

The Growing Challenges of Compliance in a Mobile World

An Osterman Research Executive Brief

Published December 2010

SPONSORED BY



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

Overview

USE OF MOBILE PLATFORMS IS INCREASING

Mobility in its greater context – namely, enabling employees to work from any location – is becoming more common as a means of increasing organizational flexibility, reducing operating expenses, reducing taxes and improving customer service. Mobile messaging is a key component of this trend by enabling properly equipped workers to send and receive email, SMS, and other types of mobile messages (e.g., BlackBerry Messenger [BBM] and other types of mobile instant messaging); to access the Web and Web 2.0 applications; and to use corporate applications and communicate in a variety of ways regardless of where they work.

The use of mobile platforms is increasing at a rapid pace. For example:

- Gartner forecasts that the sale of tablet PCs will increase from 19.5 million units in 2010 to 154.2 million in 2013¹.
- Morgan Stanley forecasts that the number of mobile Internet users will exceed desktop Internet users by the end of 2013².
- IDC estimates that worldwide smartphone shipments in the third quarter of 2010 totaled 340.5 million units, up 14.6% from 297.1 million units during the same period in 2009.
- An ABI Research report³ predicts that by 2013, one-quarter of mobile devices will be smartphones.
- A Pew Internet study found that as of September 2010 72% of US adults send and receive text messages, up from 65% a year earlier⁴.
- An Osterman Research survey found that one-third of employees in mid-sized and large organizations in North America will use an employer-supplied and employer-funded mobile device by 2011.

What this means is that mobile messaging will continue to grow at a strong pace throughout the next several years, driven primarily by the need to mobilize the workforce in an effort to reduce overall corporate costs, speed decision making and improve employee efficiency. While mobile capabilities will displace some traditional computing and communications, the primary effective will be additive as organizations layer mobile messaging capabilities in with the rest of the communications and computing infrastructure they already have in place.

¹ http://reviews.cnet.com/8301-31747_7-20019725-243.html

² *Internet Trends*, April 12, 2010, published by Morgan Stanley

³ <http://is.gd/gORa2>

⁴ <http://www.pewinternet.org/Reports/2010/Cell-Phones-and-American-Adults.aspx>

MANY USE A MOBILE PLATFORM AS THEIR PRIMARY DEVICE

Given the rapid increase in the number of mobile devices in use – and smartphones in particular – it is no surprise that mobile devices are becoming the primary device used by a growing number of users, replacing desktops and laptops as the platform of choice while traveling, while working from home, and sometimes even in the office. The growth in use of mobile devices is being driven in part by the increasing sophistication of the capabilities available on mobile platforms, as well as by improvements in processing horsepower in these devices. In turn, more capable mobile devices are enabling newer applications in a variety of industries, including insurance, financial services, energy, healthcare and other, often heavily regulated, industries.

Increasingly, mobile devices will replace the iconic desktop phone as the de facto communications tool for employees within the office. According to an Osterman Research survey of mid-sized and large organizations, nearly one-half (46%) of employees use a mobile device within the organization. Given this trend, by 2011 more than one-half of employees will use mobile devices at work.

Within large organizations, this trend is even more dominant. Mobile devices are already used by more than one-half of large organizations and that will grow to 58% by 2011. More than 40% of smaller organizations currently use mobile devices within the organization, a number that will grow to more than one-half by 2011.

With the mobile device becoming the dominant means of communications, organizations will need to improve the way they manage these devices. About one-quarter of organizations will seek to prevent employees from storing sensitive data on the mobile device, but most organizations will rely on mobile device management platforms over the next two years to help manage and secure that data. As part of this process, these platforms will likely be called upon to address compliance requirements for mobile devices much as has been done for desktop and laptops.

The predominance of mobile clients has implications for telephony vendors, as well. The move towards fixed mobile convergence (FMC) will continue to grow as organizations look to consolidate around a single communications device much as they consolidate around a single computing device – a PC or laptop. For telephony vendors, this suggests that they will need to continue to deliver effective mobile communication support.

Mobile Platforms Present Unique Challenges

IT OFTEN LACKS THE CONTROL THEY NORMALLY WOULD HAVE

There are a number of challenges that IT departments face when attempting to manage mobile devices, not least of which is the fact that IT typically can exercise less control over how these devices are used. For example:

- **Users are more autonomous**
Mobile users tend to be more autonomous because they are outside of the office and so IT cannot control how devices are used. Users will often connect to carrier-

provided networks to access the Web or email, they will connect to local Wi-Fi hotspots in coffee shops and hotels, and so forth. The result is that IT does not control their users' Web or email experience to nearly the same degree as when users are in an office environment.

- **Archiving is much more difficult**

Data is more difficult to archive because some of it is stored on the mobile devices themselves. A 2010 Osterman Research survey found that 2% of all corporate data is stored on users' smartphones. While this may not sound like a tremendous proportion of data, consider that an organization with just 10 terabytes of data under management will typically have 200 gigabytes of data on mobile devices.

- **Monitoring content is more difficult**

Monitoring content sent from and received by mobile devices is much more difficult than it is from a conventional desktop infrastructure. Because various types of communications must be closely monitored in financial services, energy, healthcare and other industries, users on mobile devices represent a significant liability simply because their content cannot be easily monitored. This means that legal and regulatory violations are easier to commit, which can lead to adverse legal judgments and regulatory sanctions.

- **Compliance is also difficult**

According to an Osterman Research survey, nearly two in five organizations finds managing policies for e-discovery or regulatory compliance to be difficult or very difficult, while 35% find managing other types of policies to be this difficult. Managing mobile policies for issues like e-discovery and regulatory compliance is slightly more difficult than managing other types of policies. Larger organizations, in particular, have a more difficult time with compliance and e-discovery policies. The survey found that nearly one-half of respondents indicated that managing such policies were either "difficult" or "very difficult".

- **The environment is more diverse**

The normal desktop infrastructure consists of mostly Windows machines and possibly some Macs and maybe a few Linux machines. The typical mobile environment, on the other hand, is much more diverse, typically consisting of BlackBerry devices, Android devices, iPhones, Windows Mobile devices, Symbian devices and other platforms. Further, new devices – with different versions of these operating systems – are introduced frequently into the network.

THE OBLIGATIONS TO MANAGE MOBILE ARE NO DIFFERENT

Despite the fact that the mobile computing environment is significantly more difficult to manage than a normal desktop infrastructure and presents a number of unique challenges, organizations have the same obligations to comply with legal and regulatory requirements when managing the mobile infrastructure. Specifically:

- **Content must be archived**

A variety of content must be archived in order to comply with legal and regulatory requirements. This includes posts to social media sites like Twitter and Facebook,

instant messages, text/SMS messages and voice communications, as well more traditional communications like email.

- **Mobile devices must be managed properly**

Because of the growing number of legal requirements to manage content and the significant number of regulatory requirements that exist, content sent from mobile devices must be managed properly. Add to this the requirement for any organization to comply with basic best practices for the use of these devices in the context of ensuring that offensive, sensitive or confidential content is not sent inappropriately.

What Should Your Next Step Be?

DON'T LIMIT USE OF MOBILE PLATFORMS BECAUSE OF COMPLIANCE

Mobile platforms are extraordinarily useful because they permit users to remain productive wherever they are, they allow significant cost reductions by changing existing processes, and they provide competitive advantages given that many organizations are not yet taking full advantage of mobile computing. This is particularly true in heavily regulated industries that have a large proportion of employees who are often away from their desks – such as insurance adjusters, energy traders, doctors and brokers – and that also have stringent compliance requirements that must be satisfied.

The key for decision makers then is not to shy away from the use of mobile devices because of the strict compliance requirements that must be met. Instead, mobile devices should be deployed wherever they can offer benefits – in conjunction with the appropriate tools to manage them.

IMPLEMENT TECHNOLOGY THAT WILL ALLOW ARCHIVING AND MONITORING OF CONTENT

It is absolutely essential that any organization, but particularly those in heavily regulated industries, deploy technology that will allow the management and archiving of content sent from mobile devices. Specifically, this technology should:

- Permit corporate policies focused on mobile content to be managed easily.
- Archive all relevant content, including emails and text/SMS messages. This capability should also include robust search and retrieval capabilities to support early case assessment, e-discovery and data mining applications.
- Flag messages for supervisory review, a critical compliance requirement in the financial services industry to monitor broker-dealers for misleading statements; and in the energy industry to prevent communication across ethical walls, to name but two of the many applications for review.
- Provide detailed reporting for purposes of monitoring enforcement with corporate policies.

- Monitor all content. Ideally, this will include real-time monitoring for potential policy violations and other content.
- Encrypt content to comply with specific regulatory requirements, such as the Health Insurance Portability and Accountability Act and to prevent data breaches of various types.
- Support all of the mobile platforms that are in use in an organization.

About TextGuard

TextGuard's flagship TextGuard™ service provides a complete solution for the monitoring, capture and archiving of SMS messages, Blackberry Messenger and Blackberry PIN-to-PIN messages sent from company mobile devices. All text messages are identified, collected, and archived in a format that is easily accessible, allowing companies to establish meaningful internal compliance policies regarding mobile devices and to meet compliance mandates from all relevant regulatory bodies. TextGuard presently supports Blackberry®, Windows Mobile® and Android® operating systems.

TextGuard™ features include:

- Comprehensive capture & archiving of SMS, PIN to PIN and BBM messages
- Encryption
- Search and retrieval
- Policy management
- Intelligent Storage Manager
- Easy to use Roles-based Web user interface
- Reporting & Statistics
- Offered as a SaaS solution

TextGuard has robust monitoring, archiving and search capabilities. First and foremost, enterprises can set their own automatic flagging of messages for compliance and supervisory review based upon message content, recipients, and/or senders. The solution also provides other web-based configurable policy enforcement workflow tools for reviewing and annotating conversations. Our advanced search capabilities allows for quick and efficient retrieval of messages.

With the TextGuard mobile compliance administration console, managers of enterprise IT departments have immediate web-based administrative console for the end users of mobile devices which provides a single point of reporting for each mobile device. This console provides real-time usage reports and data visualization charts. In addition, TextGuard supports ad hoc reporting delivered on demand, or scheduled to email, ftp, or file shares.

TextGuard is provided on a software as-a-service (SaaS) basis, meaning that mission-critical data is hosted in TextGuard's state-of-the-art data centers thus allowing enterprises to avoid large capital expenditures for infrastructure build-out. The

outsourced model offers relief from a replacement schedule, staffing expenditures (and man-hours) and additional large capital outlay, and provides peace of mind in knowing that, in the event of a disaster, mission-critical data will be available. Internal IT personnel can refocus on core competencies rather than wasting time and energy on archiving-related issues like storage, software, database management and server maintenance. TextGuard support is available 24x7, 365 days a year, from the same architects of our proprietary software and services.

TextGuard offers two deployment options:

- The standard TextGuard Client Edition service begins with the download of a lightweight, client software application to the mobile device. Once the software is installed, it automatically registers the device on the TextGuard engine server. When a message is then sent from (or received by) from the device, the client makes a copy of the message and delivers such message to the TextGuard message archiver where it is encrypted and stored. The software supports all existing text message types and generates audit log files automatically.
- Enterprises that primarily use the BlackBerry device for their employee's mobile communications and have or control a BlackBerry enterprise server can take advantage of the TextGuard BlackBerry Enterprise Server edition. In this solution, the TextGuard application processes logs that are obtained directly from the BES with an installed script. All messages are then captured from that point and sent to the TextGuard message archiver for archiving. The TextGuard BES Edition allows for easier provisioning of users since no software has to be installed on the device. In addition, the BES Edition is more "tamper-resistant" since only IT professionals have access to the BES.

For more information, TextGuard can be contacted at:

TextGuard, Inc.
1375 Broadway
Suite 100
New York, NY 10018

646.536.5559
information@textguard.com
www.textguard.com

© 2010 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.