a few courts have held in legal right jurisdictions that organizations do not have possession, custody, or control over BYOD devices where there was no contention that the employer had any legal right to obtain employees text messages on demand.<sup>25</sup>

A “consent” or “acknowledgement” or other agreement that the employee signs and that recognizes that the organization owns or controls the ESI would likewise give the organization possession, custody, or control of the ESI, and the resulting obligation to consider the device when meeting its discovery obligation. Thus, organizations should carefully consider how a

---

25. *Id.*; *Matthew Enterprise, Inc. v. Chrysler Grp. LLC*, No. 13-cv-04236-BLF, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015); *Ewald v. Royal Norwegian Embassy*, No. 11-CV-2116, 2013 WL 6094600, at \*10 (D. Minn. Nov. 20, 2013) (refusing to order production of text messages from content from personal mobile devices because plaintiff did not make any showing that she is entitled to personal devices and she “has had ample opportunity to conduct that discovery”).

policy that asserts ownership may increase the likelihood that a court will find that an organization does indeed have legal control over such information, thereby increasing discovery-related obligations.<sup>26</sup>

Courts and parties should also consider the practical implications of commanding employees to turn over devices that the employees bought and paid for. Even if an organization has possession, custody, or control over a device, the organization should not be required to use a threat of termination to force the employee to turn over the device. Such a rule would impose too heavily on the relationship between employees and their employer. On the other hand, employers should advise opposing counsel if they are practically unable to collect from employee-owned devices ESI that is within the scope of discovery (i.e., the ESI is relevant, unique, proportional, and within the possession, custody, or control of the employer).

*Comment 3.c. Even if ESI on a mobile device is relevant, the ESI is not within the scope of discovery if it can be collected from a more accessible source.*

Under many BYOD programs, a significant amount of content on employee-owned devices is duplicative of ESI stored by the organization in other places. Further, the duplicate ESI stored by the organization is typically more accessible than the content stored on the device. In determining whether to preserve or produce ESI content stored on BYOD devices, an organization should evaluate whether the BYOD device is likely to

---

26. See H.J. Heinz, Co. v. Starr Surplus Lines, Ins. Co., No. 2:15-cv-00631-AJS, 2015 WL 12791338, at \*4 (W.D. Pa. July 28, 2015) (finding Heinz had possession, custody, and control of BYOD device based on Heinz BYOD policy that indicated Heinz owns the property on the devices and that it can delete content from devices in its sole discretion).



contain relevant, unique content—for example, through interviews or sampling. Organizations may also rely on their BYOD program and their Information Governance program to reach reasonable conclusions about whether relevant ESI on employee-owned devices is likely to be unique.

As explained in Comment 8.a. of *The Sedona Principles*, organizations should first look to more accessible sources of relevant ESI before going to less accessible sources:

The primary sources of information for the responding party should be those that are routinely accessed in the ordinary course through ordinary means. Once those primary sources are exhausted, the responding party arrives at a “phase gate” or “decision gate,” where it must consider whether additional, unique, and discoverable ESI exists within less readily accessible sources and, if so, whether the preservation and potential production of that information through extraordinary means is consistent with the proportionality requirement of Rule 26(b)(1).<sup>27</sup>

Applying this concept to mobile devices, organizations may look to ESI from more accessible sources (e.g., company servers) before collecting ESI from mobile devices.

At least one court has found that a public official’s private phone contained public records subject to an open records request, where it was shown that the phone contained government business communications, the township was reimbursing the employee for the use of the phone, and the employee could

---

27. *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, Cmt. 8.a. (2018).

not “privatize his public correspondence.”<sup>28</sup> A trend appears to be growing among state legislators to treat as public records any messages on officials’ or government employees’ personal devices concerning government business.<sup>29</sup> Even so, public employees’ communications on personal devices may be subject to Constitutional protections.<sup>30</sup>

***Comment 3.d. The concept of proportionality also limits the scope of discovery of ESI on employee-owned devices.***

BYOD greatly expands the opportunities for an organization’s users to create and retain ESI in ways that may be well suited for the individual user’s needs, but that render preservation and collection for discovery laborious, disruptive, and expensive. As discussed in Comment 3.c., discoverable ESI found on BYOD devices may be duplicative of ESI stored in more accessible sources and, as noted under Principle 1, some of the unique or duplicative content may contain the user’s personal information and, potentially, the personal information of third parties. The confluence of these issues can be found in an organization’s everyday business activities.

*Example i.* The chief executive officer (CEO) of ABC Corporation receives an email from her assistant with an attached draft presentation. Using her smartphone, the

---

28. *Paint Township v. Clark*, 109 A.3d 796, 809 (Pa. Commw. Ct. 2015); *but see City of San Jose v. Superior Court*, 169 Cal. Rptr. 3d 840, 856 (6th Dist. 2014), *review granted and opinion superseded*, *City of San Jose v. S.C. (Smith)*, 326 P.3d 976 (2014) (holding that the California Public Records Act did not impose an affirmative duty to search devices and accounts of its employees and officials for messages relating to City business).

29. *See, e.g.*, TEX. GOV’T CODE § 552.002(a-1) and (a-2), TEX. LOC. GOV’T CODE § 201.003(8).

30. *See City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010).

CEO composes an email forwarding the presentation to the chief financial officer (CFO). The CFO receives the email on his smartphone as his flight is about to depart and downloads and saves the presentation file. During the flight, he edits the presentation, saves the revised version on his smartphone, and composes an email explaining his revisions and attaching the edited presentation file. On landing, he sends the email to the CEO, who then opens the email and attachment on her tablet for viewing on a larger screen. She saves the file to her tablet, makes further edits to the presentation, and then emails the edited file back to the CFO. The two smartphones and tablet are each of different manufacturers and use different operating systems, and each is synchronized to a separate personal cloud account for file storage and backup that is owned and controlled by the individual. The CEO is careful to use a personal email account for family correspondence, but her personal email synchronizes to both her smartphone and tablet and her cloud storage accounts. Her personal emails include the college transcript of her adult daughter, an evaluation from her minor son's therapist, and correspondence with an attorney regarding her role as the legal guardian and trustee of her elderly mother's trust. Applying the proportionality factors, the burden of collecting the various drafts from the various sources likely outweighs the benefit, unless the presentation is so central to the case that drafts of the presentation are extremely important in resolving the issues in the case.

In the above example, an exchange of just three emails between executives created numerous copies of potentially non-identical files stored on multiple devices and accounts and commingled with communications implicating the privacy interests

of third parties who have not previously consented, and may be unwilling or unable to consent, to disclosure of their sensitive personal information to ABC Corporation's counsel. In the first decade of discovery, the paradigmatic example of disproportionate discovery burdens was disaster-recovery-tape backups. ESI on backup tapes was equally inaccessible and required great effort and expense to restore, whether for the organization's ordinary business needs or for discovery. For example, locating a single email message on a backup tape was equally burdensome to accomplish, whether the reason for locating that email was to satisfy business needs or satisfy discovery obligations in litigation. The problem with accessing ESI on mobile devices is often different, in that individual employees can access the ESI for their own business uses (e.g., the CEO in the above example can easily access the draft presentation), but the organization cannot easily access the same information from all the various sources for discovery.<sup>31</sup> Thus, device content can be accessible for business needs in this context, and still not be proportional for purposes of discovery. This distinction may be critical to a proportionality analysis for discovery of ESI on personally-owned devices.<sup>32</sup>

---

31. As another example, some BYOD ESI is not readily accessible to the organization in the course of regular business, such as deleted text messages that may reside on the device but cannot be accessed by a lay user, but only through forensic acquisition.

32. "Free" solutions may fail to properly preserve text messages on cell phones. For example, using cell phone operating system software to sync cell phones with a computer hard drive may not copy all unique ESI from the cell phone, and the process may not store the ESI in a sound manner that can be used for discovery purposes. Further, syncing features may be inadequate, or may be changed by the software provider. Additionally, such processes are not always scalable or user-friendly. "Free" does not necessarily equate with "proportional" or "reasonable."

The proportionality analysis should look beyond the discovery costs in any single case, and consider the impact that discovery will have on the organization's BYOD program. As stated in Comment 3.d. of The Sedona Conference *Commentary on Proportionality in Electronic Discovery*, an effective information governance program should help organizations reduce discovery costs and risks, and, conversely, organizations should not benefit from a poor information governance program that results in large quantities of unique, relevant ESI residing in locations that are difficult to access for discovery:

Information retention policies may also affect the proportionality analysis. Where a party's information retention policies serve reasonable organizational or commercial purposes, burden, expense, or delay attributable to such policies should not be held against the party claiming burden. Conversely, where information retention policies do not serve such purposes, associated arguments of burden, expense, or delay should be discounted.<sup>33</sup>

Applying proportionality in this manner will incentivize organizations to align their management of BYOD usage with their discovery obligations. Moreover, it will incentivize organizations to address discovery costs when considering adoption of BYOD and the design and operation of their IT systems relating to BYOD.

Implicit in this basic policy argument is an assumption that reliable, practicable methods for managing BYOD presently exist and may be implemented at a reasonable cost.

---

33. The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141, Cmt. 3.d. (2017).

***Comment 3.e. Organizations should consider their employees' privacy interests before collecting ESI from employee-owned devices.***

As both a legal and practical matter, employees' expectations of privacy are generally greater for devices that they own than for devices that their employer provides. Organizations may have to balance varying privacy obligations with discovery obligations in the different jurisdictions in which it does business, with sometimes conflicting legal standards.<sup>34</sup> Often, the determination of which country's data privacy laws apply to the data stored on a BYOD device must be made on a case-by-case basis. Organizations can work with outside privacy counsel and local counsel to analyze factors such as whether data privacy rights are based on the citizenship of the employee or the physical location of the device. *See* Appendix B, *infra*, for a discussion regarding country specific considerations.

If a BYOD device contains unique, relevant data, but is subject to data protection laws, several opportunities to balance data protection with U.S. discovery obligations exist, including: (1) limiting the scope of discovery to only relevant and necessary protected data; (2) establishing a stipulation or protective order regarding protected data; (3) planning for phased discovery and collecting data from easily accessible sources first; and (4) potentially planning an in-country collection and review in order to minimize the transfer of protected data outside of the country.

Organizations also face an inconsistent and complex landscape of court rulings that increase their risk of potential liability to employees when the organization accesses BYOD devices to collect unique, relevant content. For example, in the context of

---

34. *See* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 17 SEDONA CONF. J. 397 (2016).

employer-provided devices, courts have recognized public sector employees' privacy expectations in personal text messages,<sup>35</sup> and private sector employees' privacy expectations in attorney-client emails sent via employee-owned webmail accounts.<sup>36</sup> In contrast, other courts have found employees' expectations of privacy waived when using the computer systems owned by their employer.<sup>37</sup>

Many organizations attempt to require broad privacy waivers from users as a condition of the organization's consent to BYOD usage. This approach may be inconsistent with local law in some jurisdictions. Even if such broad user privacy waivers are enforceable, commingled BYOD ESI may include information implicating the privacy rights of third parties not bound by the waiver. The example of the CEO using her tablet and smartphone in Comment 3.d., *supra*, illustrates how the personal communications of a user may intersect with multiple, distinct legal and ethical relationships, raising privacy concerns for each.

---

35. *Quon*, 560 U.S. at 760 (acknowledging city employee's "reasonable expectation of privacy" in text message communications sent via a cell phone issued by the municipality in the context of a Fourth Amendment search and seizure claim; however, the Court did not resolve the parties' disagreement over *Quon's* privacy expectations).

36. *See, e.g., Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650, 663 (N.J. 2010).

37. *See, e.g., Order, In re Grand Jury Subpoenas Dated May 14, 2014 & January 13, 2015*, No. 1:15-mc-02227-JBW (E.D.N.Y. Dec. 3, 2015) (unsealed) (Weinstein, S.J.) ("The employee was warned by the company that the documents created during employment were company property. . . . As company documents they would not be subject to a privilege between the employee and an attorney acting for the employee and also for the company."); *Holmes v. Petrovich Dev. Co., L.L.C.*, 191 Cal. App. 4th 1047, 1071 (Cal. Ct. App. 2011) (plaintiff had no expectation of privacy in personal email sent on a work computer when plaintiff was notified in writing that her employer could inspect her computer at any time at its discretion).

**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.

*Comment 4. Organizations should proactively manage employee-owned devices.*

Proactive 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.

Eliminating the BYOD device as a relevant storage location for discovery, to the extent reasonably feasible, would require a combination of technology, policy, and user training solutions. Avoiding retention of unique emails sent or received on the user's organization email account is a common practice whereby there is complete synchronizing of transmitted and deleted email between the device and the network, and the retention period is the same on both the corporate email server and on the device. At least in theory, implementing these account settings—i.e., prohibiting use of personal email and cloud accounts for organization ESI, and prohibiting users from saving organization files locally on the BYOD device—may substantially reduce the relevance of the BYOD device for discovery of business information. However, in practice, an organization may need to rely primarily on technology safeguards to implement and enforce these restrictions by “locking down” the device settings and using MDM security software applications, as discussed in Comment 2.d., *supra*. User training complements



such technology solutions. The goal of user training is not simply to communicate the organization's policy, but also to persuade users to support the policy. Sophisticated users will find opportunities to "work around" BYOD restrictions and frustrate the organization's BYOD management unless they accept these restrictions as valid and credible.

Again, policy, technology, and training offer viable solutions to substantially reduce the problem of commingled personal data and organization ESI on BYOD devices. For example, several software developers market partitioning applications<sup>38</sup> to segregate personal data on BYOD devices. Many of the same solutions that an organization may rely upon to aggregate organization ESI on a corporate network or other centralized storage location may also be used to exclude personal data—such as using separate email accounts for personal and business communications, or excluding business files from local storage on the BYOD device so that, in theory, the only unique files saved locally to the device are personal user content. In the context of managing personal data, training is especially important to inform users of how to use the BYOD device in a manner that does not compromise their personal privacy. Such training may mitigate the need for broad organization-imposed privacy waivers.

Reasonable measures to regulate BYOD usage should be considered by an organization. What constitutes reasonable may vary among organizations depending upon the size and complexity of the organization or the frequency with which the organization is a discovery respondent. Within a particular organization, different approaches may be appropriate for different users based upon their organization roles and their degree of sophistication as IT consumers. BYOD may be inappropriate

---

38. For example, Google's "Android for Work" and AT&T's "Toggle" provide partitioning functionality.

for some users because it is prohibited by law or regulations. For example, some employees may be prohibited from using personal devices while performing certain functions to protect public safety (e.g., railroad locomotive engineers) or to prevent criminal or fraudulent schemes (e.g., traders on the securities markets). Comment 3.e., *supra*, discusses the extent to which local law protecting user privacy rights may impact an organization's ability to implement effective BYOD management.

An important part of proactive BYOD management is developing regularly recurring processes for documenting and validating the organization's methods. As a discovery respondent, the organization may be required to defend its reliance on these methods to define the scope of its preservation and collection. Well-documented processes may be essential for the organization to actually enjoy the benefits of its investment in careful BYOD management.

**Principle 5: Employee-owned devices that do not contain unique, relevant ESI need not be considered sources for discovery.**

*Comment 5.a. Responding parties should make reasonable efforts to determine whether mobile devices contain unique, relevant ESI.*

As explained in Principle 3, *supra*, 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 existence of a “reasonable basis” can be shown many ways, including the following:

- An interview of key custodians determines none of the custodians used their mobile devices to communicate about issues relevant to a case, and, where this may be in dispute, none of the ESI created by the communications was unique to the devices.
- Critical evidence in a case is formulae in a spreadsheet stored on a computer and, therefore, have absolutely nothing to do with any data that could be uniquely stored on a cell phone.
- The only communications about the issues or events involved in a case are through an email application that fully synchronizes with the organization’s servers; the email can be collected from the servers and not from the BYOD devices.
- The organization has in place a BYOD policy or technology controls reasonably designed, with due care and in good faith, to prevent the storage of unique, relevant ESI on BYOD devices. Where this is the case, the organization should preserve and collect the most accessible copy of such ESI from non-BYOD sources, such as active email files or a designated legal hold archive of such email files (if an organization has such a system in place).

As with other potential sources of ESI, the concept of proportionality applies to dictate what steps an organization must take to determine whether the devices contain unique, relevant ESI.<sup>39</sup>

---

39. See *supra* Comment 3.d.

**Comment 5.b.** *BYOD programs can give organizations a reasonable basis to believe that employee-owned devices do not contain unique, relevant ESI.*

Where an organization relies on its BYOD policy to avoid preservation or collection of ESI from BYOD devices, cooperative discussion and non-privileged information exchange with opposing counsel regarding what ESI is (and is not) stored on the BYOD devices, and what other sources of data are reasonably available, may reduce or eliminate formal discovery or motion practice.

*Example i.* An organization has a BYOD device policy or protocol that ensures all email sent from and received on the BYOD device is also stored on the email server, all deletions made in Outlook synchronize to the device, and the retention period is the same in Outlook and the device. After reasonable inquiry, the organization can reasonably conclude that unique, business-related ESI is not stored on the device. Absent any other showing, the organization should be relieved of the burden of preserving and collecting ESI from the device.

As many courts have opined, Rule 26(b)(1) and (g) impose a reasonableness standard for discovery, and do not require perfection.<sup>40</sup> Extending this to the realm of preservation of BYOD

---

40. *Reinsdorf v. Skechers U.S.A., Inc.*, 296 F.R.D. 604, 615 (C.D. Cal. 2013) (“[W]hile parties must impose a reasonable construction on discovery requests and conduct a reasonable search when responding to the requests, the Federal Rules do not demand perfection. *See, e.g., Cache La Poudre Feeds, LLC v. Land O’Lakes, Inc.*, 244 F.R.D. 614, 618–19 (D. Colo. 2007) (parties have ‘an obligation to construe . . . discovery requests in a reasonable manner’); *Metropolitan Opera Ass’n, Inc. v. Local 100, Hotel Employees and Restaurant Employees Int’l Union*, 212 F.R.D. 178, 223 (S.D.N.Y. 2003) (Rule 26(g) requires a ‘reasonable inquiry under the circumstances’); *Moore v. Publicis Groupe*, 287 F.R.D. 182, 188 (S.D.N.Y. 2012) (“[T]he Federal Rules of Civil Procedure do

devices, it may always be a possibility that due to a technology bug or loophole, or to a user's activities, instances of unique, relevant ESI on a BYOD device may go undetected—despite an organization's reasonable efforts. The 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.

*Example ii.* The organization in the example above advises that users of BYOD devices can download attachments from email messages to their devices and those downloads are not synchronized to the organization's systems. If, after reasonable inquiry, the organization determines that such downloads are infrequent and that the attachments are not significant to the issues in the case (e.g., custodian interviews demonstrate that no custodians regularly used the download feature to organize relevant information into meaningful compilations), the organization is not required to preserve or collect ESI from such devices.

*Example iii.* An organization has in place a BYOD program reasonably designed, with due care and in good faith, to prevent the storage of unique, business-related ESI on BYOD devices. If the organization takes reasonable steps to confirm that its employees comply with its program, that organization need not preserve or collect ESI from BYOD devices.

---

not require perfection.'). *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of America Securities, LLC*, 685 F. Supp. 2d 456, 461 (S.D.N.Y. 2010) . . . 'The reasonableness of the inquiry is measured by an objective standard. . . .' *National Ass'n of Radiation Survivors v. Turnage*, 115 F.R.D. 543, 555 (N.D. Cal. 1987).").

*Example iv.* An organization makes reasonable inquiry during custodian interviews to confirm that the custodians comply with the BYOD program, which therefore provides the organization with a reasonable belief that unique, relevant ESI does not exist on BYOD devices. At a later deposition, however, a key custodian discloses that she used her BYOD device to store relevant ESI, in contravention of the organization's BYOD policy. If that ESI is proportional to the needs of the case, the organization should collect ESI from the device and produce non-privileged relevant information. The organization should also take reasonable steps to determine whether other employees with relevant ESI also violated the BYOD policy. If the organization fails to produce non-privileged relevant information from the device of the custodian who originally disclosed violation of the BYOD policy, a challenging party could then move to compel discovery of this device and the court may reasonably grant such a motion where a compelling need is shown, though it should not make *post hoc* judgments about preservation of the device based on information not previously known to the organization. Additionally, the court could allow limited discovery on the issue of whether other key custodians similarly used their devices in contravention of the policy, whether the information stored on their BYOD devices is material and unique, and whether the burden of obtaining the ESI is proportional to the needs of the case.

***Comment 5.c. Parties and courts should take reasonable steps to protect business information in cases where the organization is not a party.***

The above comments address the situation where the organization is a party and some of the organization's ESI is relevant

in the litigation, but personal information is not. Sometimes, however, the roles are reversed and the employee is a litigant, but the organization is not. In those cases, the organization's data is not relevant, but the employee's information is. Where a BYOD device is a target of discovery solely for the personal information on the device, a court should allow an organization to remove from the device, or otherwise exclude from discovery, any ESI it can demonstrate is non-relevant, business information. In such situations, the organization would benefit from clauses in its BYOD policy that give it the right to be notified and to remove or otherwise protect any such business information prior to collection. The objective is to ensure that the organization's non-relevant data is not subject to discovery. In the absence of a third-party request or other similar obligation to preserve such ESI, an organization does not have a duty to preserve or collect personal ESI stored on BYOD devices.

*Example i.* In a domestic dispute involving an employee, discovery is taken from the employee's BYOD device. In the absence of a compelling need or showing otherwise, the parties should notify the organization and work with it to ensure that document collection from the device excludes organization information, or allow the organization to remove non-relevant business information from the device (subject to other preservation requirements that may be in place).

### **APPENDIX A: DEPARTMENTAL COLLABORATION GUIDE**

Collaboration among departments or people of various disciplines should be undertaken when organizations develop a BYOD policy and BYOD practices (“BYOD program”). Collaboration is not a legal requirement, but rather an aspirational best practice. When developing a BYOD program, consider consulting with these departments: Finance, Human Resources (HR), Information Governance (IG), Information Technology (IT), Legal/Compliance, and Security. Smaller organizations may not have all of these departments, or they may have combined or outsourced some functions. Furthermore, an organization’s structure and purpose may necessitate consulting with people in other specialty areas not included here. Below is a chart outlining the potential benefits of consulting with departments in each specialty area and questions to address to each, but the chart’s primary purpose is to help guide organizations identify which specialty areas to include when developing a BYOD program.



*Specialty Areas to Include When Developing a BYOD Program*

	Benefits of Consulting	Questions to Ask
<b>Finance</b>	<ul style="list-style-type: none"> <li>• Understand financial issues for BYOD program, including indirect or hidden costs</li> <li>• Coordinate potential employee reimbursement for BYOD</li> </ul>	<ul style="list-style-type: none"> <li>• How will BYOD devices be financed (purchase, lease, or rental)?</li> <li>• Are there any agreements that govern the provision of BYOD devices or data/phone services?</li> <li>• How will costs increase or decrease if there is a change to the BYOD program?</li> </ul>
<b>Human Resources (HR)</b>	<ul style="list-style-type: none"> <li>• Understand employment issues</li> <li>• Articulate HR objectives for BYOD program</li> <li>• Coordinate with existing HR policies and procedures</li> <li>• Determine roles for HR in implementation and enforcement</li> <li>• Identify state and country laws that may impact BYOD program</li> </ul>	<ul style="list-style-type: none"> <li>• How does HR currently handle BYOD devices?</li> <li>• How does HR handle use of technology and communication in its various policies?</li> <li>• How does HR handle technology training?</li> <li>• Will BYOD program include employees and contractors or organization agents?</li> <li>• How will the BYOD program be rolled out to employees?</li> <li>• Should all employees be eligible for the BYOD program?</li> <li>• How will HR exit-interview processes incorporate questions about BYOD?</li> </ul>

	<b>Benefits of Consulting</b>	<b>Questions to Ask</b>
<b>Information Governance (IG)</b>	<ul style="list-style-type: none"><li>• Determine how BYOD will affect management and governance of data</li></ul>	<ul style="list-style-type: none"><li>• Do any information management policies or processes need to be revised?</li><li>• How will BYOD affect data governance and record retention?</li></ul>
<b>Information Technology (IT)</b>	<ul style="list-style-type: none"><li>• Understand IT objectives and requirements for BYOD program</li><li>• Coordinate with IT to enable elements of the BYOD program</li><li>• Determine roles for IT in implementation and enforcement</li><li>• Create proprietary apps for use on BYOD devices</li></ul>	<ul style="list-style-type: none"><li>• How does IT currently handle BYOD devices?</li><li>• How does IT handle remote access?</li><li>• What types of devices will be included?</li><li>• What geography is included?</li><li>• How does IT handle technology training?</li><li>• How will IT handle BYOD devices when an employee leaves the organization?</li></ul>

	<b>Benefits of Consulting</b>	<b>Questions to Ask</b>
<b>Legal/ Compliance</b>	<ul style="list-style-type: none"><li>• Identify state and country laws that may impact BYOD program</li><li>• Understand impact on preservation and litigation, and other disclosure mandates</li><li>• Understand impact on third-party requests for information</li><li>• Consider employment issues that arise from BYOD</li><li>• Identify and assess relevant record retention requirements</li></ul>	<ul style="list-style-type: none"><li>• How will risk increase and decrease if there is a change to the BYOD program?</li><li>• How will BYOD affect identification, preservation, collection, and all other discovery steps?</li><li>• How will compliance with the BYOD program be reviewed?</li><li>• How will Legal/Compliance exit-interview processes incorporate questions about BYOD, particularly as related to any information that may be under preservation?</li></ul>

	Benefits of Consulting	Questions to Ask
Security	<ul style="list-style-type: none"><li>• Understand security risks</li><li>• Establish security risk tolerances</li><li>• Implement security requirements</li><li>• Identify processes for protecting confidential and private information</li></ul>	<ul style="list-style-type: none"><li>• How will BYOD devices be secured?</li><li>• How will BYOD devices access organization systems?</li><li>• How will BYOD devices be locked out of or removed from accessing organization systems?</li></ul>

Many of the items suggested for consideration impact multiple specialty areas within an organization that may, and hopefully will, bring different perspectives to the table for discussion. For example, when an organization is determining the scope of a BYOD program, and which employees or contractors should be eligible for BYOD, Finance will be interested because of the cost and ability to charge back to a business unit, while HR may be interested in the issues with rolling out different policies for different roles or departments. Below is a chart that suggests which areas may need to be consulted regarding common topics confronted by an organization implementing a BYOD program.

*Topics for Multiple Specialty Areas  
within an Organization to Consider*

	Finance	HR	IG	IT	Legal/ Compliance	Security
Eligible Employees	X	X	X	X	X	X
Eligible Data			X	X	X	X
Eligible Devices	X			X	X	X
Security Requirements	X			X	X	X
Eligible Apps	X			X	X	X
Training		X		X	X	X
Compliance Monitoring	X	X		X	X	X
Notice to and Consent from Third Parties			X		X	
Device Tracking	X			X	X	X
Budget	X	X	X	X	X	X
Types of ESI on BYOD Devices		X	X	X	X	X

Consultation with its various departments can help the organization consider implications and risks identified by each area and in theory will result in a more robust and well-planned BYOD program. It is important to have a clear project plan with timelines and a project manager that can shepherd the various

organizational departments through the creation, implementation, and initial compliance audit for the BYOD program.

## APPENDIX B: BYOD IN THE INTERNATIONAL CONTEXT

There are unique legal challenges to the successful implementation of a BYOD program, particularly in the international context and due mainly to data privacy and data protection laws. In the European Union and many other jurisdictions, data privacy is considered a human right. Therefore, when developing a BYOD program, organizations should consider and understand the various data protection laws and regulations in the countries that they operate, especially those laws that apply to BYOD and the workplace, including concepts such as employee monitoring.

Employers will also face unique legal challenges due to international data privacy and data protection regulations that may impact discovery. The Sedona Conference *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)* (hereinafter “*International Litigation Principles*”) provides guidance for navigating such global discovery challenges.<sup>41</sup> The *International Litigation Principles* contains discovery obligations for the employer, which include striving to show due respect to the data protection laws of any foreign sovereign, operating under a standard of good faith and reasonableness, limiting scope of preservation and discovery of protected data, using a stipulation or court order to protect protected data, demonstrating that appropriate data protection safeguards are in place, and retaining protected data only as long as necessary to satisfy business or legal needs.<sup>42</sup>

---

41. The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, THE SEDONA CONFERENCE (January 2017), <https://thesedonaconference.org/publication/International%20Principles%20on%20Discovery%2C%20Disclosure%20%2526%20Data%20Protection>.

42. *Id.*

Organizations should contact both local counsel and local data protection authorities when considering instituting global BYOD programs. Individual countries may have specific and nuanced definitions of personal data and regulatory bodies may have commented specifically on BYOD best practices. For example, the French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), released BYOD guidelines in early 2015 that detail best practices for BYOD in France.<sup>43</sup> In 2013, the German Federal Office for Information Security (BSI) published guidance on BYOD issues.<sup>44</sup> In 2013, the Information and Privacy Commissioner of Ontario, Canada, partnered with a telecom organization to issue a whitepaper on BYOD policies and development strategies.<sup>45</sup> Also in 2013, the United Kingdom's Information Commissioner's Office (ICO) issued guidance regarding the UK Data Protection Act of 1998 and its application to BYOD policies.<sup>46</sup> These are a few examples of a broad array of guidance on BYOD that has been issued from various regulatory agencies across the globe.

---

43. CNIL, *BYOD: quelles sont les bonnes pratiques?* (Feb. 19, 2015), <https://www.cnil.fr/fr/byod-queelles-sont-les-bonnes-pratiques> (unofficial translation available at <http://www.hl dataprotection.com/2015/03/articles/international-eu-privacy/cnil-releases-byod-guidelines>).

44. Hunton & Williams LLP, *German Federal Office for Information Security Issues Guidance on Consumerization and BYOD*, PRIVACY & INFO. SECURITY L. BLOG (Feb. 7, 2013), <https://www.huntonprivacyblog.com/2013/02/07/german-federal-office-for-information-security-issues-guidance-on-consumerization-and-byod>.

45. Ann Cavoukain, OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, & TELUS, *BYOD (BRING YOUR OWN DEVICE): IS YOUR ORGANIZATION READY?*, PRIVACY BY DESIGN, at 1 (December 2013), available at <https://www.ipc.on.ca/wp-content/uploads/2013/12/pbd-byod.pdf>.

46. UNITED KINGDOM'S INFORMATION COMMISSIONER'S OFFICE (ICO), *BRING YOUR OWN DEVICE (BYOD)*, available at [https://ico.org.uk/media/for-organisations/documents/1563/ico\\_bring\\_your\\_own\\_device\\_byod\\_guidance.pdf](https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf) (last visited November 25, 2017).