

WHITE PAPER

**Enforcing Regulatory Compliance
in Smartphone-Enabled Workplaces**

CONTENTS

Executive Summary	1
The Impact of Smartphones on Regulatory Compliance	2
Introduction	2
Communications and Data Protection Regulations.....	2
Complications Arising from Smartphone Proliferation	3
End-Point Security	4
EPS and Smartphones	4
Communications Review & Control	4
Internal Communications.....	4
External Communications	5
Communications Review Mechanisms	5
Communications Archiving	5
METAmessage Advanced Compliance Tool	6
METAmessage Features.....	6
METAmessage ACT End-Point Security	6
The METAmessage Advantage.....	7
METAmessage ACT – Rules-Based Control	8

Executive Summary

Many industries are subject to regulations, such as FINRA in the financial services sector, SOX in public companies and HIPAA in healthcare, that include provisions to provide data protection, communications control and information flow management. As new technologies are adopted, organizations need to review and adapt their compliance systems to adequately respond to new threats and risks. No technical advance had posed as significant a challenge to this process as the introduction of wireless communications devices, smartphones in particular.

Whether protecting against inadvertent dissemination of sensitive data or deliberate attempts to violate information security, regulations require that organizations prepare comprehensive systems and procedures to minimize risk. Most organizations have introduced software solutions to assist IT departments in mitigating risk factors. However, as smartphones are becoming widely used they introduce a new threat level because of their highly mobile nature, the flexibility of communication methods available and the resulting difficulty of controlling information flows.

As a result, IT departments must adjust their compliance mechanisms to account for the new threats to which this has given rise. In addition to voice calls, most smartphones are able to communicate via multiple messaging systems, such as e-mail, SMS and BlackBerry® PIN. Often, existing solutions do not provide effective regulatory compliance for smartphones, sometimes necessitating organizations to prohibit their use.

This document outlines the main issues IT departments need to consider when addressing regulatory compliance for smartphones and how Onset Technology's METAMessage Advanced Compliance Tool resolves these issues.

Smartphones introduce a new threat level because of their highly mobile nature, the flexibility of communication methods available and the resulting difficulty of controlling information flows.

Organizations need to provide data protection, communications control and information flow management.

The Impact of Smartphones on Regulatory Compliance

Introduction

A host of industries are subject to regulations that have been implemented to protect stakeholder and consumer interests. These regulations, such as FINRA (NASD, NYSE) and SEC in the financial services sector, SOX in all public companies and HIPAA in healthcare, cover a wide variety of functional areas relevant to the specific industry and types of organizations.

The need to provide data protection, communications control and information flow management are among the central themes of such regulations. As new technologies are adopted organizations need to review and adapt their compliance systems to adequately respond to new threats and risks. The introduction of wireless communications devices, smartphones in particular, poses perhaps the most significant challenge to this process.

Communications and Data Protection Regulations

Regulatory bodies have rightly identified communications and data protection as critical areas requiring regulatory oversight. Whether protecting against inadvertent dissemination of sensitive data or deliberate attempts to violate information security, regulations task organizations with preparing comprehensive systems and procedures to minimize the risk to stakeholders (including organizations, shareholders and employees) and consumers alike. Most organizations have introduced complex systems and intricate procedures to meet this challenge and a variety of software solutions are available to assist IT departments in mitigating risk factors.

Risks can be broadly divided into the following groupings:

- **Malicious External Attacks** – Attempts by parties external to the organization to gain access to sensitive information. Means may include hacking, malware, data snooping and more.
- **Intentional Internal Information Breaches** – Attempts by members of the organization to gain unauthorized access to sensitive information and/or transmit such information to external parties.
- **Unauthorized Internal Contact** – Attempts by members of the organization to communicate with members of departments or groups in an attempt to circumvent regulations. For example, attempts by individuals to exert inappropriate influence on the contents of research reports.
- **Accidental Information Breaches** – The unintentional transmission or loss of sensitive data, for example by accidentally sending e-mails to the wrong recipient.

Note: Research shows that the majority of the information breaches are non-malicious, unintentional mistakes, such as an individual forwarding a message to an external contact without noticing that it contains confidential information.

Complications Arising from Smartphone Proliferation

Smartphones introduce a new threat level because of their highly mobile nature, the flexibility of communication methods available and the resulting difficulty of controlling information flows. As smartphones become increasingly prevalent in regulated industries, especially within financial services, IT departments must adjust their compliance mechanisms to account for the new threats to which this has given rise. In addition to voice calls, most smartphones are able to communicate via multiple messaging systems such as e-mail (corporate and/or personal), SMS, PIN (BlackBerry® only), MMS and Instant Messaging.

Corporate e-mail may already be covered by existing enterprise compliance solutions, although extending those solutions to cover smartphone-based e-mail may not be possible. Even if mobile e-mail is already covered by existing enterprise solutions, these solutions do not yet effectively exert control over information being transmitted using other methods. Also, given that smartphones may change ownership within an organization, it is necessary to have a mechanism to ensure that people don't inadvertently send sensitive information to the wrong recipients.

As a result of these issues, regulations often compel the organization to prohibit (and block) the use of devices over which they lack control, or, preferably, employ new technological solutions to enforce regulatory compliance on these devices*.

IT departments must adjust their compliance mechanisms to account for the new threats.

* For example, FINRA Regulatory Notice 07-59, Supervision of Electronic Communications, notes that FINRA members are directed to "prohibit employees from the use of electronic communications unless such communications are subject to supervisory and review procedures developed by the member" and further, "to the extent members prohibit certain types of communication media, consideration should be given to taking technological steps to block or otherwise regulate their external and internal use".

Smartphones require a unique set of EPS features to tackle the specific threats associated with their use.

End-Point Security

End-Point Security (EPS) is broadly defined as a technology security doctrine based on the idea that the first line of defense is the device itself and technological solutions should be implemented directly on the device to counter security risks. This is then used in conjunction with centralized security technologies, such as firewalls, e-mail rules and spam/virus filters, to minimize risks.

While EPS has traditionally applied to end points within an organization's computer networks, such as PC's, servers and the like, technological advances have necessitated expanding the definition beyond the network to any electronic device which may contain or access the organization's assets but which may not always be located within the organization's premises. That includes laptop computers, POS devices, portable storage devices (hard disks, USB thumb drives, etc.), and smartphones.

EPS and Smartphones

These devices are outside the enterprise network and are often, if not primarily, used for work-related communications and may access resources and information contained within the organization. As a result, smartphones require a unique set of EPS features to tackle the specific threats associated with their use.

IDC has identified two types of EPS solutions that are relevant to smartphones: solutions that control the ability of the device user to engage in unauthorized communications, what IDC terms Behavior Blocking; and, Information Protection and Control, which encompass solutions that discover, protect and control sensitive information*. It is important that any compliance solution address both these types of EPS approaches in order to effectively satisfy the relevant regulatory requirements on smartphones.

Communications Review and Control

Enforcing compliance on smartphones requires solutions that address the specific risks outlined previously: facilitating review and supervision of communications; controlling message flow between recipients; controlling message content; handling different message media; and, keeping a record or archive of all messages. Message flows can be divided into two categories – internal, meaning all intra-organizational communications, and external, meaning to parties outside the organization.

Internal Communications

In some sectors, such as financial services, internal communications are heavily regulated. The concept of separating departments or groups of users is commonly referred to as a "Chinese Wall." A Chinese Wall is an information barrier implemented within an organization to separate people who are prohibited from being in contact, generally due to issues of conflict of interest. This can be, for

* IDC Executive Brief, "The Rising Concerns Over Endpoint Security", March 2008
http://www.techworld.com/cmsdata/whitepapers/5784/IDC_Endpoint_Security.pdf

example, to isolate people who make investment decisions from people who are privy to undisclosed material information which may influence those decisions.

External Communications

When messages are sent outside the organization, risks are multiplied. As with internal messages, communication may be to unauthorized recipients, and should therefore be restricted or controlled. In addition, messages to customers, or consumers in general, are often subject to regulations requiring that a record of each message be retained for a specific period of time.

Communications-Review Mechanisms

Often, regulations will state that organizations must provide a system for communications to be reviewed by a designated reviewer or supervisor. This message review necessitates that copies of messages be sent to the reviewer to ensure that they conform to regulations.

There are two commonly adopted methods for review:

- **Lexicon-Based Review** – The organization employs a software solution that scans all messages for a list of sensitive words or phrases and flags messages with questionable contents for review. The organization can make changes to the lexicon as necessary.
- **Random Review** – No logic or ‘intelligence’ is associated with this process, rather a pre-determined percentage of messages are automatically selected and sent for review.

Both methods are commonly used but the nature of the random review will render it somewhat more risky versus a well-implemented lexicon-based system.

Communications Archiving

As mentioned, most organizations are required to retain a record of some or all communications, especially external. For example, investment advisors are required to retain copies of all advisory messages. Since smartphones now enable a variety of communication methods, archiving solutions must provide adequate record retention for all message-types, including SMS and BlackBerry PIN.

Most organizations already have existing solutions in place for retaining communications which include complex electronic discovery (e-discovery) functionality for search and review. It is therefore important for any smartphone compliance solution to integrate with such existing solutions in order to take advantage of the existing solutions and avoid having multiple repositories and multiple discovery interfaces.

Archiving solutions must provide adequate record retention for all message types including SMS and BlackBerry PIN.

METAmessagE Advanced Compliance Tool

Onset Technology has developed the METAmessagE Advanced Compliance Tool (ACT) in order to allow organizations to easily extend regulatory compliance to BlackBerry® smartphones. METAmessagE ACT is a client-server solution built on the proven 5th-generation METAmessagE platform, delivering a comprehensive suite of features to exert maximum supervision and control.

METAmessagE Features

METAmessagE ACT offers the following rule-based features for smartphones:

- **Sender/Recipient Control** – to avoid unauthorized communications between users (Chinese Wall), ACT maintains white/blacklists of addresses on user smartphones so administrators can control who can communicate with whom.
- **Content Control** – administrators can define keyword lexicons and message rules to control messages containing sensitive information.
- **Message Attribute Control** – administrators can define different rules for different message types. For example, they can block the forwarding of messages marked as confidential to recipients outside of corporate boundaries.
- **Flexible Rules-Based Actions** – when defining ACT Rules, administrators have full control over what action should be taken. Options include: deliver to recipient; log only; copy suspected message to supervisor; redirect message for supervisor’s approval; or, block the message. If desired, ACT can also notify the user of the policy violation.
- **Enhanced Message Archiving** – ACT archives inbound and outbound SMS and PIN messages and adds sender/recipient information and other data before archiving for enhanced e-discovery and search capabilities. ACT integrates directly with existing enterprise archiving solutions to minimize the impact on established e-discovery procedures.
- **PIN Address Management** – automatic maintenance of BlackBerry PIN addresses to ensure delivery to correct users, even as BlackBerry smartphones change.

METAmessagE ACT End-Point Security

Because the METAmessagE ACT client application is installed on the smartphone, it is a true End-Point Security solution. This means METAmessagE processes messages locally on the device and handles outbound messages as well as inbound messages received to the device.

The client application applies corporate policy to messages (currently e-mail, SMS and PIN; soon also MMS and IM), enforcing message control, ensuring that messages don’t contain sensitive words or phrases and checking for unauthorized

Because the METAmessagE ACT client application is installed on the smartphone, it is a true End-Point Security solution.

recipients. Any rule violation can be reported to an administrator and messages can be copied to a reviewer for additional supervisory action.

The METAMessage server is used for policy definition and management. Administrators use the server to create and wirelessly transmit rules, word/phrase lexicons and white/blacklisted addresses to the ACT client. The server also monitors the BlackBerry Enterprise Server (BES) for BlackBerry PIN address changes and automatically updates those changes on all devices.

For archiving, the METAMessage ACT client sends copies of messages to the METAMessage server which can be integrated with the organization's existing archiving solution. The archiving process takes place in the background without any intervention by the user.

The METAMessage Advantage

Onset Technology is an industry-leading developer of solutions for smartphones and Onset is one of Research In Motion's top independent software vendors. With extensive experience developing applications for BlackBerry, being the first company to develop spell-checking and attachment viewing functionality, Onset has unparalleled knowledge of the BlackBerry smartphone operating system and server environment.

METAMessage enables organizations to take full advantage of the power of smartphones while mitigating risks associated with information and asset security. With regular updates from Onset that implement the latest regulatory requirements, organizations can ensure that the solution is always up-to-date.

Onset Technology has a roadmap to enhance the product for Windows Mobile and other smartphones when they develop enterprise solutions.

METAMessage enables organizations to take full advantage of the power of smartphones while mitigating risks associated with information and asset security.

METAmessage ACT – Rules-Based Control

Message Control Types

Recipients Management

- White/blacklists
- Allowed/blocked domains
- Allowed/blocked external SMS
- Allowed/blocked external PIN

Lexicon-based Rules

- Inappropriate words
- Sexual harassment protection
- Intellectual property, trade secrets
- Pattern: credit card numbers, Social Security number, routing numbers
- Severity thresholds – how many violations occur before rule is triggered

Message Attributes Rules

- Forward of confidential message
- Forward outside of corporate boundaries
- Forward encrypted message

Message Control Behavior

Inform End User

- Pop-up message to notify user and allow to correct the violation
- With or without logging

Ask for Confirmation

- Pop-up message to confirm whether to override the policy.
- If confirmed, deliver to destination with copy to supervisor

Copy to Supervisor

- With or without end-user notification

Redirect Message

- Redirect to supervisor
- With or without end-user notification
- With or without copy to supervisor

Block Message

- With or without message deletion
- With or without end user notification
- With or without copy to supervisor

About Onset Technology

Founded in 1997, Onset Technology is the creator of METAMessage®, a suite of unique software solutions that enhance the functionality of smartphone deployments. METAMessage® offers solutions for financial institutions, government agencies, healthcare, law firms and a broad range of other enterprises. Since its introduction, METAMessage has been widely adopted by Fortune 1000 companies and government agencies and has been sold to over 1,400 customers with more than 150,000 users. Onset has developed extensive experience and methodologies for working with large multinational enterprises, system integrators and tier-1 carriers worldwide.

For more detailed product information,
visit our web site at www.onsettechnology.com

or contact:

US Sales: salesinfo@onsettechnology.com, or
International Sales: int_sales@onsettechnology.com.

US Headquarters

460 Totten Pond Road
Waltham, MA 02451
+1 (781) 916-0040

US Regional Sales Offices

101 Constitution Ave. NW
Washington, DC 20001
+1 (202) 742-4645

323 Broadway #340
New York, NY 10013

International Headquarters

2 Maskit Street
Herzliya Pituach 46733,
Israel
+972 9 956 1615

+1 (877) 847-8329

343 Soquel Dr. #335
Santa Cruz, CA 95062
+1 (877) 847-8329

Marketing Contact:

Zack Silbinger, zack.silbinger@onsettechnology.com

©2008 Onset Technology Inc. All rights reserved. METAMessage® and METAMessage for Wireless are trademarks of Onset Technology, Inc. Other product or service names mentioned herein are the trademarks of their respective owners.

This document is provided for informational purposes only and Onset makes no warranties, either express or implied, in this document. Information in this document is subject to change without notice. The entire risk of the use or the results of the use of this document remains with the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Onset Technology.

Onset may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Onset, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.