INDUSTRY BRIEF

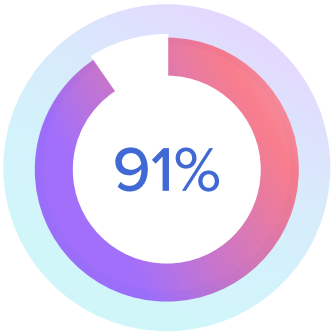
Guide to Mobile Communications Capture

smarsh®

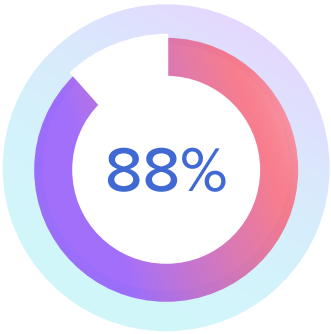
Is your compliance strategy keeping up with your firm's actual use of mobile?

Evolving generations have shifted the collective mindset toward immediacy when it comes to everyday interactions. Millennial and Gen-Z workers are choosing to text or chat rather than send an email, which has impacted overall business communications.

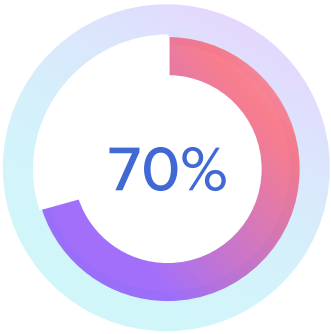
For instance, research shows that text SMS open rates are as high as 98%, compared to just 20% of all emails.[1] On average, it takes 90 seconds for someone to respond to a text and 90 minutes to respond to an email.[2]



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

Mobile devices have transformed our society. They have brought communications to the next level by enabling rapid responses around the clock. People have grown so accustomed to this level of communication that the expectation is ever present, particularly in their business affairs. Customers prefer text and the functionality that mobile apps offer, employees tend to oblige.

With mobile devices being integral to the workplace, regulated organizations need to ensure their mobile strategy has a modern approach to compliance. They must have the ability to enforce policies and meet regulatory requirements governing the capture of digital communications.

[1] "Tap Into The Marketing Power of SMS"

[2] "Email Marketing VS SMS Marketing the Stats"

The benefits of enabling mobile communications

Improved collaboration
Mobile communication enables the firm's workforce to respond more quickly, both internally and externally.

Increased flexibility
Multi-device applications like Microsoft Teams and Zoom empower employees to start a conversation on a mobile device and finish it on a computer, and vice-versa. This increases availability, productivity and responsiveness.

Enhanced security
Mobile applications like WhatsApp and WeChat support end-to-end encryption protocols, providing a secure channel for confidential decision-making.

Preferred channel
Employees choose mobile, flexible communication channels over email. Mobile apps are often preferred to maximize real-time critical and confidential financial decision-making.

Strengthened relationships
Customers want to start conversations easily and receive instant support. Faster resolutions and responses to customer inquiries lead to higher customer satisfaction, loyalty and revenue growth.

The unique challenges of capturing mobile content

Adopting mobile devices under any ownership model means firms must have a way to set and change communications policies. Compliance departments need a solution that allows them to correlate and supervise voice, text and chat activities for enforcement, traceability and e-discovery.

Even if mobile devices aren't initially involved in discovery, they often hold information that becomes relevant to the discovery process. This could be voice, text messages or more intensive content delivered through mobile apps. In many cases, it's a combination of two or more of these communication channels. The challenge is not only in capturing these communications but being able to preserve the communications in full context.

Mobile apps present a more complex problem. Without a proactive capture solution in place, businesses must go through the arduous task of collecting mobile devices to harvest the data. These reactive approaches — including the use of forensic tools and collecting content directly from carriers — are not quick, easy or without risk.

It's possible that data captured this way is incomplete or corrupted. Additionally, extra attention is required to ensure that distinctions between business-related and personal communications are clear. This is important so that firms take the appropriate steps to ensure compliance with the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and other similar privacy regulations.

Once mobile-generated data is collected, the issue of how to search, review and produce it must be resolved. It's challenging for businesses that don't have existing processes designed to review and produce mobile content to meet investigative requests. It can be time-consuming and expensive to reactively devise methods for understanding lengthy asynchronous chat discussions. Emojis and other unique features also lengthen and complicate the review process.

Mobile technology risks in regulated industries

Mobile devices have become common and crucial tools in the financial services industry. But their benefits have also created compliance risks when all forms of communication need to be captured and retained for regulatory purposes.

With historically large fines and sweep exams spreading through the industry, firms must address these challenges and implement effective policies and procedures around mobile use. Following headline-making enforcement actions, financial institutions are shifting to corporate-owned device only policies and also prohibiting specific channels like WhatsApp and Telegram.

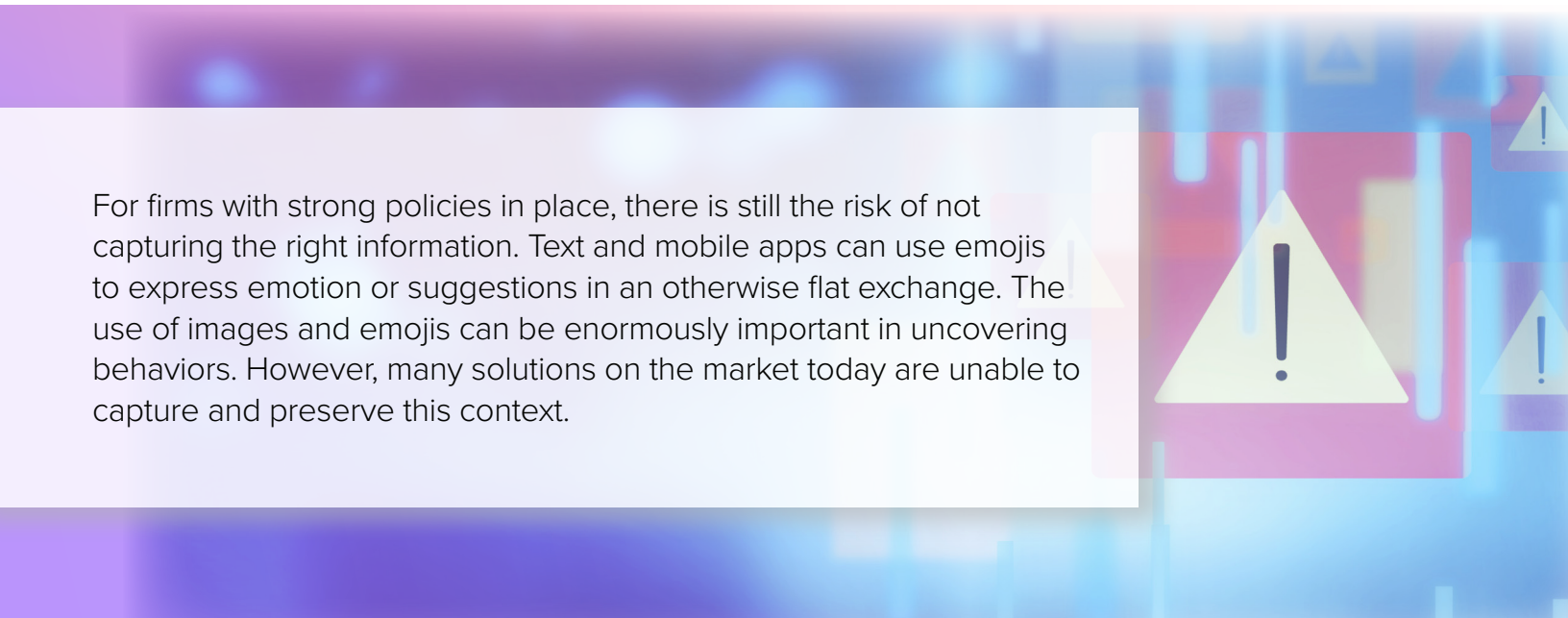
Even if firm leaders believe that the risks outweigh the benefits, prohibition of mobile apps or restricting mobile use to just voice and SMS text isn't enough:

1. There's a high likelihood that employees will either disregard or be unaware of them based on communication trends
2. Policies are either poorly defined or not actively monitored for compliance

In the most tightly controlled model, corporate-owned devices make enforcing policies easier. In this scenario, policies can more easily be enforced, but the firm will still need to capture the content of the communications. In the more flexible bring-your-own-device (BYOD) model, where employees use their personal devices for work, both policy enforcement and content capture are a concern.

But do businesses have to use two different technology solutions to address these compliance concerns? Fortunately, the answer is no. There are comprehensive solutions on the market today that can both capture electronic communications from mobile devices and allow businesses to establish and manage policies.

For firms with strong policies in place, there is still the risk of not capturing the right information. Text and mobile apps can use emojis to express emotion or suggestions in an otherwise flat exchange. The use of images and emojis can be enormously important in uncovering behaviors. However, many solutions on the market today are unable to capture and preserve this context.



Reducing mobile technology risks

5 steps to mitigating mobile risks

There are five critical steps businesses can take to mitigate the risks posed by mobile devices:

1

Actively develop mobile device governance

All stakeholders and employees must review existing mobile device or communication policies. Having this discussion can reveal if policies that protect the business are empowering employees or hindering their productivity. As part of governance, establish a mobility task force that:

- Assesses the existing mobile environment
- Refreshes policies per user group
- Updates policies as new apps and functionalities are deployed
- Examines the latest trends and benchmarks

2

Actively develop mobile device governance

Capturing mobile-based content, including its unique metadata, emojis and GIFs, enables firms to adhere to regulatory guidance on digital communications more effectively.

3

Capture content the right way

It's vital that organizations capture mobile communications in their native form, complete with full context and metadata. If the firm operates solely in the U.S., this means being able to capture text content directly from mobile carriers such as AT&T, Verizon and U.S. Cellular, to name a few.

Having the ability to capture all the message types (e.g., SMS, MMS, RCS) is essential to fully understanding sent and received communications. This applies to both corporate-owned and BYOD policies.

Content that's captured in native format and in context is extremely beneficial during e-discovery. Firms can quickly and easily review records in context rather than taking up resources to sort and compile information. A fast, effective e-discovery process can prevent costly legal fines and penalties.

4 Proactively define supervision protocols

Communications supervision isn't just an ongoing requirement for regulated users involved in the marketing or sales of financial products. Supervision practices can also be used to inspect how business data and information are being shared across different mobile devices and apps.

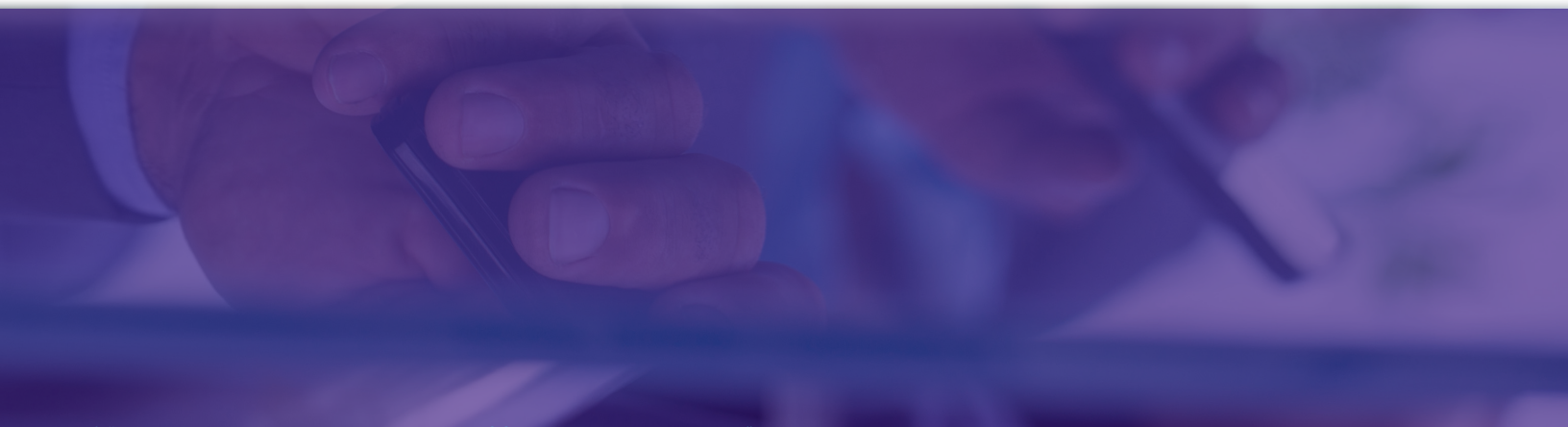
Businesses should immediately learn about employee messages that are in violation of corporate policies long before an investigation occurs. Proactive inspection of messages, including the use of prohibited apps, can help refine protocols and reduce compliance risks.

5 Train and retrain employees

Training employees isn't a one-and-done session. Businesses must review existing protocols, stay in front of demand for new tools and adapt to additional regulatory guidance. Training and continually training employees are integral steps for staying in front of risks.

DID YOU KNOW?

100 billion messages are sent via WhatsApp every day.[3]



[3] "WhatsApp is now delivering roughly 100 billion messages a day"

Limitations of common but outdated solutions

Businesses that have yet to decide to use a specialized mobile capture solution have likely used a variety of alternatives. Prohibition policies, custom-built or licensed solutions and the use of text-to-landline numbers are a few of the most popular:

Prohibition policies

This approach prohibits all mobile devices or prohibits just mobile apps. Businesses thinking about this strategy have several considerations:

- How likely will their workforce comply with the policy? What are the associated risks to reputation and fines if employees don't comply?
- What will the response be from their clients, including those who demand to communicate over text?
- Is the policy prescriptive enough? Does it include outlining the consequences of policy violations?
- Is the policy informed by all the stakeholders?
- Does the policy enable employees or inhibit their productivity?

Custom-built or off-the-shelf products

Some businesses take on each new communications channel using a one-off approach. This narrows their focus to thinking about content capture as a point solution for each type of communication instead of the broader view of all interactions and related data. For internal teams, this is rarely seen as a "part of their job," so ongoing maintenance isn't a priority.

They will either contract a third party to develop a connection to the content or license an off-the-shelf product to provide the same capability. Organizations leaning toward this strategy should consider the following:

- Who will support maintenance and potential disruption in the captured data flows?
- Will off-the-shelf products continue to meet the needs of the business as the content sources release updates and enhancements?
- How many other communication channels are currently supported?
- At what rate are new channels added?

Other considerations

Text to landline

Firms that know they must include text as part of their communications strategy but are still wary of increased risk exposure may choose to use text-to-landline solutions. This allows employees to interact with prospects and customers using their preferred communication channel, but the employee is still tied to their desk.

When using this option, businesses should consider how likely it is that employees will share their personal numbers to move their conversations to their mobile devices.

Forensic device collection

Many firms continue to rely on forensics tools like Cellebrite, which were originally designed for investigations and e-discovery. The service providers and tools are familiar, as is the primary challenge: mobile content that is either corrupt or incomplete, leaving possible exposures in response to regulators.

Carrier-based capture

Like forensic collection, some firms are familiar with the process of requesting and retrieving historical mobile content directly from carriers. Aside from response to court requests with specific time constraints, the process of working with carriers is rarely fast, easy or without complication, which results in incurring extra legal costs.

Simplify your firm's mobile compliance strategy

Businesses that still rely on prohibition policies are stifling productivity and creating a huge opportunity for risk exposure. Those who approach communications capture on an "as needed" basis instead of committing to a comprehensive solution are increasing internal workloads and risk exposure as well.

But firms shouldn't have to deal with multiple niche vendors to satisfy their regulatory obligations — it's costly and can create compliance gaps. Nor should they need to buy "good enough" solutions that require constant maintenance and updating to just barely keep up with evolving communication habits, trends, technologies and regulations. It's expensive in the long run and opens the door to legal and compliance risk.

Compliance departments should seek a specialized solution that can future-proof against potential exposure. But, more importantly, it will allow the compliance team to create, unify, manage and coordinate policies across platforms and devices.

Fortunately, established technologies have been available in the market for several years. These include both technologies that allow direct-from-carrier capture as well as containerization approaches that enable devices to be partitioned to segregate personal from business communications.

Working with vendors that support both approaches as a firm evolves its device policy over time — and as its workforce becomes primarily remote — has its benefits. Mainly, it provides firms with the maximum flexibility to respond to change without disrupting vital communications.

smarsh®

Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals in a wide variety of digital communication channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com

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 - 06/23

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

© 2023 Smarsh, Inc. All rights reserved