ACCESSDATA

WHITE PAPER

Do benefits of personal devices at work outweigh drawbacks?

Summary of findings from the June 2018 AccessData and Corporate Counsel Business Journal Research Study

Introduction

Not all that long ago, using a personal electronic device at work might have been cause for a reprimand. Today, with the widespread acceptance of employee use of the iPhone, iPad, smartwatch and other personal devices for work—"Bring Your Own Device," or "BYOD"—one could imagine a reprimand for *not* bringing a personal device to the office.

The embrace of BYOD programs by employers and employees, which is transforming workplaces everywhere, brings with it a complex mix of benefits, costs and risks. The benefits cited most frequently include lower IT costs for employers, increased productivity, and higher morale for employees who say using their own devices for work adds much-needed balance to their personal and professional lives.

But as the line between work life and personal life blurs, so does the line between employee and employer ownership of the data associated with these increasingly powerful devices. And therein lie many of the risks associated with BYOD.

The issues related to these rapid changes—the first iPhone was released just 11 years ago—are especially stark when it comes to the preservation and collection of electronically stored information (ESI) on personal devices used for business purposes. According to Tod Ewasko, director of product management and development for AccessData, the challenges at the intersection of BYOD and e-discovery are significant.

> "BYOD seems like a cost savings initially, but on the other side of the coin, it becomes unfeasible for IT to manage."
>
> Tod Ewasko
> director of product management and development
> for AccessData

"BYOD seems like a cost savings initially, but on the other side of the coin, it becomes unfeasible for IT to manage," Ewasko says. "When it comes to forensic and e-discovery collection of data, getting it off those devices can be a nightmare."

According to a recent survey conducted by AccessData and *Corporate Counsel Business Journal* (CCBJ), that nightmare is growing scarier. The respondents, senior corporate counsel at major companies across an array of industries, already are concerned over the deluge of emails and texts with which they have to deal. Now, however, they are confronting the need to access data across a dizzying array of applications and platforms that, on any given workday, might include Skype, Slack, Box, Dropbox, Facebook, Twitter, What'sApp, Instagram, and wearables such as the Apple Watch and Fitbit. Fully 85 percent of employers, according to the survey, find the burgeoning data sprawled across disparate sources troubling.

This white paper looks at the evolving BYOD landscape in light of e-discovery and other disclosure demands. The focus is on three areas explored in the survey:

- corporate attitudes and concerns regarding BYOD programs;
- e-discovery challenges arising from the use of personal devices for work; and
- managing the risks of corporate personal device programs.

The full survey results, available here, were also the subject of a one-hour webinar recently hosted by AccessData and CCBJ. The program looks at the risks associated with allowing individuals to access and share company information through non-monitored personal devices and highlights best practices for establishing and administering BYOD programs in light of potential pitfalls related to e-discovery demands.

"The risks at the intersection of BYOD and e-discovery are very real," Ewasko says.

The State of BYOD Today: Finding Solid Footing in the Corporate Workplace

There's no doubt that BYOD/personal device programs are proliferating rapidly. The AccessData/CCBJ survey shows that almost 70 percent of organizations allow employee use of personal devices for work-related purposes, and that number is climbing fast. Recognizing the benefits of allowing employees to use personal devices for work, and searching for cost savings wherever they can find them, companies are flocking to BYOD programs.

Unfortunately, many of these initiatives are being launched without adequate consideration of the risks, many of which arise from e-discovery in the course of litigation and the data identification, preservation and collection requirements associated with government and internal investigations. Indeed, many company BYOD programs are flying blind.

Among the most interesting findings in the survey, perhaps none is more telling than this: while most

employers now permit—or encourage—the use of personal devices for work-related matters, 40 percent of companies do not have a BYOD or personal device policy and/or a formal procedure for collecting employee devices or data. Another 22 percent have only informal collection procedures.

Given that more than 25 percent of survey respondents say that their organization faced at least one matter or investigation in the last 12 months involving collection of data from more than one personal device, that's a troubling situation. Clearly, adoption of BYOD programs is outstripping the creation of strong policies and a procedural infrastructure for dealing with the demands of e-discovery, including widespread cloud-based storage of data.

> Eighty-five percent say discoverable data on personal devices troubles them, and almost one quarter say it is a critical concern.

"It's amazing to think about how many apps are streaming data up to Amazon Web Services or some other cloud repository," says Ewasko. "Just within the last few years, it has grown exponentially."

As data sources and storage locations have multiplied, so have employers' concerns. Eighty-five percent say discoverable data on personal devices troubles them, and almost one quarter say it is a critical concern. In addition, more than half cite work-related data associated with wearables and smart devices other than phones, tablets and computers as a growing concern. A mere 15 percent say data preservation and collection are no concern at all.

Nevertheless, the march toward BYOD adoption continues. Depending on the survey, it won't be long before more than 80 percent of organizations in the U.S. are allowing at least some of their workers to use their personal devices for company business. For many IT teams, it is impossible to run fast enough to keep up.

Challenges Abound in Widespread Use of Personal Devices for Work Purposes

Organizations face myriad issues in allowing employees to use their personal devices for work. These include, among others:

- The variety of data types implicated;
- The location(s) where that data resides;
- The company's lack of ownership and/or control of employee devices;
- The difficulty of protecting and/or collecting the data.

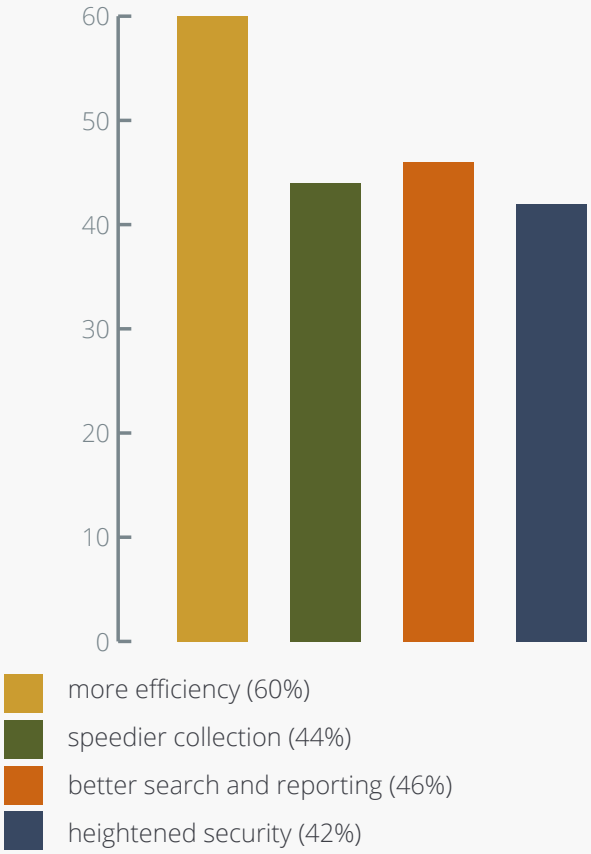
Moreover, according to the AccessData/CCBJ survey, many organizations face these challenges with the equivalent of one hand tied behind their backs.

As noted above, despite the growing use of personal devices for work, mounting concern about discoverable data on those devices, and direct experience with investigations and matters requiring data collection, many companies have been lax about adopting formal policies and procedures concerning discoverable data on personal devices and the collection of that data.

Location and ownership of the data are clearly problems. Much ESI is making its way to one or more of the well-known cloud services, and a large portion of data is now stored in more than one place—the cloud, company servers, locally on employee personal devices. Companies are hamstrung as they do not own the devices and cannot simply seize them from employees as they could company-owned devices. Moreover, the data on those devices is a perplexing mix of personal and professional, which can raise privacy concerns in e-discovery scenarios.

Aggravating an already difficult situation, many organizations—well over half in the survey—report that they rely on manual intervention (e-mail) for data collection. This raises a wide array of challenges, including security, inefficiencies, and the need to use different tools to access different data sets.

Organizations are seeking a wide range of improvements in data collection



In the face of such considerations, the cost savings associated with the advent of BYOD programs can start to diminish. That's one reason why experts such as AccessData are frequently asked by companies to help their IT departments collect data from devices to which they don't have access.

"That's the biggest problem with bringing your own devices to work," says Ewasko. "Data exists that may or may not be company related. You had access to devices previously because IT gave employees the system and usually created administrative passwords so they could get into it whenever they wanted to. Now it's user created, and IT has to ask the user to get into that device. Some companies end up closing their eyes from a corporate standpoint, hoping they don't get in trouble."

Of the companies with direct experience manually retrieving discoverable data from employee personal devices for investigations and other matters, many say they confront difficult challenges. According to the AccessData/CCBJ survey, these include: inefficient workflows, the need to deploy different tools for different data sets, unreliable results, and data security.

As a result, organizations are seeking a wide range of improvements in data collection, including more efficiency (60%) and speedier collection (44%); better search and reporting (46%); and heightened security (42%).

Given that so many organizations are using manual processes to collect data even though they are plagued by workflow, reliability and security issues, it is hardly a surprise that they are dissatisfied with their current approach. More than two out of three have engaged at least one—and in a significant number of cases many—service providers to help with data collection. And the majority of survey respondents—more than 60 percent—representing companies of all sizes, say they plan to procure a new or replacement solution—software—to help with the data collection process.

Policies, Practices and Protocols: The More You Know, The More You Can Do

In a recent white paper, "Successful eDiscovery in a Bring-Your-Own-Device Environment," multinational semiconductor manufacturer Intel discusses how and why its legal and IT departments worked together to design a BYOD program with e-discovery as the very first consideration.

"In our experience, any data in the enterprise may be identified for a legal matter—ranging from sensitive financial and intellectual property data to the seemingly benign, casual instant message," the company wrote. "Intel IT's e-discovery team needs to be able to locate and access ESI wherever it exists in the enterprise, whether the data is on corporate backup tapes, laptops, desktop PCs, or on personally owned tablets and smartphones."

The company recites the benefits and challenges it had to balance in its approach to enabling personal devices in the enterprise. With the many benefits, including security, productivity, flexibility and satisfaction, came big challenges. The biggest of all, it says, was "how to perform e-discovery on personally owned devices."

Intel is a gargantuan enterprise with untold resources, but enterprises of all sizes and shapes are facing the same challenges as BYOD programs transform their workplaces. Four of 10 respondents to the AccessData/CCBJ survey have faced the same challenge as Intel in the last 12 months: how to efficiently, effectively and safely collect data from employee-owned devices. Looking forward, more than nine in 10 expect to access employee data in the next 12 months, including from the following sources: mail apps (94%), text (72%), voicemail (55%), cloud (51%), and social media (43%).

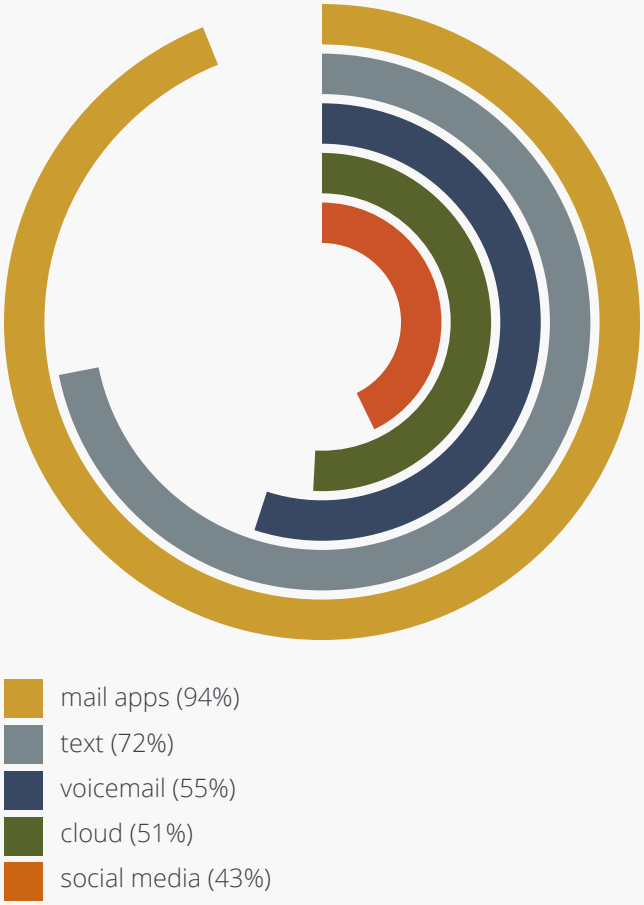
Given the uncertainty around both the legal requirements of e-discovery, which continue to evolve, and the rapid advance of technology, which if past is prologue will evolve even faster, the air of concern among our corporate legal respondents is understandable. Outside experts such as AccessData, with its focus on digital forensics, are providing substantial assistance by spotting trends around data types in the forensic market before they start to emerge in the commercial sector.

"New data types producing evidence will usually show up in law enforcement about five years before they become a pain point for corporations," Ewasko says.

Ewasko lays out a step-by-step process that organizations can use to help assure their BYOD programs are on solid ground:

- **Classify your data.** If your company cares about IP, if there are certain servers that contain a software company's source code, or if you have proprietary information that you don't want leaked, you're going to classify that as critical.
- **Establish procedures aligned with your classifications.** Who and what has access to the data? Continue the process until risk is mitigated by procedures, policies and permissions.

Nine in 10 companies expect to access employee data in the next 12 months, including from the following sources:



- **Test and test again to ensure it worked.** If in scanning your network you uncover data that shouldn't exist outside of your main critical servers, pull it off and remediate it.
- **Investigate how the data came off those critical servers.** If your permissions bar an administrative assistant from getting to critical data, maybe your investigation will discover that it was somehow on their desktop.

This is where forensic investigation tools are important for compliance, HR, and cyber investigations. They help you look for root causes on a system to determine what happened that put your data at risk. You can then take the necessary steps, including enacting changes in policy, to prevent it from happening again.

The challenges of performing e-discovery on personally owned devices that seem to get smaller and smarter every day are daunting. They are not, however, insurmountable.

AccessData delves into this with a compliance tool that helps you understand where data is located on a network. If you're looking for somebody who accidentally (or purposely) pulled down Social Security numbers or medical records with specific codes, you can find that on the network and remove it.

There are, however, no magic bullets. This is an iterative process. It has to be to stay a step ahead in such a rapidly evolving environment. By consistently going through this process from start to finish and constantly updating policies and procedures, your organization can prevent leakage of its most important data. That will solidify the foundation—and help secure the many benefits—of a robust BYOD program.

Conclusion

The challenges of performing e-discovery on personally owned devices that seem to get smaller and smarter every day are daunting. They are not, however, insurmountable.

Appropriate policies and procedures, buttressed with expert forensic guidance and battle-tested software, can spell the difference between a successful BYOD program that delivers on the many benefits organizations expect when they open their doors to personal devices at work and a program that visits financial and reputational harm on an organization.

As the AccessData/CCBJ survey results show, most organizations have already made the choice to go down the BYOD road. The question now is whether they want to make the trip as safe and enjoyable as possible.

ACCESSDATA®

CCBJ Corporate Counsel Business Journal

Whether it's for investigation, litigation or compliance, AccessData® offers industry-leading solutions that put the power of forensics in your hands. For over 30 years, AccessData has worked with more than 130,000 clients in law enforcement, government agencies, corporations and law firms around the world to understand and focus on their unique collection-to-analysis needs. The result? Products that empower faster results, better insights, and more connectivity. For more information, visit www.accessdata.com

Visit us online:
www.accessdata.com

Global Headquarters
+1 801 377 5410
588 West 300 South
Lindon, Utah

North American Sales
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales
+44 20 7010 7800
internationalsales@accessdata.com