GUIDE

5 Steps to Compliance in an Evolving Mobile Landscape

For Financial Services

smarsh®

For so many of us, the mobile devices we carry in our pockets are at the epicenter of how we work. Calendars, messages and documents are easily accessed before we leave our homes for the day. Once handled exclusively over desk phone and email, many business interactions are now done entirely on mobile devices.

Text messaging has changed how we communicate, inside and outside of business, for good reason. Texts have higher and faster response rates than phone calls and emails, which increase productivity – a premium value in today's always-on society.

16,000,000+ texts are sent every minute

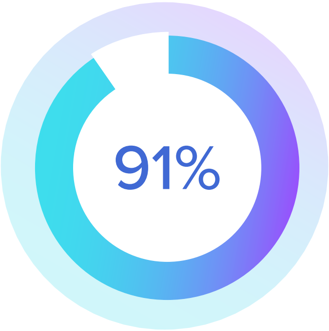
100 billion messages are sent via WhatsApp every day

90 seconds | 90 minutes

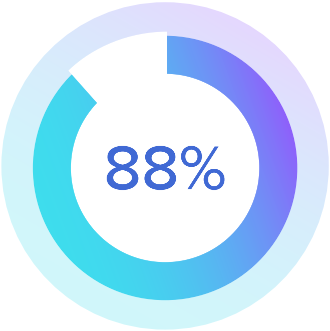
The average person responds to a text message in 90 seconds, compared to 90 minutes for an email

98% of all text messages are opened, while only 22% of emails are opened

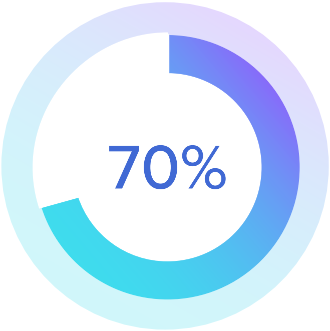
Of course, our mobile habits at work also apply to our everyday use. Checking the weather, scrolling through the latest news, setting an alarm – no matter what you do, your phone or mobile device is nearby. The smartphone has gone from luxury to appendage.



of mobile users keep their smart phone within reach



of employees use mobile phones for work while on personal time



of employees' office phones will be replaced by mobile devices

The increase in mobile connectivity has enabled people to communicate in many interactive ways – calls, text messages, WhatsApp, social media, collaboration apps like MS Teams and Zoom and various other emerging apps. However, what this means for organizational security and regulatory compliance may seem overwhelming. It's more complicated today than it ever has been to archive and monitor employee communications, which leaves regulated companies vulnerable to risk with a high surface area to monitor.

In the news

Regulatory Roundup: Record-Breaking Penalties Provide a Glimpse into 2023

The SEC enforcement results, released November 15, 2022, were record-breaking due to the number of enforcements issued and the size of the fines assessed. The agency announced the following numbers:

- 6.5% increase in the total number of enforcement actions
- 20% increase in actions against broker-dealers in FY 2022
- 9% increase in investment adviser and investment company cases

The SEC assessed more than $4.194 billion in penalties in the 2022 fiscal year, a 200% increase from the prior year.

There are valuable lessons to be learned from these high-profile cases. They span industries and roles, but these incidents are especially pertinent for regulated firms such as financial institutions and organizations requiring electronic records management.

When the collection and supervision of employee communications is mandated, wrapping your policies and procedures around a massive collection of mobile data can be a heavy-duty operation. But a well-thought-out plan, combined with a comprehensive solution for capturing, archiving, and monitoring mobile data, is the key to staying ahead of risk – and out of the headlines.

Unique mobility risks: knowledge gaps

As quickly as we've adapted to communicating on mobile devices in our personal and professional lives, many businesses have fallen behind in adjusting recordkeeping processes to follow suit. This is risky behavior for regulated organizations. In many cases, gaps in knowledge prevent these organizations from establishing a modern mobility strategy and enabling a thriving workforce.

Policy Gaps

Companies should outline explicit rules about how employees are permitted to use their mobile devices and which applications are allowed or prohibited for business use. The rules need to be realistically feasible and accommodating to a cross-generational workforce.

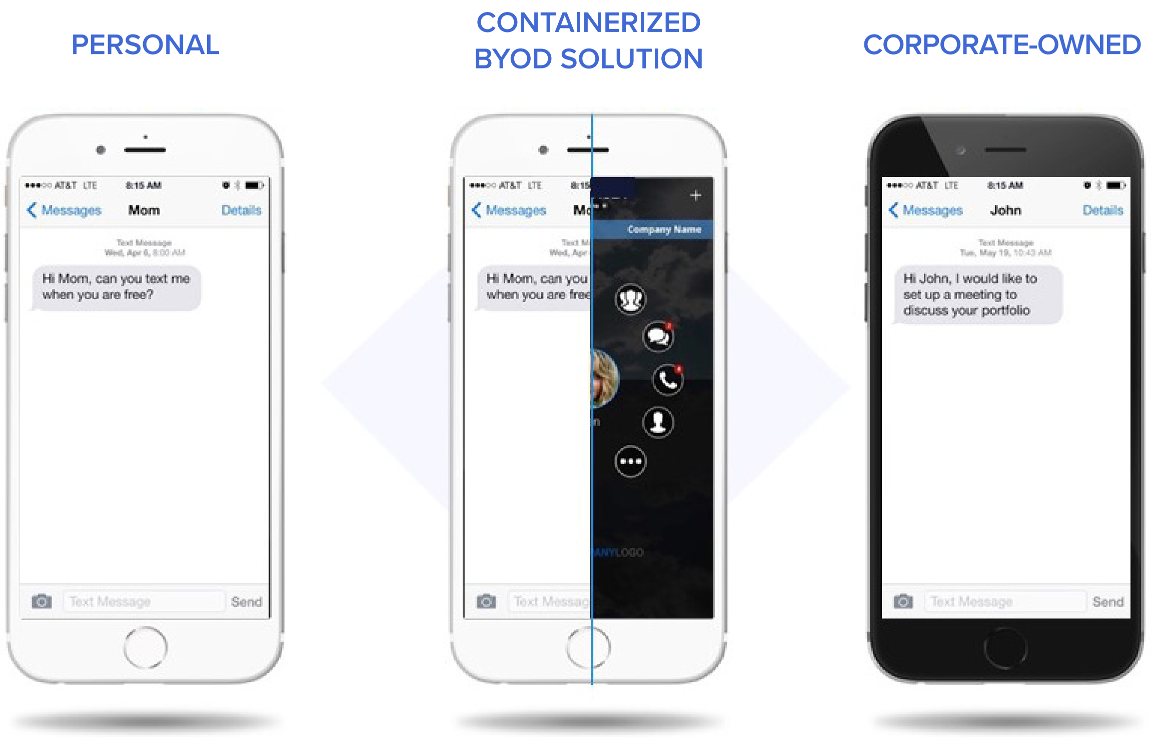
The adoption of a mobile strategy among regulated firms and recordkeeping practices varies widely. When asked, some companies have said they:

- Do not have a documented mobile policy
- Prohibit the use of mobile devices entirely
- Do not allow employees to send "business-related" messages to clients
- Will collect text messages from mobile carriers if necessary
- Rely upon employees to preserve their communications

Over **40 percent of millennials** communicate with their financial adviser through video chat. Moreover, nearly **40 percent of millennials** and **23 percent of Gen X** investors text with their financial adviser.

Company Owned/Personally Enabled corporate-owned devices devices are trending again because they are easier to monitor and secure. The alternative is to implement Bring Your Own Device (BYOD) policies. In the case of BYOD, employees use their own phones and containerization or Electronic Device Management (EDM) solutions are installed over the top to capture business communications.

Companies accommodating modern channels make their organizations attractive to workers and customers alike. Technology solutions for collecting and archiving communications for corporate-owned devices or BYOD help make this possible in regulated industries.



Hi Mom, can you text me when you are free?

Hi John, I would like to set up a meeting to discuss your portfolio

Risk gaps

Regulated firms and sophisticated IT groups understand the need for a proper communications archiving solution, even if their policies aren't fully developed. But there are additional reasons to be proactive about the risk of mobile beyond compliance obligations.

If a corporation issues phones to its workforce, investigations by the legal department, human resources or regulators could mean confiscating phones and scanning through every relevant communication on every single device. Without a BYOD capture solution, relying on the user to preserve all their texts or IMs is certainly a leap of faith.

Intellectual property or sensitive information may be communicated or exchanged on mobile devices. Firms without airtight governance processes face risk here too.

Potential areas of risk:

- compliance and regulatory obligations
- e-discovery for legal investigations
- information security and data privacy
- human resources investigations

Technology gaps

Technology to support capturing, archiving and supervising all interactive mobile communications is the cornerstone of a reliant, risk-averse mobile program. Traditional document and email collection solutions aren't suited to the mobile model of communication, which includes interactive and encrypted messaging applications.

It can be time consuming and expensive to figure out how to accommodate modern communications with an old tool. Some important considerations:

- Can you collect mobile communications data with your existing technology?
- Is it capturing all the interactive, contextual data?
- If you're capturing the data, is it stored in an archive that allows you to easily search for and review what you need to find?
- Have you considered applications that can be applied to employee devices in a BYOD situation?

Your technology solution needs to address the full spectrum of your company's mobile needs.

5 steps to stay ahead of mobility

We've laid out five essential steps to help manage these knowledge gaps and work toward a seamless, scalable, forward-thinking mobile communication solution.

1 Start with good governance

Mobility considerations are just one part of a comprehensive corporate governance program. Strong governance means involving all relevant stakeholders, and depending on your organization, this may span several departments: legal, compliance, IT, HR, sales, etc.

As a group, discuss the best course of action for your business regarding communication among employees, clients and partners. Address the common policy, risk and technology gaps and how they apply to your business.

Each stakeholder should be involved in the entire process of technology selection so their relative departmental needs are represented. As you make these evaluations, remember that where there's risk, there is also value. Communications data can provide a wealth of insight for competitive organizations, and a solution that natively captures and archives the full spectrum of mobile data supports those efforts.

2 Execute a mobility-first strategy

Mobile devices aren't going anywhere, so your data retention and preservation strategies must evolve.

Regarding your policies, risks and technology infrastructure, enabling mobility should be front and center. If those gaps are filled, potential risks should decrease, and employees should be enabled to focus on bottom-line company goals. Here are some steps for outlining a mobile-first strategy:

- Within your governance program, establish a mobility-focused task force
- Assess your mobile environment and determine where it helps or hinders your business goals
- Set up employee focus groups to elicit information about how they are using mobile devices for their jobs and use that information to refresh your mobile policy
- Socialize the plan with executives and client-facing leadership to get final buy-in
- Circulate documentation and train all employees; account for on- and offboarding
- Update policies as new applications and functionalities are deployed

3 Understand mobile collection and preservation alternatives

Many organizations struggle with collecting and preserving mobile content by using expensive services and archaic methods like scraping screens from individual phones. They choose these laborious practices even as they recognize that the extracted data is likely incomplete and out of context.

And preserving communications data when employees leave is another issue. How do you collect data from a former employee's phone? What about password management on a corporate-issued phone when passed from one person to another?

Migrating to a comprehensive solution for collecting and preserving high volumes and varieties of communications data streamlines the process for you. It doesn't have to be an expensive, time-consuming effort.

4 Adjust your inspection protocols

Remember that you can be proactive about collecting and monitoring employee communications – it doesn't have to be after the fact. Take real-world examples of incidents that could have been avoided had there been inspection protocols for supervision in place on the front end. The mobility task force should take these proactive steps while you're adjusting your mobile program:

- Examine the native capabilities of each communications source you're allowing. Is there API access? Is there metadata or event data that needs to be included?
- Tune supervisory policies to cut down on white noise and focus on monitoring high-risk terms and phrases.
- Leverage AI/surveillance to manage the sheer volume of mobile data and understand multiple, heterogeneous networks.
- Develop an internal playbook for offboarding employees that accounts for device transfer processes like password/key management.

Whether the need is an internal audit or investigation, legal discovery or compliance, your procedures for fulfilling those needs should be thought through and integrated from start to finish.

5 Train, train and retrain

We say this often because it bears repeating but training employees on mobile usage policies early and often is critical to a successful, low-risk communications environment.

Ensure training is explicit and includes both acceptable and prohibited uses for mobile communication by department and job role. When you give context to your use policies with a "why," staff will be more likely to follow the rules. Stay engaged with employees as channels evolve, and reassess your policies as needed.

Utilize the corporate resources that are available to you to standardize training. Automate policy enforcement with existing infrastructure and incorporate it into onboarding processes wherever possible. If your company has a corporate training program, work with that team to implement a mobile training course.

Smarsh helps you manage mobile

The Smarsh Capture Mobile Suite offers solutions that meet all mobile compliance needs, whether voice or message capture on corporate-owned devices, personal devices, consumer applications, or collaboration platforms.

Our suite features expanded telecom carrier and support of essential consumer apps to deliver unmatched communications capture. Capture Mobile empowers organizations to fulfill regulatory compliance requirements enforced by the SEC, FINRA, Dodd-Frank, MiFID, FCA and IIROC.

This single solution enables organizations to capture mobile communications in their native format while collecting broader context for retention and supervision purposes. Smarsh has enhanced its suite to provide improved functionality to organizations that use end-to-end encrypted mobile communications apps, including WhatsApp, WeChat, Signal, Telegram and other popular instant messaging apps.

While regulations continue to evolve and grow more complex, Capture Mobile reduces the complexity of solving mobile compliance issues while making it easier for firms to conduct their business without the fear of fines.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions.
You must consult your legal team regarding your compliance with applicable laws and regulations.

Guide - 05/23

☎ 1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh