WHITE PAPER

The Growing Importance of Archiving Mobile Text Messages

An Osterman Research White Paper

Published June 2017

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

Mobile devices are used increasingly in the workplace – Osterman Research data demonstrates that about one-third of the typical information worker's day is spent working on a mobile device, and much of this involves send or receiving text messages and other communications. Moreover, 28 percent of employees use a company-supplied smartphone and 36 percent use a personal smartphone for business purposes.

However, despite the fact that mobile users generate and store business records on their mobile devices, only a small proportion of this content is ever archived, despite the fact that archiving electronic content from corporate email and other systems has been a best practice for many years. This failure to archive content from mobile devices put organizations at risk of running afoul of their compliance obligations, it makes them unable to produce content in response to eDiscovery orders, it prevents all content from being placed on legal hold, and it does not allow the sharing of important business content from mobile users.

In short, a failure to archive content from mobile devices increases corporate risk and makes organizations more susceptible to compliance and legal violations.

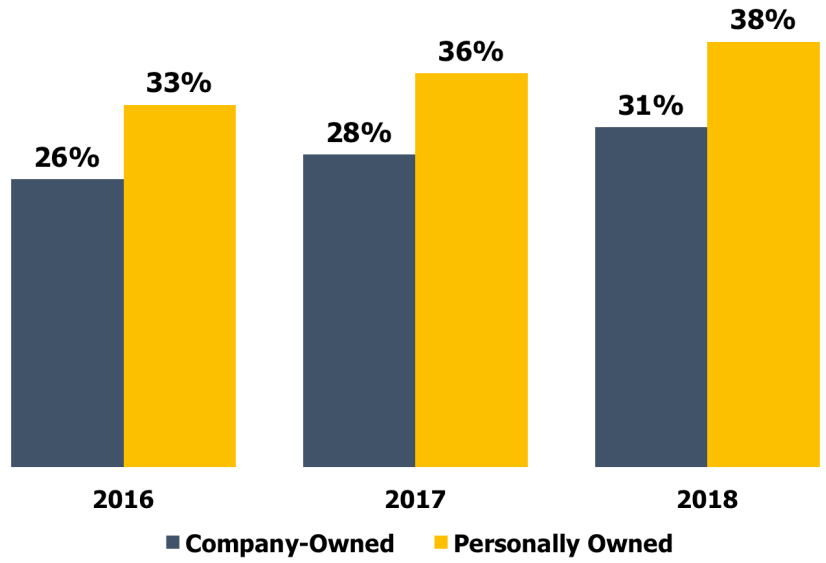
ABOUT THIS WHITE PAPER

This white paper was sponsored by TeleMessage – information about the company is provided at the end of the paper.

THE GROWING IMPORTANCE OF MOBILE

Osterman Research has found that roughly one-third of the typical information worker's day is spent working on a mobile device, and an even greater proportion of work-related content is accessed using mobile devices. The impetus for the growing use of mobile devices is driven by a number of factors, although the use of personally owned devices is a key factor in their adoption in the workplace. As shown in Figure 1, the use of company-owned and personally-owned smartphones is on the increase.

Figure 1
North American Penetration of Company- and Personally-Owned Smartphones, 2016-2018



Source: Osterman Research, Inc.

A failure to archive content from mobile devices increases corporate risk and makes organizations more susceptible to compliance and legal violations.

The move to personally owned devices – the so-called Bring Your Own Device (BYOD) trend – is pervasive today in organizations of all sizes. It enables users and IT to improve worker productivity and generate greater employee satisfaction, reduce costs and innovate faster. The trend toward BYOD reflects the general trend of enabling anytime, anywhere collaboration for workers who expect to be as productive away from the office as they are when working within their corporate network.

GROWTH OF MOBILE MESSAGING IN THE WORKPLACE

The use of messaging applications on mobile devices, such as email and SMS/text messaging, are among the most common applications of mobile devices in the workplace. The vast majority of users who employ a smartphone for work-related uses employs some type of messaging-related application on a regular basis.

WHY ARCHIVE TEXT MESSAGES FROM MOBILE DEVICES?

ELECTRONIC CONTENT MUST BE ARCHIVED

Any archiving solution a) ingests email and other digital content, b) indexes that content, and c) places it into archival storage where it can be searched and produced for a variety of purposes. Archiving of email and other digital content has been a best practice for many years, first in heavily regulated industries like financial services and life sciences, but later across all industries. The primary drivers for archiving will vary by organization and industry, but include the following:

- **Regulatory compliance**
  Virtually every organization has some level of regulatory requirement to retain and produce content. While strict regulatory obligations exist in several key industries, such as financial services, insurance, healthcare, energy, utilities, government (e.g., for Freedom of Information Act requests), and life sciences (as discussed later in this paper), every organization has an obligation to retain and properly manage certain types of data. These regulations obligate organizations to retain information like financial documents, certain types of email correspondence, employee records, and communications with clients. Even metadata must be preserved in many cases.

  Another important consideration for archiving in the context of regulatory compliance is the retention of data by public companies to satisfy the Sarbanes-Oxley Act (SOX). The failure of public companies to comply with the archiving and other provisions of SOX can result in significant penalties. Outside of the United States, various countries and other jurisdictions (such as the European Union, or EU) have similar types of regulations. A notable example is the General Data Protection Regulation (GDPR) that will go into effect in May 2018, and that will impose strict data protection obligations on any country that holds or processes on data subjects in the EU.

- **Supporting litigation and eDiscovery**
  Almost every business organization will eventually become involved in a legal action of some sort, either as a plaintiff, as a defendant, or as an interested third party. Consequently, organizations must retain information they might need in order to pursue a legal action or defend themselves in one. Every organization has an obligation under requirements like the Federal Rules of Civil Procedure (FRCP) to search for and produce electronic content, such as email, files and text messages. The duty to produce this information might be based on an eDiscovery order from a court, or it can occur when decision makers become aware that litigation might be forthcoming, requiring the organization to place a "litigation hold" on relevant data in order to prevent its deletion.

- **End-user self-service**
  A key benefit of an archive is the ability for end users to access their older content for long periods without the requirement to store this data on "live" servers or in an email inbox. By archiving this content and giving users access to it, both IT and end users benefit: IT can place strict quotas on mailbox size, which speeds the backup and restoration of servers; and users benefit by having access to content as old as they need. Plus, users can readily access their older content without having to bother IT with requests to search for and restore these files.

- **Retention of corporate memory**
  Another key driver for archiving is the ability to retain relevant information to maintain an appropriate record of an organization's history – it's corporate "memory".

THE DISTINCTIONS BETWEEN ELECTRONIC CONTENT ARE BLURRING

As noted above, email archiving has been a best practice for the past couple of decades. For example, in the United States the Financial Industry Regulatory Authority (FINRA) has required various types of financial services companies to archive email communications with their clients. In 2003, FINRA specified that instant messages had to be archived, and in 2010 FINRA issued new guidance for the archiving of social media content. At the same time, the notion of "archiving" has expanded beyond just email to other types of content, such as files, text messages and, in some cases, voicemail.

Over time, the fundamental shift in archiving has been away from archiving specific types of content, such as email, and toward the retention of business records, regardless of the medium in which they may be found or the system that created them. This shift is being driven by regulators and courts expanding their view of the types of electronic content that should be retained.

The fundamental shift in archiving has been away from archiving specific types of content, such as email, and toward the retention of business records.

THE CONSEQUENCES OF FAILING TO ARCHIVE TEXT MESSAGES

Almost every organization will face litigation at some point, either as a defendant, plaintiff or otherwise interested third party. If a legal action is reasonably expected at some point, decision makers immediately need to identify and preserve all of the content that might be considered relevant for the duration of the potential legal action. As one example, a claim for a breached contract with a contractor could necessitate the retention of emails and other content between employees and the contractor, or between employees talking about the contract or the contractor's performance. A good data archiving capability will allow organizations to immediately place a hold on data when requested by a court, regulator or on the advice of legal counsel, allow it to suspend deletion policies and practices, and to retain the data for as long as needed.

A legal hold placed on data from mobile devices will usually be more difficult than for data on conventional, IT-managed platforms like email systems. While some organizations notify employees of their need to hold data, this is not effective as a means of ensuring that a legal hold actually takes place. Parties to litigation that do not hold Electronically Stored Information (ESI) properly are subject to various 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.

In the same way, eDiscovery on mobile devices is more difficult than it is for conventional platforms. A key issue for legal and IT staff charged with accessing relevant content for eDiscovery purposes is that they might not even be aware that certain documents may exist or be relevant. This could 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 the legal and IT staff are aware of content that they might need for eDiscovery, they might not be able to access it from mobile devices.

If ESI from a mobile device cannot be gathered in response to an eDiscovery order, the organization can face sanctions, fines or adverse inference instructions. For example:

- In early 2017, a banker formerly with the firm of Jefferies Group LLC was fined £37,198 by the UK's Financial Conduct Authority (FCA) for using WhatsApp to share confidential information about two Jefferies clients with a friend. (WhatsApp provides end-to-end encryption between recipient and sender, which is not considered best practices in highly regulated firms.) Even though the banker is not alleged to have profited from his sharing of the confidential information, the FCA sought to impose a heavy fine in this case.

- In order to prevent the type of compliance problem experienced by Jefferies, Deutsche Bank AG banned the use of WhatsApp and other text messaging and chat apps for work-related communications. The bank made this rather extraordinary and disruptive change because of its perceived inability to archive this content as it does with emails.

- In the case of *Barrette Outdoor Living, Inc. v. Michigan Resin Representatives*[1]. Barrette sued John Lemanski, a former employee, claiming that Lemanski defrauded Barrette. Lemanski, even though having received an email notice to preserve ESI by Barrette, purchased a new mobile phone and returned his old device to the carrier. Further, 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. Moreover, the court indicated that "at trial, there will be an adverse inference that Lemanski's cell phone and personal laptop contained information unfavorable to Lemanski…"

This is a good example of the importance of maintaining a well configured mobile archiving solution, since it would have permitted Barrette to archive all of the relevant content it needed from both the mobile device and the laptop before Lemanski could have deleted it.

COMPLIANCE CHALLENGES

Organizations worldwide operate within the constraints of regulations and other compliance obligations based on the industries, countries, regions and legal jurisdictions in which they operate. In principle, the concept of compliance obligations, whether based on specific regulations or legal requirements, is straightforward: an external organization with a mandate and authority imposes requirements that must be met or a variety of penalties can be imposed. The regulations are often defined as actions that need to be taken (e.g., store all email messages for three years), or actions that *should not* be taken (e.g., do not delete important email messages), along with an evidence trail to show that the rules were followed. As a result, compliance is the ability to prove beyond reasonable doubt that an organization has met the conditions of the imposed requirements. The production of evidence to demonstrate compliance requires internal procedures, structured processes and technology-based systems.

Among the various challenges that organizations face from a compliance perspective in the context of mobile archiving are the use consumer-focused messaging apps, the use of personally owned devices over which IT may have little or no control, lack of support by certain carriers, and the costs associated with archiving this content.

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

KEY ISSUES TO CONSIDER

With respect to electronic communications and the data they generate, a set of general and common requirements are imposed across many industries, countries, and regions. Broadly speaking:

- Electronic communications should be captured, stored in a secured location, and be unchangeable once captured. For most organizations, this is not being done for communications that take place using mobile devices.

- These communications must be retained for a certain length of time, normally three to seven years, but sometimes much longer (or indefinitely). The records must not be changed or deleted during this period.

- When necessary, organizations must be able to produce verifiable and authentic copies of all communications that meet certain criteria. This requires good search tools that can identify relevant communications, and the ability to create a collection for further review.

- Once the retention period for communications has been reached, those messages can be validly deleted. However, if messages that have reached their expiration date are being held for a current or potential investigation, deletion must not occur until the legal hold has expired.

- The unauthorized access to systems and data should not occur. A way of controlling access to systems and data is necessary, and encryption of data may be necessary.

KEY REGULATIONS

In the United States, there are a number of regulations that require retention of data. For example:

- **Financial Services Organizations**
  The Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), PATRIOT Act, and Gramm-Leach Bliley Act (GLBA) – among many other regulations – impose particular requirements on financial services organizations. FINRA, for example, sets various requirements on the capture, monitoring, and archival of broker communications, and it demands a supervisory review process. GLBA imposes rules on privacy of financial information about customers, and sets standards on how to protect this information. The PATRIOT Act requires an identity trail for customers opening new accounts.

- **Healthcare Organizations**
  The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets various requirements on protecting health information that is "individually identifiable." There are a number of technology, policy, and procedural requirements to safeguard this information when stored and transmitted.

- **Organizations that Serve the US Federal Government**
  The Federal Acquisitions Regulations (FAR) require that contractors to the US federal government preserve all records, both hard copy and electronic, for between two and four years. This covers organizations that provide both physical products and services.

- **State and Local Governments/Public Sector Agencies**
  The Freedom of Information Act (FOIA) gives citizens the right to request access to records held by any federal agency. While agencies can respond to FOIA requests in the order in which they are received, there are situations where expedited processing is required. Most states and municipalities have similar open-records or "sunshine" laws.

Electronic commun-ications should be captured, stored in a secured location, and be unchange-able once captured.

- **Publicly Traded Organizations**
  Sarbanes-Oxley (SOX) requires that the financial records of publicly traded companies be preserved for up to seven years, and these records must be available for review by the SEC at any time.

- **Designated "High-Risk" Organizations**
  Chemical manufacturing and energy distribution facilities, along with transportation operations, are designated as high-risk operations under the Homeland Security Act. These types of organizations have security and recordkeeping requirements with which they must comply.

AROUND THE WORLD

Outside of the United States, various countries, regions, and economic blocs have their own regulations, such as:

- The EU Data Protection Directive for data privacy in the European Union.

- The successor to the Data Protection Directive, the General Data Protection Regulation (GDPR) that will go into effect on May 25, 2018.

- The Markets in Financial Instruments Directive (MiFID) II, which will go into effect on January 3, 2018, includes increased protections for investors and enhanced supervision of certain financial markets. This will result in an increased focus on data retention and production to enhance transparency of financial dealings.

- The Investment Dealers Association of Canada requires financial services organizations to retain communications across a variety of channels (IDA 29.7).

- The province of Ontario, Canada implemented the Personal Health Information Protection Act (PHIPA) as one of two parts of the Health Information Protection Act in 2004. PHIPA requires any entity that possesses or maintains healthcare-related information to manage this content securely and to ensure that healthcare records are "retained, transferred and disposed of in a secure manner" (2004, c. 3, Sched. A, s. 13 (1). Amendments to PHIPA added specific requirements with regard to the management of electronic health records 2016, c. 6, Sched. 1, s. 1 (13)). The Personal Information Protect Act (PIPA) – which applies to organizations in Alberta, British Columbia, Ontario and Quebec – includes similar types of provisions.

- Another Canadian requirement is the Personal Information Protection and Electronic Documents Act (PIPEDA), which includes the provision that "The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held. (4.7 Principle 7 – Safeguards)"

- The Government of Canada has established specific requirements for the retention of various types of government records. For example, the *Policy on Electronic Authorization and Authentication* and the *Policy on Internal Audit* suggests that some electronic records should be retained for up to six fiscal years.

- FCA SYSC 9.1.2 requires financial services firms to have a common retention platform for all records related to MiFID-focused business operations.

- The Swiss Financial market Supervisory Authority (FINMA) requires the retention of all electronic communications that employees send in the context of securities trading.

WHO SHOULD BE INTERESTED IN TEXT MESSAGE ARCHIVING?

TRADITIONAL ARCHIVING VENDORS

Today, most archiving solutions do not include an option for the archival of content from mobile devices, such as text messaging. However, vendors of traditional archiving solutions should seriously consider adding the ability to archive content from mobile devices if they have not already done so. The primary focus here would be emails and text messages, although other content from mobile devices that would not otherwise make its way to corporate servers or other platforms should be archived, as well.

Traditional archiving vendors can develop their own solutions for the archival of text messages and other content, but it often makes more sense to partner with existing firms that have already developed the technology and simply integrate these solutions.

TELECOM OPERATORS

Similarly, telecom operators are also a prime market for mobile archiving capabilities given the hundreds of billions of texts sent each year, a large percentage of which include content that their customers will want to archive. SMS and other mobile content that contains business records should be archived, but today many cannot archive these records in a way that satisfies business requirements.

ENTERPRISES

More heavily regulated organizations, such as those in financial services, healthcare, life sciences, energy or government must satisfy a variety of regulations with regard to retention of content, as discussed above. 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 sample regulations and those like them typically do not differentiate between the platforms that are used to create or store electronic content – if business records were created on a mobile device, they should be archived like any other communications.

Organizations using various and inconsistent methods for archival of text messages makes the process inefficient, expensive and prone to error.

BEST PRACTICES TO CONSIDER

OVERCOMING THE DIFFICULTIES IN ARCHIVING TEXT

There are a number of difficulties associated with the archival of text messaging content. For example:

- Text messages sent using telecom carriers are often retained only for brief periods, and so these providers cannot be relied upon a source of archived text messages for long periods.

- Since some companies operate in multiple countries using carriers that often do not provide any sort of text messaging archival service, enterprises often employ different methods to archive text messages, such as doing a physical backup of a device.

- Further complicating the archival of text messages is the lack of commonality for archiving content depending on the device in use. Some solutions pull content directly from the server (e.g., with the BlackBerry Enterprise Server), while others install an app on the mobile device that transmits text messages to the archive. Other tools, such as SMS Backup+ for Android devices, will move text messages into a user's Gmail account where they can be backed up or archived indirectly.

The bottom line is that organizations using various and inconsistent methods for archival of text messages makes the process inefficient, expensive and prone to error. The result can be incomplete archives of text messages and the consequences that go along with this level of inconsistency. It is essential to choose the right vendor that can provide a consistent and unified method for text message archival.

LOCATE YOUR DATA

Decision makers must know where their data is located – a practice that is becoming more difficult in an increasingly mobile business environment. Corporate information is normally spread 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, particularly content that is stored on mobile devices. Decision makers need to be able to identify all relevant data on mobile devices – presentations, text messages, documents, spreadsheets, notes, photos, instant messages, emails, call logs and all other relevant data – and gain access to it when needed. 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 case, it is essential as an information governance best practice.

DON'T LIMIT USE OF MOBILE PLATFORMS BECAUSE OF THE COMPLIANCE CHALLENGES THEY PRESENT

Some decision makers may opt to limit the use of mobile devices because of the challenge of archiving data from them. Our advice is don't: mobile devices create tremendous value by enabling greater productivity, and so limiting their use is counterproductive.

IMPLEMENT TECHNOLOGY THAT WILL ALLOW ARCHIVING AND MONITORING OF CONTENT FROM MOBILE DEVICES

At a minimum, the appropriate technologies should be deployed that will enable all content on mobile devices to be copied to IT-managed systems in real time or near real time. Better yet, organizations should deploy a true archiving solution that will enable archiving directly from mobile devices. 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. A text message archiving solution should be deployed that is both scalable to meet current and future demand, and that can archive text messaging content from all relevant sources.

SUMMARY

Text messaging is an important channel of communication for business users in a number of contexts: communication between employees, between employees and business partners, between support organizations and customers, etc. However, while archiving of "traditional" content like corporate email has been a best practice for many years, the vast majority of organizations today do not archive their text messages. The result is that many of these organizations are not in compliance with various regulations regarding retention of business records, they face increased legal risk by not archiving content that might need to be produced during litigation, and they are not preserving other content that has business value. To remedy these problems, decision makers in both heavily and lightly regulated organizations should implement a text messaging archiving solution that will integrate with their existing archiving capabilities.

ABOUT TELEMESSAGE

TeleMessage is widely recognized as an innovative messaging leader providing enterprises and mobile operators with mobility solutions and next-generation wireless communication technologies. Founded in 1999, TeleMessage has been helping organizations of all sizes across industries, including healthcare, government, financial services, energy and network carriers globally to leverage the power of the mobile channel with our robust communications platform. TeleMessage's products include: Mobile Archiver – mobile communication archiving for regulatory compliance, litigation preparedness and eDiscovery; Secure Enterprise Messaging and Mass Messaging - messaging solutions successfully deployed and used by thousands of enterprises, trusted by dozens of telecom operators, reaching hundreds of millions of users powering billions of messages through customers' networks. TeleMessage equips your workforce with the most complete, secure and integrated mobile enterprise solutions.

TeleMessage

www.telemessage.com

@TeleMessage1

468 Great Road, Suite 2

Acton, MA 01720

+1 978 263 1015

17 Ha-Mefalsim Street

Petach-Tikva 4951447

P.O. Box 3668

Israel

+972 (3) 922 5252