WHITE PAPER

The Growing Need for Mobile Device Archiving

An Osterman Research White Paper

Published March 2014

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

One of the most important shifts in corporate work over the past several years has been the adoption of mobile devices in the workplace and the impact this has had on how employees do their jobs. Consider:

- Our research found that 33% of the typical information worker's time is spent doing work on a mobile device.
- We also found that 42% of work-related content is *accessed via* mobile devices, while 31% of content is *created* on mobile devices.
- A growing number of users have deployed mobile applications and cloud-based storage repositories that house corporate content without any sort of IT oversight.

Despite the rapid growth in the proportion of work that is now being accessed and created on mobile devices, our research found that only 50% of the work generated on a mobile device is actually ever archived to a central corporate location so that it is accessible for eDiscovery, regulatory compliance or other purposes.

However, even among organizations that archive mobile content, only 48% of archiving for this content occurs immediately and continuously. Another 29% of mobile archiving systems impose short delays before mobile content is archived, while for another one in eight users, there can be long periods before content is archived.

KEY TAKEAWAYS

The bottom line is that a growing proportion of corporate content is generated and accessed on mobile devices, but archiving of this content is not keeping pace. A failure to adequately archive content, regardless of the platform on which it resides, can result in a variety of problems, such as an inability to adequately place a legal hold on data, failure to find and produce all relevant content for eDiscovery or regulatory audits, spoliation of data, fines, sanctions, adverse inference instructions and other consequences.

Consequently, all organizations should implement archiving solutions for their mobile platforms and related content sources that permit this content to be searched and produced when needed. Best practice dictates that any mobile archiving solution is part of overall comprehensive archiving strategy that accounts for SMS/MMS, email, files, social media and other business records.

A growing proportion of corporate content is generated and accessed on mobile devices, but archiving of this content is not keeping pace.

ABOUT THIS WHITE PAPER

This white paper was sponsored by GWAVA, MobileGuard and Smarsh. Information on each company and their relevant solutions is provided at the end of this paper.

THE GROWING IMPACT OF MOBILITY

While a smartphone or tablet may be the customary definition of a "mobile" device, for purposes of this white paper, we have included laptops in the mix, as well, since laptops, along with smartphones and tablets, are mobile devices that generate content that must be archived. In fact, Osterman Research surveys have found that roughly 5% of all corporate content is maintained on mobile devices, although mobile communications are typically more critical from an archiving perspective than communications on conventional devices.

SMARTPHONES AND TABLETS

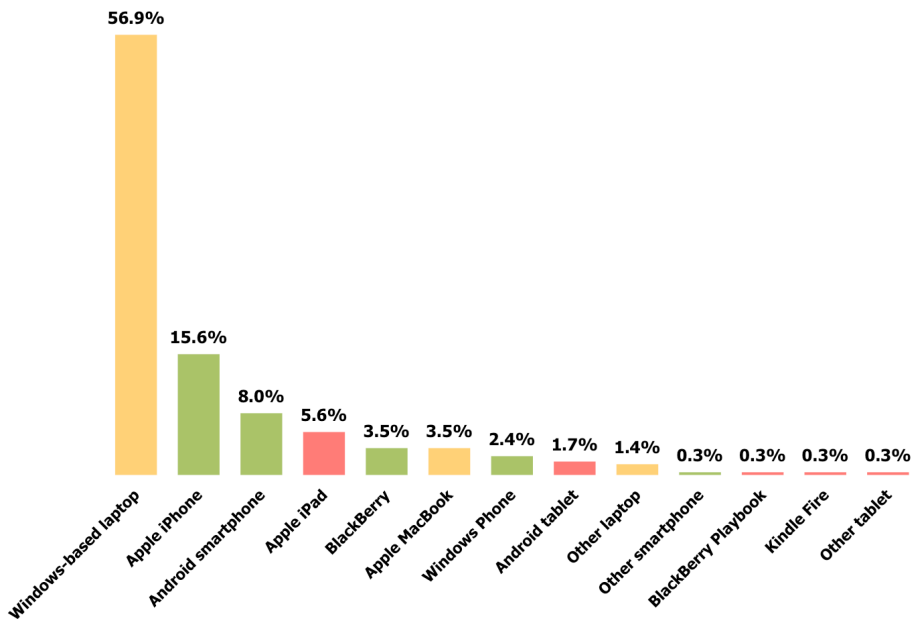
The vast majority of information workers employ mobile devices as an integral part of their work experience. Osterman Research has found that more than 80% of

organizations surveyed have employees who use mobile devices on a regular basis and that, in many cases, these are personally owned devices, not devices supplied by their employer.

Our research found that 30% of the mobile devices in use are employee-owned, although this is heavily skewed by the much greater penetration of employee-owned smartphones and tablets. For example, while only 18% of laptops are employee-owned, 49% of smartphones and tablets are owned by employees. We also discovered that employees in larger organizations are more likely to have a laptop as their primary mobile device, while employees in smaller organizations are more reliant on smartphones and tablets. Overall, we discovered that a much greater proportion of primary mobile devices used for work-related purposes were personally owned in smaller companies: 36% of these devices are personally owned in companies of under 1,000 employees, compared to only 25% in larger organizations.

The survey that we conducted for this white paper found that the most common primary mobile device in use is a Windows laptop, followed by an iPhone, an Android smartphone and an iPad, as shown in Figure 1.

Figure 1
Primary Mobile Device in Use



Source: Osterman Research, Inc.

Our research also discovered that users in smaller organizations employ more mobile devices for work-related purposes than their counterparts in larger organizations: a mean of 2.68 devices for employees in smaller organizations versus 2.43 for users in larger ones. The number of mobile devices in use has important implications for archiving practices, since the greater the number of devices in use, the more likely it is that content can be lost or corrupted if not archived immediately.

The number of mobile devices in use has important implications for archiving practices, since the greater the number of devices in use, the more likely it is that content can be lost or corrupted if not archived immediately.

MOBILE IS ABOUT MUCH MORE THAN DEVICES

While much of the emphasis on mobile focuses on the devices themselves, there are two other important trends in the context of mobile archiving:

- Bring Your Own Applications (BYOA), including the growing variety of mobile business apps for smartphones and tablets that store data and allow users to create data more easily, such as EverNote, WhatsApp, Pages, etc.

- Bring Your Own Cloud (BYOC), including the large number of cloud-based storage tools like Dropbox, OneDrive/Skydrive, Google Drive, etc.

The growth of BYOA and BYOC is being driven by a number of factors:

- Many mobile users are not satisfied with the applications and services offered to them by their IT department and consequently want to provide their own superset of features and functions to fill the gaps. For example, users who work from home or while traveling may not want to take files with them on a USB stick and manually synchronize this content when back in the office. A cloud-based file sync and share tool is a much more efficient way to manage this content, despite the potential security and content management risks it can introduce.

- IT often governs users' activities with corporate-managed applications. For instance, implementing limits on the size of email messages that can be sent or received. While IT does this to maintain acceptable levels of email server performance, it can prevent users from sending large files as part of their work. As a result, many users will opt for a free or low-cost, cloud-based file transfer tool to circumvent these rules.

- Many users simply prefer the ease of use and optimized interface of cloud-based or mobile apps compared to the more traditional capabilities that IT offers to them.

- Users who employ their own mobile devices are free to download apps as they please. IT, on the other hand, must typically provide a justification for implementing new tools and evaluate their security, performance and ability to be integrated into existing work processes.

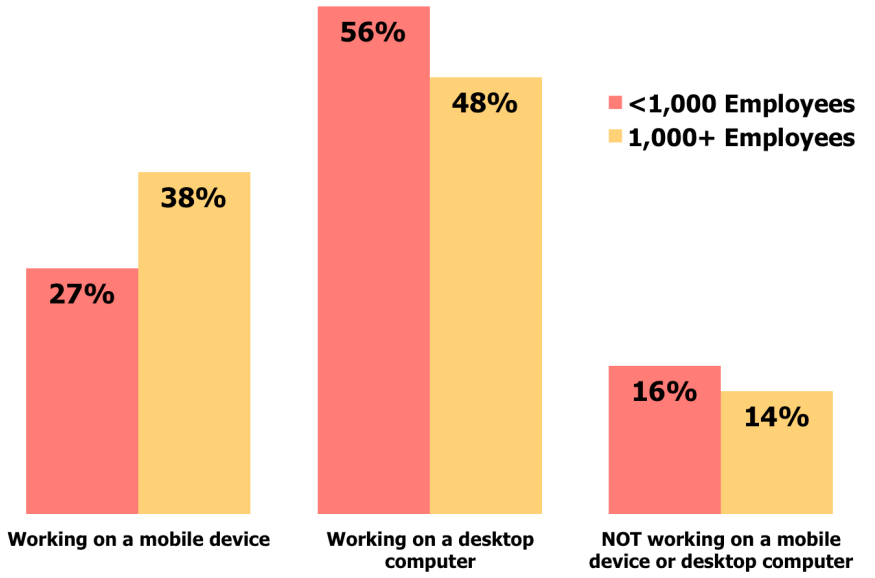
The result is that users are heavily influencing the tools that are used in the enterprise. While employees must still meet the security and information governance requirements that IT is obligated to impose, they will be much more satisfied, and in turn more productive at their work, when they have at least some involvement in the types of tools and applications that should be used

THE CHANGING NATURE OF WORK

Our research found that for information-focused employees, 33% of the time that they spend doing work is spent on a mobile device, while 52% is spent at a desktop computer. There are significant differences in these figures based on the size of the organization. We also found, as shown in Figure 2, that information-focused workers in larger organizations are more likely to use mobile devices than their counterparts in smaller firms.

For information-focused employees, 33% of the time that they spend doing work is spent on a mobile device.

Figure 2
Distribution of Work Time by Venue

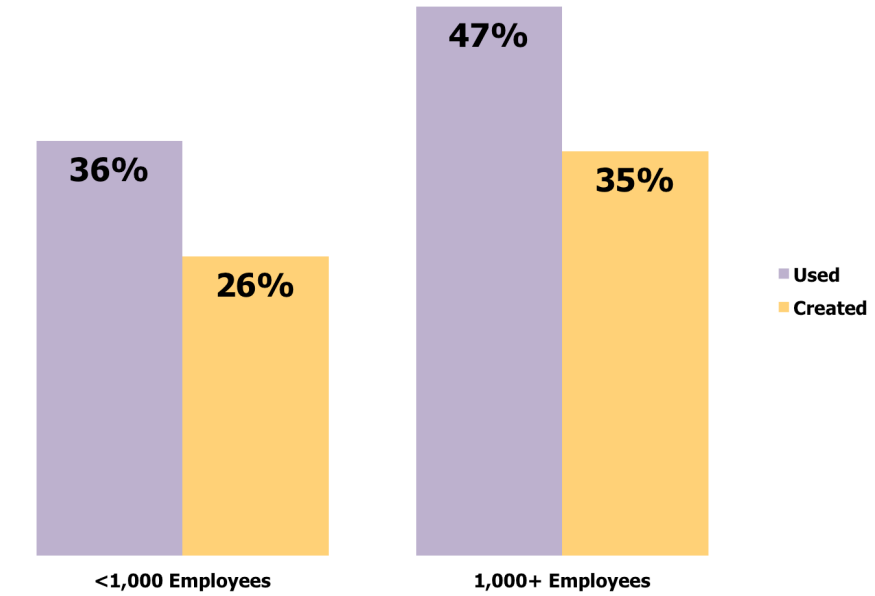


Source: Osterman Research, Inc.

The result has been that a significant proportion of content is accessed and generated on mobile devices. We found that 42% of work-related content (email, documents, databases, social media, etc.) is *accessed* on mobile devices, while 31% of content is *created* on mobile devices, as shown in Figure 3 (although here again there are significant differences based on organization size).

42% of work-related content is used on mobile devices, while 31% of content is created on mobile devices.

Figure 3
Proportion of Content Accessed and Created on Mobile Devices



Source: Osterman Research, Inc.

THE IMPLICATIONS OF BYOD, BYOA AND BYOC

The consumerization of IT – as exemplified by the continuing adoption of Bring Your Own Device (BYOD), Bring Your Own Applications (BYOA) and Bring Your Own Cloud (BYOC) – represents a paradigm shift in the nature of corporate work and employee behavior. While there are serious issues raised by these trends that must be addressed (see page xx), BYOD, BYOA and BYOC, if managed properly however, will yield significant benefits to organizations of all sizes and across all industries.

The increasing functionality and utility of mobile devices, cloud storage and specialized applications enable users to create and consume a growing proportion of content while mobile. Users can be more productive and work from virtually any location, instead of being limited to working only from an office or a desktop computer. In theory, this allows organizations to become more agile because employees are working remotely with greater efficiency and with less reliance on being in a specific location to do their work.

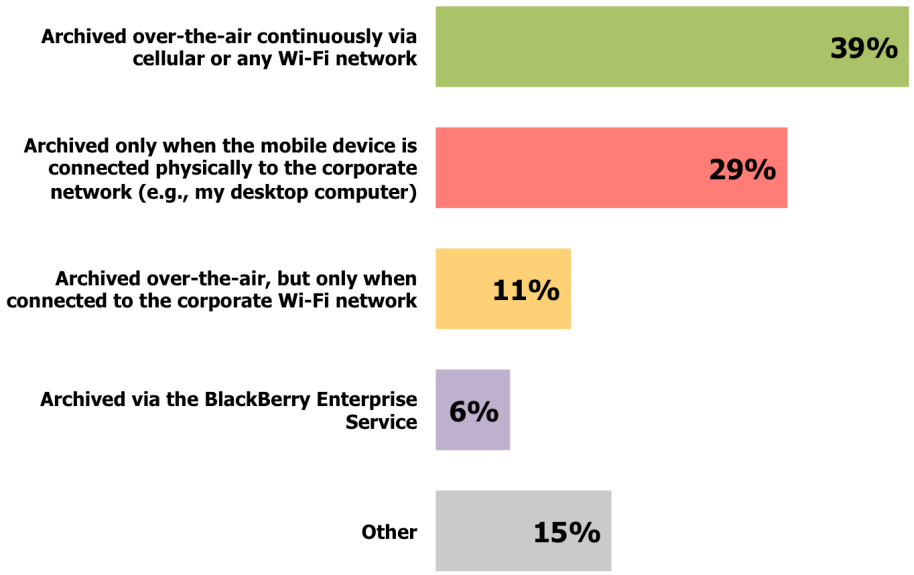
THE IMPLICATIONS OF MOBILITY ON ARCHIVING AND DATA SECURITY

MOBILE DEVICES ARE OFTEN DISCONNECTED FROM THE CORPORATE NETWORK

Our research found that among users whose mobile content is archived, only two out of five have this content archived continuously. Three out of 10 have their mobile content archived only when connected physically to the corporate network, while one in nine have their mobile content archived only when connected to the corporate Wi-Fi network, as shown in Figure 4.

The capture of mobile content is sporadic for the majority of mobile users whose content is archived.

Figure 4
Mobile Archiving Practices Among Organizations That Archive Content

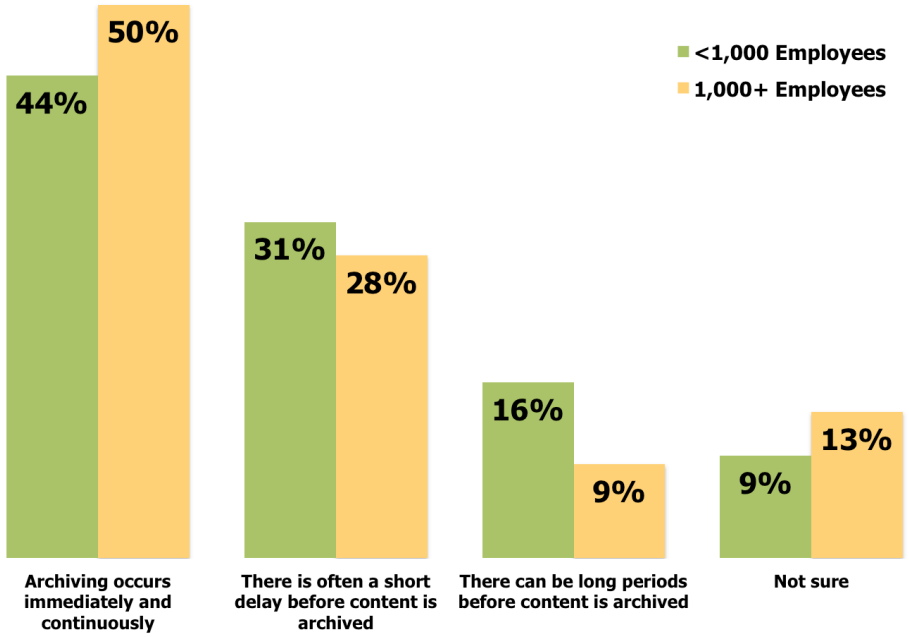


Source: Osterman Research, Inc.

Meanwhile, as shown in Figure 4, only about two in five users' mobile content is archived over-the-air continuously. A growing proportion of content is either not archived to a central location in a timely manner, or it is not archived at all, let alone backed up or archived in real time. As shown in Figure 5, no more than one-half of

users whose mobile content is archived report that archiving occurs immediately and continuously. The balance indicated that there are delays in mobile content archiving, while many simply are not sure how much of a delay they experience.

Figure 5
Mobile Archiving Practices



Source: Osterman Research, Inc.

BYOD, BYOA AND BYOC MAKE THE PROBLEM WORSE

The mobile archiving problem is made significantly worse by the consumerization of IT: namely, the growing use of personally owned mobile devices, mobile apps and cloud-based storage repositories:

- Content that is created and stored on personally owned devices is under the primary control of the employee, not the employer. Employees who create and store corporate content on mobile devices, without also maintaining an up-to-date archive of this content on corporate systems, increase corporate risk by making some content inaccessible.

- Similarly, content created using personally deployed mobile apps can create its own set of risks when information is generated and stored in formats that may not be compatible with corporate systems. This makes corporate content, even if it is archived, more difficult to access and process. IT has little control over the types of personally deployed applications in use and may be completely unaware of them.

- The existence of content stored in the cloud, such as in a personally managed Dropbox or OneDrive account, can be completely outside of IT's knowledge. IT, legal or other functions within a company may be completely unaware of these repositories, and may subsequently go through an eDiscovery exercise, impose a legal hold, or attempt to satisfy a regulatory audit without knowledge of or access to all relevant content. Even if the organization is aware of this content, but cannot access it – for example, because of an employee's departure from the company – the result will be the same.

The mobile archiving problem is made significantly worse by the consumerization of IT: namely, the growing use of personally owned mobile devices, mobile apps and cloud-based storage repositories.

The bottom line is that mobility – particularly personally managed mobile devices, applications and content repositories – makes content less archivable and less accessible to organizational decision makers.

THE CONSEQUENCES CAN BE SERIOUS

Mobility introduces a number of problems – some of them quite serious – in the context of archiving and managing corporate content. Organizations that cannot today meet their formal and informal compliance obligations for mobile content should consider the consequences of their inability to do so.

CONTENT MANAGEMENT FOR LITIGATION IS MORE DIFFICULT

Virtually all organizations will face litigation at some point, either as a defendant, plaintiff or otherwise interested third party. If a legal action is "reasonably anticipated," it is necessary that an organization immediately begin to identify and preserve all of the content that might be considered relevant for the duration of the legal action. For example, a claim for a breached contract with a contractor could require retention of emails and other electronic documents between employees and the contractor, or between employees talking about the contract or the contractor's performance. A well configured eDiscovery and data archiving capability will allow organizations to immediately place a hold on data when requested by a court or regulator or on the advice of legal counsel, to suspend deletion policies and practices, and to retain the data for as long as necessary.

Organizations that must place a legal hold on data will find doing so on mobile or personally managed, cloud-based data more difficult than for data on conventional, IT-managed platforms. While some organizations use notifications to alert employees of their need to hold data, this is highly ineffective as a means of enforcing a legal hold. Parties to litigation that do not hold Electronically Stored Information (ESI) properly are subject to a variety of consequences, including harm to the organization's reputation, added costs for third parties to review or search for data, court fines or other sanctions, directed verdicts or adverse inference instructions.

Similarly, eDiscovery in a mobile environment is much more difficult than it is for conventional platforms that are located behind the corporate firewall. A key issue for legal and IT staff charged with accessing relevant content for eDiscovery purposes is that they may not even be aware of the existence of certain pieces of content that might be relevant. This content might include documents, spreadsheets, notes and other data that were created on a mobile device and might have been copied to a personally managed cloud repository, but not to a centralized corporate archive. Even if legal and IT staff is aware of content that they might need for eDiscovery purposes, they might not be able to access it from mobile devices or personally managed cloud data sources.

An organization that cannot or will not produce ESI from a mobile device in response to an eDiscovery order can face sanctions, fines or adverse inference instructions. An interesting case in this regard is *Barrette Outdoor Living, Inc. v. Michigan Resin Representatives*[1]. Barrette sued John Lemanski, a former employee, claiming that Lemanski defrauded Barrette. Lemanski, despite having been emailed a notice to preserve ESI by Barrette, acquired a new mobile phone and returned his old device to the carrier. Moreover, after Barrette had filed a motion to compel Lemanski to provide his laptop for imaging, Lemanski deleted roughly 270,000 files that he claimed were personal and not relevant to the case at hand. The court disagreed with Lemanski's actions and ordered him to pay Barrette $35,000 in compensation. In addition, the court indicated that "at trial, there will be an adverse inference that

Mobility – particularly personally managed mobile devices, applications and content repositories – makes content less archivable and less accessible to organizational decision makers.

[1] http://www.americanbar.org/content/dam/aba/publications/litigation_news/barrette-mich-resin.authcheckdam.pdf

Lemanski's cell phone and personal laptop contained information unfavorable to Lemanski…"

This case is illustrative of the importance of maintaining a properly configured mobile archiving capability, since such a solution would have allowed Barrette to archive all of the relevant content it sought from both the mobile device and the laptop before Lemanski could have deleted it.

HEAVILY REGULATED ORGANIZATIONS MUST ARCHIVE MOBILE CONTENT

Heavily regulated organizations – e.g., those in the financial services, healthcare, life sciences, energy or government space – must satisfy a variety of regulations with regard to retention of content. This includes retention of content from mobile devices, as in the following examples:

- FINRA Regulatory Notice 07-59 states that, "….FINRA expects a firm to have supervisory policies and procedures to monitor *all* electronic communications technology used by the firm…" It is important to note that the content of the message determines its classification as a "business record" and whether or not it needs to be retained.

- The Federal Energy Regulatory Commission (FERC) Order No. 717 requires that all emails, voicemail, text messages and other communication between energy companies' transmission and marketing functions must be retained for five years.

- 45 CFR 164.316 states that healthcare-related "Covered Entities" must "retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later."

These regulations and those like them typically do not differentiate between the platforms that are used to create or store electronic content.

FERC Order No. 717 requires that all emails, voicemail, text messages and other communication between energy companies' transmission and marketing functions must be retained for five years.

USER AND PRODUCTIVITY ISSUES

Another potential problem with an inability to access archived content from mobile devices or personally managed cloud repositories is that users will often not have access to the most recent versions of documents, resulting in version control issues. For example, a traveling employee who creates documents on his or her tablet and cannot archive this content will create a situation in which others who need access to this information will not have it available. They may have to wait for these documents to be made available, or they may mistakenly work on incorrect versions.

DATA MINING IS MORE DIFFICULT

One of the fundamental difficulties created by an increasingly mobile workforce – particularly one in which a large number of personally owned devices is used – is that data mining becomes more difficult. Because a large proportion of content is stored on mobile devices that may not be accessible to the organization at large, a significant part of an organization's content that might otherwise be mined and analyzed cannot be. Mobile devices, applications and cloud repositories result in additional sources for data mining purposes. Content stored outside of corporate systems may never be accessible.

RECOMMENDATIONS

UNDERSTAND WHERE YOUR DATA IS

First and foremost, decision makers must know where their data is located. Corporate content is normally distributed across a range of platforms, including file servers, email systems, desktop computers, laptops, smartphones, tablets, employees' home computers, backup tapes, archives, cloud file repositories, USB sticks, and employees'

personal accounts of various types. While most of this content is accessible to the organization at large, much of it is not.

It is essential that decision makers be able to identify the location of all relevant data on mobile devices – documents, spreadsheets, presentations, notes, text messages, photos, instant messages, call logs and all other relevant data – and gain access to it. This includes content from both company-supplied and personally managed devices that might contain corporate data. While this might not be an easy undertaking in every circumstance, it is essential as an information governance best practice.

DEVELOP THE RIGHT POLICIES

Second, decision makers must develop policies that will enable full and ready access to all of their corporate content, including the content that is stored on mobile devices. While the policies will vary based on the industry that an organization serves, its BYOD policies, the geographic distribution of its users, its corporate culture, etc., these policies should include some key elements:

- A clear set of statements about which devices, mobile applications and cloud-based content repositories are permitted for use in the organization when accessing, creating and storing information.
- Which devices, applications and repositories are not permitted for use with corporate content.
- A requirement that users grant to the IT department access to any and all corporate content, regardless of its location, even if that data is stored in a personally managed account.
- A clear statement that the organization maintains the right to gain access to all corporate content under the control of the employee, even if that content is on a personally owned device and even if the employee is no longer actively engaged with the company.

Decision makers must develop policies that will enable full and ready access to all of their corporate content, including the content that is stored on mobile devices.

IMPLEMENT TECHNOLOGIES THAT WILL ENFORCE POLICIES

Finally, the appropriate technologies must be deployed that will, at a minimum, enable copying of all content on mobile devices, in cloud-based repositories and from mobile applications to IT-managed systems in real time or near real time. The much better choice, however, is to deploy a true archiving solution that will enable archiving directly from mobile devices, from user-managed cloud repositories and from any mobile application data store. Best practice dictates that any such archiving solution place content directly into a centralized archive so that all content, regardless of the platform that generated it, can be searched and managed holistically.

SPONSORS OF THIS WHITE PAPER

Retain Mobile securely archives mobile communications for Android and BlackBerry

As mobile devices begin to permeate organizations and companies worldwide, companies must have the ability to quickly archive all of the communications data that is produced by these devices. This ensures compliance with corporate policies or government regulations and helps to reduce legal liabilities.

Retain Mobile helps to assure that companies:

- Meet regulatory compliance standards (SEC, FINRA, FRCP, Sarbanes-Oxley, HIPAA)
- Monitor smartphone usage to ensure compliance with corporate policies Z10

www.gwava.com
@GWAVA
info@gwava.com
+1 866 464 9282

Retain Mobile securely archives SMS/MMS and phone call logs for Android devices (2.2 and above) as well as BBM, PIN, SMS/MMS and phone call logs for BlackBerry 10 devices.

How Retain Mobile Works for Android
Retain Mobile operates through a lightweight app that is installed on each device. This app captures all SMS/MMS and phone call log data. The captured data is then automatically sent to and stored in your Retain archive in the cloud or on-prem.

How Retain Mobile works for BlackBerry
When it comes to BlackBerry, Retain archives all mobile communications for BlackBerry Devices via the BlackBerry Enterprise Service (BES). Retain for BlackBerry pulls the data directly from the BlackBerry Enterprise Service itself; therefore, individual BlackBerry device communications are tracked and logged without the need for an app to be installed on each BlackBerry device. And Retain for BlackBerry archives all data to the Retain unified archive database. There, the data is easily reviewed, retrieved, discovered and published--on demand.

With Retain Mobile you keep and safeguard all of your organization's valuable information; moreover, your organization stays compliant and your sensitive data stays secure within your organization.

Retain Unified Archive
Retain provides world-class unified message archiving, eDiscovery and publishing for organizations looking to:

- Reduce Costs
- Manage complexity
- Mitigate risk on-premises or in the cloud

With Retain Mobile you can archive everything into one location: email, social media interactions, and mobile messaging. With Retain you're ready to seamlessly archive single- or mixed-messaging platform environments, as well as to archive your social and mobile messaging, all in one central location. Once they are archived, messages are then securely stored in a single, unified Retain data archive where they can be easily accessed through the Retain web access archive viewer.

MobileGuard™, formerly TextGuard, is the pioneer and leader in providing comprehensive mobile communication monitoring and archiving solutions since 2007. To ensure regulatory compliance and provide risk management, MobileGuard's compliance platform offers the most complete solution for your mobile workforce.

MobileGuard's suite of compliance solutions enables your company to maintain efficiency using mobile technology while working within your current regulatory environment, (e.g., FINRA, FERC, HIPAA, Dodd-Frank, Federal Rules of Civil Procedure). With such a solution in place, all mobile communications are monitored and archived according to the policies and settings you define, and easily managed from the MoblieGuard portal.

The comprehensive solutions offered by MobileGuard can be delivered as standalone products, or seamlessly integrated with existing email archiving systems.

- **NetGuard** is a comprehensive mobile compliance solution for enterprises that provides unified, device independent, real-time monitoring, alerts, capture, archival, and analysis across mobile, social, and corporate communications. It supports all operating systems including but not limited to: **Apple iOS, Android, Blackberry and Windows.**

mobileGuard

www.mobileguard.com
@MobileGuardNYC
info@mobileguard.com
+1 646 459 4354

- **MessageGuard™** for SMS/MMS provides complete capturing, monitoring, and archiving of SMS, MMS, BBM, PIN-to-PIN, Instant Messages and Call Logs sent to and from company mobile devices, (Mobile Client Application OR BES Application)

- **VoiceGuard™** is a client-based solution that enables companies to record and archive all incoming and outgoing voice calls from company-issued or sponsored smartphones. All recording is done automatically with no user intervention required.

- **CloudChat™** provides an employee-to-employee cloud communication solution. Instant messaging as well as voice conversations may be monitored and archived to meet regulatory requirements, lower the risk of compromised data as well as meeting regulatory requirements.

For a free 30-day trial of MessageGuard, please visit http://www.mobileguard.com/registration.

Smarsh delivers cloud-based archiving solutions for the information-driven enterprise. Its platform enables organizations to archive, search, supervise and produce the entire range of digital communications from one central location, including email, public and enterprise social media, Web, instant messaging and mobile messaging.

Founded in 2001, Smarsh helps more than 20,000 organizations meet regulatory compliance, e-discovery and record retention requirements. The company is headquartered in Portland, Ore. with offices in New York City, Atlanta, Boston and Los Angeles. For more information, visit www.smarsh.com, follow @SmarshInc on Twitter or like Smarsh on Facebook at www.facebook.com/SmarshInc.

www.smarsh.com
@smarshinc
sales@smarsh.com
+1 866 762 7741
+1 503 946 5980