wgs

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 & Production (WG1)

May 2018
Final/Prepublication Version
Cite as "19 Sedona Conf. J. 495 (forthcoming 2018)"



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

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 (forthcoming 2018), *available at* https://thesedonaconference.org/publication/Commentary%20on%20BYOD.

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. Haskel, 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 though 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

Also available as part of the eCourse
Hooked on CLE: January 2022

First appeared as part of the conference materials for the
2021 E-Discovery Essentials session
"Discoverability of Mobile Devices, New Technology and Social Media Platforms"