smarsh®

THE DEFINITIVE GUIDE TO ELECTRONIC COMMUNICATIONS CAPTURE

For Effective Compliance and Risk Management

Overview

A strong electronic communications compliance program is foundational for a variety of crucial business use cases, from recordkeeping and supervision to e-discovery and internal investigations. The secure, effective capture of electronic communications is a prerequisite for enabling these critical business functions. However, a clear understanding of the benefits and risks of communications capture, and available capture technologies, is often missing from an organization's overall compliance strategy.

Under the pressure to manage an ever-increasing volume and diversity of communications data, staying one step ahead of new channels is a distinct challenge. Evaluating options to streamline and automate the capture process is vital to establishing a scalable, sustainable compliance program that can evolve alongside the changing communications landscape.

The “Definitive Guide to Electronic Communications Capture” is a comprehensive resource full of definitions, recommendations and guidance for developing effective, high-value compliance programs. It focuses on capturing and managing electronic communications in a modern, highly regulated financial services organization.

This guide is divided into six main sections, related to the key communications content categories used by today’s business workforce:

- Email
- IM & Collaboration
- Conferencing Technologies
- Mobile
- Social
- Voice

You’ll find the tools and information you need to develop a strong communications capture strategy and understand the compliance risks and benefits of enabling new communication channels. You’ll become familiar with the latest capture technology options and be able to evaluate and improve your existing solutions to move your business forward.

Table of Contents

Introduction

What are electronic communications?

In the context of this guide, the term “electronic communications” refers to the communications generated by regulated firms for business purposes. This includes any electronic data, such as emails, chats, posts, recordings, emojis, application and document sharing, and attachments transmitted entirely or partially in a digital format. Electronic communications can be sent across various communication channels, including email, IM & collaboration, conferencing technologies, mobile, voice and social media.

What is compliant electronic communications capture?

By “compliant electronic communications capture” we mean the approach used by firms to proactively capture communications for the purpose of satisfying books-and-records or supervisory obligations. In this context, proactive means capturing all communications at their point of message delivery and creating an inclusive copy of the communications. This inclusive copy is used as the system of record to satisfy regulatory requirements.

Proactive capture is opposed to reactive capture, which involves capturing specific subsets of content on-demand. This reactive approach is typically used for e-discovery or investigative purposes. Regulated firms are particularly focused on capturing communications content to satisfy FINRA Rules 4511 and 3110, SEC 17a-4 and SEC 204.2, as well as similar requirements outlined by IIROC (Canada), FCA (UK) and within MiFID II (EU).

Why is specialized electronic communications capture technology important?

The ever-changing communications landscape

The way today's financial services organizations communicate and collaborate has fundamentally — and irreversibly — changed. Business users continue to drive their organizations toward new ways to reach customers and richer ways to collaborate internally. They want to use the latest communication channels to get the information they need faster, increase their productivity and become more effective.

While the increasing variety of communication and collaboration tools benefits many organizations, it also brings a new set of complexities. In fact, some firms have difficulty merely keeping track of all the tools their employees use.

Increased demands on compliance

For those tools that have been approved, firms need to be able to:

- Capture the generated communications to meet regulatory requirements
- Identify an individual across networks, which is often complicated by multiple usernames and varying access rights
- Track information as it travels across networks that could potentially impact the business
- Ensure they can enforce policies on any tools that are being used to communicate with customers

In addition to an increased variety of communications tools, the volume of communications data has also exploded. This all means that having specialized, automated capture technology is essential for today's compliance teams to function effectively.

A look to the future

Given how quickly the communications landscape is changing, compliance teams must have a capture technology solution that prepares them for the future. When a new communication channel gains traction with employees, or when an existing channel changes, compliance teams can stay one step ahead of these developments.

Plus, communications and collaborative tools are increasingly leveraging advanced analytics, machine learning and artificial intelligence in their platforms. Compliance teams need to be ahead of "RegTech" developments so they can execute policy controls on advanced technologies that are fast becoming mainstream.

What is the regulatory context?

As the number of supported communications tools expands, so does regulatory complexity. Regulators including FINRA, the SEC, FCA and IIROC consistently state that any communications tool used to conduct business must be captured by financial firms. Capturing this content is necessary for firms to meet their books-and-records and supervisory obligations. As a result, regulated organizations must be:

1. Proactive in working with the business to determine if the risks of a new tool can be mitigated prior to its approval for use
2. Active in their inspection of communications used by regulated users to ensure that unauthorized tools are not in use

From a supervisory perspective, firms must also ensure that the capture technologies they leverage are suited for purpose. They must be capable of capturing all the conversational activity that happens on each communications platform.

Ultimately, regulators are focused on inspecting the firm's ability to enforce its written supervisory procedures and identify areas of risk — not only the review of messages. Using a capture technology that enables a firm to easily understand conversational context makes it easier to spot behaviors that could be indicators of financial risks.

As it pertains to the use of advanced communications technologies, regulators have been aggressively embracing AI/ML approaches in conducting exams. Nearly all have stated explicitly that they expect firms to embrace advances in communications technology.

Why capture technology needs to incorporate all channels, not just email:

At one time, email was the primary communication tool used in business. However, that has changed. Today, companies use collaboration and conferencing platforms such as Microsoft Teams, Slack and Zoom. They communicate in chat messages, on video, through social media and across multiple devices.

What is the status quo?

The capture options available to compliance teams today

Every communications tool in use today is unique, and the corresponding methods of content capture vary widely. Sources like email are mature, and there are well established ways to capture this content, such as journaling. However, collaboration and conferencing tools, social media platforms and mobile platforms each allow a distinct set of capture options and provide differing levels of access to their content (e.g., what level or amount of access to content they make publicly accessible via APIs). Some of these options are better suited than others for firms faced with regulatory obligations.

At the same time, rudimentary methods such as capturing screenshots or user downloads of historical content are losing favor with compliance executives. They do not provide sufficient confidence that all content, context and metadata is being collected to withstand regulatory scrutiny. Many compliance executives have taken the stance that users cannot use communications tools that the firm cannot reliably capture.

A broader perspective on electronic communications capture

The specialized, automated capture of electronic communications is fundamental to a successful compliance program. However, the value of capturing electronic communications goes far beyond regulatory compliance. More firms are now acting on the realization that risk and business value can live anywhere. The deployment of new communications tools means that information governance controls need to be extended to these new locations.

Communications generated using these new tools are business records. They require protection to ensure they do not create opportunities for data leaks or loss of intellectual property. Additionally, definitions of communications risks need to include potential violations of corporate codes of conduct, such as the recent examples of “Slack bullying” and “textual harassment.”

Captured communications data can serve as a business asset. This data can feed enterprise applications and be leveraged by multiple business stakeholders to better understand customer preferences and improve service delivery within an organization.

5 Key Use Cases for Captured Communications:

- Supervisory pre-review and policy inspection prior to content archiving
- Data retention to satisfy books-and-records regulatory obligations
- Supervision and surveillance to achieve compliance and manage risk
- Readily available native content for e-discovery and investigations
- Extractions of data insights using AI and ML to drive business decisions

How should compliance teams evaluate the benefits and risks of communications tools?

Many firms are now extending their due diligence efforts to proactively inspect new communications tools before they are permitted for use within their firms. Compliance teams are working closely with security, legal, IT and business stakeholders to weigh the benefits of new communications and collaborative tools against the risks.

Adopting tools that today's customers demand is beneficial to business in a number of ways, including improved productivity, greater customer responsiveness and a competitive advantage. Each new communications tool includes risks, too. Incremental regulatory, litigation, data privacy and InfoSec issues are among those concerns.

Every new communications platform is unique, necessitating nuanced risk management strategies. Policy updates, user training and technologies that automate policy enforcement can help to satisfy firms' thresholds for acceptable levels of risk.

How does your compliance program stack up?

Given the realities of how your organization is communicating and collaborating today, how should you assess how your compliance program stacks up against your peers? Here are some general considerations:

- **Proactive vs. reactive**: consider whether your team is fully engaged with business users to stay updated on the tools and functionalities demanded by your customers
- **Enabling vs. taxing**: most high-performing compliance teams are seeking to contribute to top-line growth and competitiveness. Equipping users with the tools they need to better respond to market and customer demands directly contributes to that perception
- **Collaborative vs. siloed**: compliance teams are working more closely with legal, IT and InfoSec to arrive at shared views of communications risk. This is opposed to viewing risk solely through a compliance lens
- **Directional vs. tactical**: innovators are anticipating what comes next. This is an absolute, undisputed reality of communications and collaborative technologies. It is inevitable that there will always be the next network
- **Risk vs. activity**: communications capture plays a vital role in ensuring that compliance teams can effectively spot red flags before they result in exposure to the firm. This is versus a sole focus on review rates and reporting

Chapter 1 - Email

Email remains the communications lifeblood for most organizations. For regulated organizations, it continues to serve as the foundation for fulfilling books-and-records obligations. Email also provides legal teams with the bulk of electronically stored information (ESI) for e-discovery, informs HR on investigative processes, and enables both internal and external business communications.

Key regulations surrounding the capture of email communications:

Since the early 2000s, regulated firms have addressed FINRA, SEC, IIROC, FCA and other recordkeeping obligations for email by capturing an inclusive copy of every business message sent or received by regulated users. Those messages can then be stored and supervised within the native messaging system, led by Microsoft Exchange. Alternatively, messages can be delivered to a third-party technology for storage and supervision to meet specific requirements, including:

FINRA Rule 4511: requires that firms preserve books-and-records for a period of at least six years (if not governed by other specific FINRA or SEC retention periods)

FINRA Rule 3110: requires that firms establish and enforce written supervisory procedures

SEC Rule 17a-4: requires that firms preserve records in non-rewriteable and non-erasable format

Investment Advisers Act, Rule 204(2): specifies recordkeeping for investment advisors

Investment Dealers Association of Canada, IDA 29.7: requires the retention of records related to business activities

MiFID II Article 16: identifies recordkeeping, storage and supervisory requirements for all communications that lead to a financial transaction

United Kingdom Financial Conduct Authority (FCA), SYSC 9.1.2: requires firms to retain business records for a period of at least 5 years

The volume of email communications has continued to grow, along with the explosion of other content sources including chat, collaboration and social media. As a result, the continued reliance on on-premise capture and archiving platforms designed for email to satisfy regulatory obligations has become increasingly challenging.

Most firms also have established practices to inspect email for potential infractions of company communications and code of conduct policies, albeit on a more ad-hoc basis. These include harassment, data leakage and IP mismanagement.

The risks associated with email communications

Capturing email to satisfy compliance obligations is not new, but it is also not without evolving risks. Here are some of the most critical:

DID YOU KNOW?

Around 300 billion emails are sent every day.[1]

External information security risk

Not surprisingly, email remains the primary threat vector for external bad actors. The threat horizon continues to expand, from non-stop spam and malware to the most sophisticated targeted polymorphic attacks and ransomware. This topic remains a top priority for FINRA, which strongly advises firms to enhance their security postures as they transition workers to remote status.[2]

Data privacy risk

Most regulated firms are subject to multiple data privacy obligations in the markets in which they operate at both the U.S. state level and internationally, including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). To date, financial regulators and data privacy authorities have taken a pragmatic stance regarding the regulated capture of business-related email. They regard the capture of email for the purpose of satisfying a regulatory requirement as sufficient to be carved out from data privacy obligations.

However, firms need to have the ability to audit and respond to Right of Access requests. They also need to be able to affirm that captured email communications are not used for other purposes. Other purposes may include selling business-related communications data to third parties when 1) the sale was not disclosed to users, or 2) users were not given suitable opt-out provisions.

Regulatory risk

Compliance supervisory users need validation that they are following written supervisory procedures that include reconciliation against email messaging data. For example, they must provide proof that they have reviewed a specific percentage of a user's email. This process becomes significantly more complex if the primary email system is not performing reliably.

Internal policy risk

Given email’s everyday use, the potential loss of intellectual property and misuse of sensitive information are always possibilities and require ongoing inspection. However, those who knowingly violate policies are most likely to use tools where they believe they can avoid detection. It should be noted that, today, given where most supervisory and inspection processes are focused, that tool is typically not email.

Deadline risk

Email is a workhorse serving the needs of multiple company stakeholders. For under-resourced on-premise email systems, this can result in challenges in meeting time-sensitive information requests. For instance, compliance users who need to search, filter and produce large quantities of email may have a difficult time meeting ad hoc regulatory requests.

Availability/outage risk

As is the case for any business-critical application, service disruptions will happen. For on-premise email platforms, the magnitude of this risk can be amplified. This is due to the nature of high availability and disaster recovery investments and their recovery time objective (RTO). It is also due to their ability to ensure business continuity during outages. Even with nightly back-up to disc or tape, time to recover email and avoid compliance gaps can be a significant risk for firms not leveraging the latest email server advances.

Capturing email for compliance: the alternatives

As email volume grows, meeting compliance requirements has become more complicated. Due to financial services recordkeeping requirements, capturing email reactively or on-demand is not a feasible option. That leaves firms with two viable alternatives:

1. Continued reliance on the primary email system:

For some firms, the primary email system can sufficiently address their recordkeeping requirements. Other firms have moved their email to Microsoft Office 365, which provides a breadth of retention management features to address core regulatory recordkeeping requirements for email. They can take full advantage of advances in the Microsoft platform via the Security and Compliance Center as well as the Records Management Center.

However, Microsoft 365 may not be capable of addressing the breadth of every firm's compliance obligations:

- **Data location:** Microsoft 365 allows users to retain data in-place. However, that can complicate the ability to ensure that users have not deleted or tampered with data.
- **Immutability:** Microsoft 365 has the external attestation of being able to address SEC 17a-4 immutability requirements via the Preservation Lock feature. However, it should be noted that this feature was designed to meet legal preservation obligations and not to satisfy regulatory retention requirements. It may therefore result in over-preserving information that can increase cost and risks.
- **Throughput:** firms should review Microsoft 365's published performance data to ensure that data can be exported at a rate that will meet their specific regulatory obligations.[3]
- **Non-email content:** for firms with growing volumes of non-email content, Microsoft 365's email-centric design will flatten collaborative and interactive sources such as persistent chats into a series of emails. These emails require threading for their conversational context to be understood. The conversion to email from original source data can lengthen compliance review time and produce a broken chain of evidence if a message is missed.
- **Supervision:** Microsoft 365's Compliance Center capabilities are best designed for firms that need to satisfy broad, cross-industry retention requirements. These features may be sufficient for those with a small number of regulated users and simple policy sets including random sampling. However, they may not be sufficient for those managing large volumes of regulated users and the evaluation of complex policies.

2. Leveraging a specialized third-party archiving system:

The other alternative for firms to satisfy financial services compliance requirements is to capture email and deliver it to external archival and supervisory systems. Many of these technologies work seamlessly with Microsoft 365 and other systems, allowing firms to:

- Let the strengths of the Microsoft 365 platform be the backbone of their email communications infrastructure. Firms can capitalize on the Microsoft investments in availability and information security across email and other Microsoft content sources
- Meet immutability standards with a purpose-built, centralized books-and-records repository that preserves records without the risk of user intervention or error
- Enable a single pane of glass view across email, non-email and non-Microsoft content sources that allows user identities and policies to be created and executed globally
- Meet supervisory obligations with purpose-built features to execute policies and manage workflows across large groups of regulated users

Despite the growth of collaboration, conferencing and mobile-based content, capturing email for compliance purposes is still required. It remains a business-critical application and will continue to be the primary carrier for important firm-related communications into the foreseeable future. Email will also continue to be a prime target for outside threats and the location where the bulk of policy infractions will occur.

Methods of capturing email to satisfy compliance obligations are mature. However, these extend well beyond meeting recordkeeping requirements to include regulatory-mandated storage requirements and supervisory obligations, as well as communication policy inspection and enforcement. Firms are best served by continuing to monitor compliance advances in their chosen email platform. They must determine if these advances are sufficient to address their specific compliance obligations. Their email platform may still need to be augmented with the use of a purpose-built third-party archival and supervisory solution to meet their regulatory needs.

Chapter 1 - Email References:

1) https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf
2) https://www.finra.org/rules-guidance/key-topics/cybersecurity
3) https://docs.microsoft.com/en-us/microsoft-365/compliance/content-search?view=o365-worldwide#content-search-limits

Lane Collins 12:50 PM
Really need to give some Kudos to @julie for helping out with the new influx of Tweets yesterday. People are really, really excited about yesterday's announcements.

Kiné Camara 12:55 PM
No! It was my pleasure! People are very excited.

Jason Stewart 2:14 PM
What are our policies in regards to pets in the office? I'm assuming it's a no-go, but thought I would ask here just to make sure what was the case.

Acme Culture Meeting 2:15 PM
Event starting in 15 minutes:
Culture Weekly Meeting
Today from 2:30 PM to 3:00 PM

Johnny Rodgers 2:18 PM
shared a post
Building Policies & Procedures
Last edited 2 months ago
SECURITY POLICIES
- All guests and visitors must sign in

Jason Stewart 2:22 PM
Thanks Johnny!

Chapter 2 - IM & Collaboration

Like email, instant message and collaboration technologies are well-suited for organizations of any size and across industries. Unique from email, however, are the multiple combinations of communication modalities offered by each platform. These include persistent chats, document sharing and co-authoring features, custom emojis, video and screen sharing and AI-enabled bots and services. These can each create distinct challenges for compliance teams.

Today's most popular platforms are Microsoft Teams and Slack, complemented by a dizzying array of functional favorites including Jira, Atlassian, Wrike and many others. These tool preferences differ across departments and functions. Add in common organizational changes and corporate acquisitions, and most enterprises are using an average of 3.8 collaboration platforms at a time.[1]

The 12 to 18 months leading up to 2020 witnessed a dramatic growth in the IM and collaboration technology space. This growth was led by Slack and Microsoft Teams, joined also by Cisco WebEx Teams, Workplace by Facebook and Symphony. Microsoft reported during this time period that more than 500,000 organizations were using Teams compared with 200,000 organizations a year ago, with 13 million daily active users (DAUs)[2], surpassing Slack's 10 million.[3]

The benefits of enabling collaboration technologies

The reasons behind this explosive adoption are clear: real, tangible ROI. Brian Hill, Principal at Wellington Consulting and long-time expert on the collaboration technology market, notes that users of these tools have realized many benefits that have fueled the category's growth.[4]

Benefits include increased productivity, improved business cycle times and improved service delivery. These all contribute to a reduction in cost and the ability to positively impact revenue based on increased business agility and responsiveness.

These points are supported by an April 2019 study led by Forrester Research.[5] In this study, users of Microsoft Teams reported a 17% reduction in daily email volume and a 19% reduction in weekly meetings. A similar study conducted by IDC in 2017 noted that users of Slack saw a 32% reduction in emails and 23% fewer meetings.[6]

MS TEAMS

17% reduction in emails received per day

18% improvement in time-to-decision

19% reduction in meetings per week

832% ROI over 3 years

(Source: The Total Economic Impact of Teams, Forrester, 2019)
Teams: 13 million daily active users

SLACK

32% less email

21% faster response time to sales lead

23% fewer meetings

86% say it’s easier to share key learnings

(Source: The Business Value of Slack, IDC Research, 2017)
Slack: 12 million daily active users

Then the world changed...

A newly remote workforce

COVID-19 abruptly and urgently drove virtually every organization into the market for collaborative and conferencing technologies, many for the first time. Firms that had previously operated with mostly in-office staff were suddenly thrust into a new paradigm. They had to consider how to supply remote workers with equipment and secure means of connectivity to corporate IT resources. Organizations have had to provide tools that allow remote work groups to continue to stay on track with key deliverables and customer commitments.

The expansion in use of these tools has been nothing short of remarkable. Slack reported a 25% increase in users in a one-month period (March 2020).[7] Microsoft noted that the use of video within Microsoft Teams increased by 1,000% in that same time period.[8]

This tremendous spike in usage has been experienced not only by established market leaders, but also by new and more niche applications. Google Meet, Houseparty, Discord, Marco Polo and other downloadable apps have gained significant traction.

But the fast adoption of collaboration tools hasn't been without challenges. Many collaboration applications offer free versions. These are typically lacking either in key features or in the controls required to capture the communications activity occurring on those platforms. Absent explicit guidance, employees are using collaboration tools with which they are already familiar or those that were easy to obtain. These are not necessarily the tools that have been approved by management.

Unfortunately, some collaboration tools and versions are not suited to meet the demands of regulated businesses. The same goes for organizations that are subject to frequent litigation and investigative demands.

The unique challenges of capturing IM & collaboration content

As noted previously, collaboration platforms consist of multiple communication modalities, and each platform offers its own unique combination:

Conversational

Discussions typically occur over a series of asynchronous messages or posts. Understanding the context of a conversation is difficult when capturing individual messages unless message ordering is preserved. This includes noting items that may have been modified or deleted since they were originally posted.

Multiple participants

Conversations on collaboration platforms often consist of multiple participants. Any one of those participants may have policy restrictions for accessing specific subjects. For example, many firms have barriers or "ethical walls" that must be enforced between broker and advisory groups. Determining which participants should be on record — as well as capturing what can be hundreds of participants in a meeting — can be challenging on some platforms.

Interactive

Conversations can persist over configurable time periods. This requires firms to monitor changes to conversations that could be relevant to compliance tasks, including noting multiple versions of a document created by co-authoring features.

Activity oriented

Unlike email, collaborative content typically behaves more comparably to a virtual meeting room. Email is the transcription of notes from a meeting versus a collaborative event, which is the actual in-person meeting experience itself. The difference can be very significant from a content capture perspective. It may be relevant to understand who has joined or left a meeting, as well as noting the identity of a meeting participant known only as "call-in user 2."

Mobile friendly

Most modern collaboration tools have been designed with a "mobile first" philosophy. Today's remote workforce may need to connect to colleagues from anywhere — including from their mobile devices while in transit. Capturing collaborative content should function independently of devices used, to ensure the complete record of a conversation has been preserved.

The risks associated with IM & collaboration technologies

Clearly, collaboration tools are highly popular and are now critical to doing business. Whether measured explicitly or more broadly, organizations are seeing their value. Compliance executives seek to enable their business to use the tools with which their employees and clients are familiar and comfortable. If your firm does not allow these channels to be used, it's likely that your competitors do.

However, collaboration tools present potential risks that can impact nearly every function of the business. They require the participation of stakeholders from all functions to ensure that a complete view of possible vulnerabilities is examined before making an investment. Those risk areas include the following:

Regulatory compliance risk

Every firm regulated by FINRA, SEC, FCA, IIROC, MiFID II or other regulatory bodies has an obligation to meet books-and-records requirements by capturing all business-related communications. Those requirements do not distinguish one communications or collaboration source from another.

In fact, FINRA Rule 4511 and SEC 17a-4 both note the requirement that those records be "true, accurate, and complete," highlighting the importance that capture methods account for the multi-modal, interactive and conversational nature of collaboration technologies. As compliance executives have frequently stated, if a communications channel can't be captured, employees can't use it to conduct business.

Data privacy risk

One challenge unique to collaboration tools such as Slack and Microsoft Teams is that they can look like places to socialize. Privacy complications can arise if collaboration tools are not used exclusively for business purposes. Content collected from those tools must be used by the firm for the stated business or regulatory purposes that are outlined in policies.

International and U.S. state privacy mandates such as the GDPR in the EU and the CCPA in California continue to emerge. Firms should be aware of how each collaboration tool will impact their ability to fulfill Right of Access requests under applicable privacy laws.

Information security risk

InfoSec remains the most closely watched risk category, spanning a broad range of topics. These include breach, outages, spam and malware infection, susceptibility to advanced targeted attacks and other potential vulnerabilities. Today's major information security providers remain heavily invested in and focused on email and web-based threats.

The result has been an increase in the incidents of malware and ransomware targeting collaborative platforms such as Microsoft Teams[9] and Slack.[10] Inevitably, those with intent on doing harm are going to follow users to popular platforms. Firms are best served to monitor the InfoSec credentials, third-party attestations and accreditations, and investments made by collaboration tool providers before investing.

Discovery review risk

Multiple communication modalities — along with the fact that conversations can be changed, modified or deleted — create new complexities for discovery programs that are designed for email. Familiar parent-child relationships of email are not as easy to decipher when there may be hundreds of participants in a persistent chat with consistently evolving content.

For firms facing frequent litigation, the risk of missing a critical conversational component is exceptionally high. Using capture tools unsuited for collaboration technology is an exposure that is catching the attention of an increasing number of legal teams.

Internal policy risk

A primary challenge in the deployment of collaboration tools is the lack of guardrails. Potential exposures can be introduced if communication policies guiding the appropriate use of intellectual property and other sensitive information are not extended to these platforms. "Zoom bombing" and "Slack bullying" are becoming familiar terms. They highlight the need for firms to consider HR and other code of conduct violations in their definitions and plans for communication risks.

Mitigating the risks of IM & collaboration technologies

For regulated firms, risk mitigation of collaboration tools has three main factors: 1) policy adjustments, 2) updated user training, and 3) selection of the appropriate capture technologies.

1. Policy adjustments

These typically take multiple forms for firms seeking to change the way they collaborate and communicate. Here are some of the most common:

Retention policies: Regulated firms have retention policies driven by mandates such as FINRA 3110 and SEC 17a-4. These must apply to all communications tools used for business purposes. Firms do not typically tie policies to specific tools, aside from the use of mobile devices. However, they do need to examine whether the types of activities conducted on collaboration tools would constitute "business records" as defined within their records classifications. Given the recent spike in usage of Microsoft Teams and Slack in particular, it will become increasingly difficult for firms not to retain those communications. At minimum, firms should inspect existing retention policies to ensure there are no implicit biases toward established communication technologies. Policies must apply equally to collaboration tools.

Communications policies: Similarly, employee communications policies should be updated to outline acceptable and prohibited usage of collaboration tools. This should be done in coordination with business stakeholders who are familiar with how those tools are being used by internal groups, as well as how they are shared with customers and partners. It is safe to presume that more explicit guardrails should be established for modalities including voice, video and app sharing than were required for email.

Supervisory policies: FINRA, SEC and other regulatory bodies do not differentiate one communications tool from another. If business is being conducted on behalf of the firm, it must be captured and supervised. Firms should evaluate existing supervisory workflows and policies to make sure they can preserve and review the interactive, multi-modal activities taking place on collaboration tools.

RECOMMENDED READING:

Managing Global Compliance: What to Do About IM and Collaboration Tools in the Enterprise

Content inspection/surveillance practices: Aside from regulated users, other risks introduced on collaboration tools by employees should be subject to periodic inspection. This is to surface code of conduct or other policy infractions. Most firms do not currently have an established, regular cadence to do this. However, proactive, periodic ad hoc inspection of content is an emerging best practice for spotting policy issues before they can damage the firm.

2. **User training:** The importance of employee training that is specific to new collaboration tools cannot be understated. As Brian Hill from Wellington Consulting noted, “A lot of organizations miss this point. Many organizations are focused on addressing this challenge clearly from a technology perspective, and that simply doesn’t work. There is no silver bullet from a technology perspective. The human capital element is really, really critical. So the training on the use of a collaboration tool needs to be very explicit; the policies need to be set up well in advance, with coordination across the various stakeholder groups. The training around those policies needs to be repeated on a regular basis and should cover other tools that are currently being evaluated. Many may have great training that can be implicitly biased toward email but might not necessarily reflect the way users interact with Slack or Teams. It’s important to address different features and functionalities that these tools have and what’s allowed and what’s not.”[11]

3. **Selecting the appropriate capture technologies:** There are different options available for capturing content from collaboration technologies. It is important to consider these alternatives in more detail.

Capturing IM & collaborative content: the alternatives

There are a variety of mechanisms available to capture the activity that occurs on these platforms. Here is a summary of the most commonly used options:

1. **Native features:** One of the most important differences among collaboration tools is the mechanism provided to capture the unique conversational content, context and metadata that each produce. Every tool is different, and some providers are not fully versed in the requirements of regulated firms. If attempting to capture content directly via collaboration tool providers, firms should consider (at minimum):

   - Vendor strategy governing what level of access they give to customers and partners for back-end functionalities via APIs or other methods of access
   - What specific content and events are accessible for capture. Collaboration platforms provide multiple functionalities including chat, video, voice, edit/delete events, app sharing, bots, etc. Knowing what is accessible will inform decisions later about which capabilities are enabled for use and which should be prohibited by either technology or policy
   - How much historical content is accessible to customers and partners, and the mechanisms by which to access that content (e.g., how quickly content can be retrieved)
   - Storage technology used by the provider to ensure that content is not re-purposed or potentially altered
   - Data security and privacy investments, third-party attestations and accreditations (ISO 27002 and SSAE-16, etc.), as well as breach notification procedures
   - Availability of premium service tiers to support API access suitable for regulated firms
   - Notification procedures for API updates and enhancements

2. **Build your own:** Some firms with large IT development resources have opted to develop their own "connectors" to collaborative content sources in order to reduce cost. While this may be suitable for some, firms should consider (at minimum):

- Whether software development fits within the firm's business strategy and has direct bearing on enhancing revenue and improving client relationships
- How many networks are currently supported, and how many new sources are added per quarter or per year. Many large firms support 80+ communications sources, and compliance teams are under constant pressure from business users to enable new tools. Like compliance teams, most internal IT development groups will be hard-pressed to stay in front of demands of the business
- How frequently collaboration tools are updated, potentially requiring changes to the firm's capture mechanism
- Who in the firm will provide support, bug fix and other fail-safe options in the event of disruption to content capture data flows
- Where the captured content is delivered for archiving and the ease of consuming complex, interactive and metadata rich collaboration content into that system

3. **Construct basic content capture as needed:** Another cost-driven approach is to rely upon outside service providers to build "connectors" to content sources as they are demanded. Many archiving providers follow this approach to initially gauge demand before investing in the "productization" of each content source connector. Considerations for those choosing this approach include:

- Skills of the service provider to build content collection assets with a relatively long shelf life, versus T&M development work
- "Ownership" of the connector, once constructed
- Whether only basic messaging content will be collected, or if metadata, event-based information and interactivity, and non-text-based data (e.g., custom emojis) content will also be collected
- Responsibility for ongoing support, maintenance and upkeep
- Assurances that the provider will not alter original content properties and will attest to their development processes if the firm is questioned by a regulator or within litigation
- Knowledge transfer and the ability for internal teams to understand the development approach if they later choose to in-source the capture of that content type

4. **License third-party providers with productized connectors to capture collaborative content:** The final option is to partner with a provider with greater expertise and specific focus on capture technologies. These providers can capture content in a manner that will withstand the rigors of financial services regulatory compliance. Given the fast pace of innovation in the collaboration technology market, the following considerations should be prioritized when selecting a third-party provider:

    - Established track record of delivering capture technologies that help firms satisfy SEC, FINRA, FCA or similar regulatory requirements
    - Proven ability to deliver at a comparable scope and scale to your firm's compliance volume and workload
    - Ability to capture all available content sources made accessible by the collaboration tool provider, including metadata and event information
    - Capture features that allow firms to enforce pre-archiving policy controls on collaboration sources where they are available. These include ethical walls, disabling features, content moderation, disclaimer filtering and message blocking
    - Presence of direct relationships with key collaborative technology providers, including listing on those websites and marketing materials
    - Content capture development methodologies that minimize the gap between new collaboration feature releases and updates to the capture solution
    - Complete portfolios of onboarding, professional services, support, training and customer success services
    - Ability to deploy content capture solutions to align with the firm's IT architectural objectives, whether on-premis, in the cloud or while in transit
    - Transparent processes to notify firms of service changes or disruptions and enable customer self-diagnosis, where possible

The already-increasing popularity of Microsoft Teams and Slack, along with a suddenly remote workforce, have moved the adoption of IM and collaboration technology onto a new trajectory. More firms are experiencing the benefits of greater productivity and improved responsiveness to colleagues and customers as a result of collaboration technologies. They are also experiencing a reduction in the issues typically associated with being overrun by email. The trend is only set to continue.

These tools create new challenges for compliance teams, given their multi-modal, interactive and conversational platforms. Any activity that occurs within a virtual meeting could potentially be relevant to a regulatory event. Such activities may include employees joining and leaving chats, individuals modifying or editing content or replies that occur hours after the beginning of a persistent chat.

The sheer variety of collaboration tools on the market is a challenge on its own. Some of these are just a free download away, and not as well-suited to enable firms to meet their SEC, FINRA or FCA books-and-records and supervisory obligations.

Firms must acknowledge that content with business value and risk can live on any collaboration tool. The surface area for loss of intellectual property, violations of codes of conduct or policy infractions has now increased dramatically. With the implementation of GDPR, CCPA and emerging laws, firms must also consider data privacy risks and their ability to respond to right of access requests that might center on the use of a collaboration tool.

In addition to regulatory risks, the choice of the wrong tool — or the unguided use of a market-leading technology — can expose a firm to several other vulnerabilities. These are led by very visible and real InfoSec threats, such as the recent increase in spam, ransomware and other advanced targeted attacks.

Compliance teams seek to allow their businesses to use the collaboration tools with which they are familiar and that enable greater productivity. Doing so requires a thorough evaluation of the benefits and risks exposed by each collaboration tool. The selection of tools should be weighted toward those where risks can be mitigated using the appropriate capture technology.

Updated policies must reflect the accepted and prohibited use of each collaboration tool modality. Additionally, guidance must be issued to users to ensure that they understand how to safely get their job done on approved tools without introducing unnecessary risk.

Chapter 2 - IM & Collaboration References:

1) https://nemertes.com/research/the-relentless-shift-from-uc-to-workstream-collaboration/

2) https://venturebeat.com/2019/03/19/microsoft-teams-is-now-used-by-500000-organizations/

3) https://www.theverge.com/2019/7/11/20689143/microsoft-teams-active-daily-users-stats-slack-competition

4) https://www.smarsh.com/webinars/assessing-benefits-costs-of-todays-collaboration-tools

5) https://www.microsoft.com/en-us/microsoft-365/blog/wp-content/uploads/sites/2/2019/04/Total-Economic-Impact-Microsoft-Teams.pdf

6) https://a.slack-edge.com/eaf4e/marketing/downloads/resources/IDC_The_Business_Value_of_Slack.pdf

7) https://investor.slackhq.com/news/news-details/2020/Slack-CEO-Stewart-Butterfield-Shares-Updated-Business-Metrics-During-Tweetstorm-on-Impact-of-COVID-19/default.aspx

8) https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/09/remote-work-trend-report-meetings/

9) https://threatpost.com/single-malicious-gif-opened-microsoft-teams-to-nasty-attack/155155/

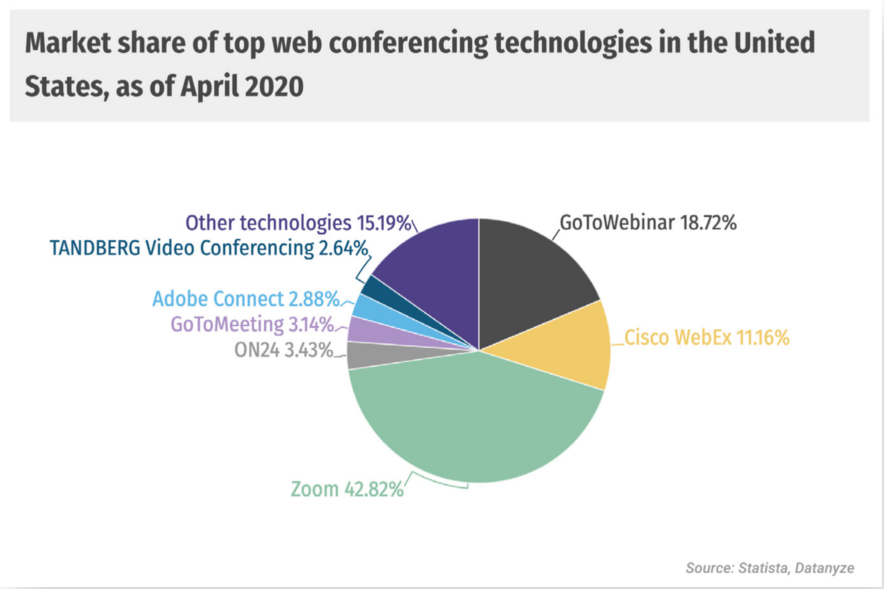
10) https://www.bleepingcomputer.com/news/security/slack-bug-allowed-automating-account-takeover-attacks/

11) https://www.smarsh.com/webinars/assessing-benefits-costs-of-todays-collaboration-tools

Chapter 3 - Conferencing Technologies

Online meetings were already a regular occurrence in our professional lives. But since the onset of the COVID-19 pandemic, they have become the estuary from which all information flows. Organizations must be able to quickly adapt to these social and environmental pressures, as well as the resulting industry changes.

In December of 2019, Zoom reported the number of daily meeting participants was 10 million. By March of 2020, that number had increased by 1900% to 200 million.[1]


Market share of top web conferencing technologies in the United States, as of April 2020

Source: Statista, Datanyze

Top 3 US Web Conferencing Apps Hit Over 70% Market Share[2]

Zoom was not the only beneficiary of the suddenly remote workforce. Other established conferencing technologies used by regulated organizations, such as Cisco Webex Teams, BlueJeans Network (recently acquired by Verizon), 8x8 and others, have experienced spikes in usage.[3,4] This has also spilled over into the collaboration space. Video use has increased exponentially, as illustrated by Microsoft Teams' 1000% video growth.[5]

Unfortunately for regulated firms, for every established conferencing technology seeing expanded use, there has also been a surge experienced by more risky newcomers. Technologies like Discord and Marco Polo, for example, have massively increased in adoption but were not designed to meet the requirements of financial services firms.

The benefits of enabling conferencing technologies

Embracing web conferencing as part of your communications strategy offers several benefits, including:

- Ability to easily and rapidly transition employees to remote work
- No scheduling conflicts like those with a physical meeting room
- Elimination of commute and travel times, adding to productive work hours
- Ability to share documents electronically with some or all attendees
- Ability to virtually meet with people anywhere in the world

Aside from saving time and resources, web conferencing can also significantly increase collaboration and customer satisfaction. Perhaps the most valuable benefit, though, is the advantage a business gains by assuring its flow of information does not have to be interrupted.

The unique challenges of capturing content from conferencing technologies

The transition to a remote work environment was daunting for many companies. Physical meetings were suddenly replaced by electronic communications, where users are sharing files, chatting about the firm's business and directly engaging with customers.

Organizations have shifted their view of conferencing technologies themselves. Rather than simply tools for "video broadcasting," business itself is being discussed, shared and delivered using conferencing technologies. This raises unique challenges, including:

- Choosing conferencing technology that is not designed to meet the requirements of regulated firms
- Inability to capture key features and modalities due to the lack of available APIs or other reliable methods of capture
- Capturing large video conference files, which are typically significantly bigger than other content types
- Enforcing communications policies across those networks
- The current lack of regulatory guidance on the capture of video conferencing content. Firms must continue to push regulators to define the parameters around necessary capture and storage of this data

Any of these challenges could have a serious impact on operations and force a business to balance compliance and productivity. These are trade-offs that could significantly raise a business's risk exposure.

The risks associated with conferencing technologies

As with any communications source, there are certain risks associated with using conferencing technologies.

Home networking risk

A sudden transition to remote work meant that many firms did not have the opportunity to set up employees with proper infrastructure. Some are now working from home at their dining room tables on the family computer that is not current on its security updates. Others may be on unprotected Wi-Fi networks or sharing bandwidth with family members that can cause connections to drop in the middle of an important client meeting.

User identity risks

Conferencing technologies all have unique controls to guard against unauthorized access to meetings. However, despite enabling waiting room features or protections for user-specific access codes, firms are only one user error away from a potential unwelcomed visitor (or “Zoom bomber”) into an important meeting.

InfoSec risks

Issues with security protections from conferencing providers are well documented. These include their use of end-to-end encryption (E2EE) and protections against malicious attacks, credential stealing and ransomware. For those conferencing providers who seek to serve the financial services industry and other regulated markets, enhancing their security posture is essential. The need to withstand rigorous security audits will be a prerequisite to ongoing adoption in those markets.

Data privacy risks

The potential presence of personally identifiable information (PII) within video conferencing is a new reality firms are facing. This has given rise to the recent adoption of the CCPA, as well as other state regulations that require that prior consent be given before recording a meeting (or video conference).

IP and data loss risk

As more companies conduct customer meetings, webinars and virtual conference presentations, they must be extra diligent about high-value or sensitive information that may be discussed or presented in an online conference. Firms are a simple screen grab or iPhone photo away from a potential loss of an important business asset.

Regulatory risk

Every regulated firm needs to meet regulatory recordkeeping, storage and supervisory requirements for communications that are approved for business use. If conferencing technologies are used, firms must capture all generated content, such as instant messaging activity.

Mitigating the risks of conferencing technologies

As with other content sources, risk mitigation of conferencing technologies is a function with three variables: 1) policy adjustments, 2) updated user training, and 3) selection of the appropriate capture technologies. Each of these deserves further exploration.

1. Policy Adjustments

Here are some of the most critical policy adjustments required to address conferencing technologies:

Retention policies - These should be adjusted to any modality that can be captured and is used for business purposes, such as instant messaging. Firms should also monitor advances in functionality provided by conferencing providers, so they can adjust capture practices as those solutions become available. They should keep up with additional guidance provided by regulators for recommended recordkeeping treatment of video conferencing technologies.

Communication policies - Video conferencing is one of the most critical areas where communications policies should be updated. Policies should outline acceptable and prohibited uses of approved conferencing platforms as well as clearly identify platforms that are prohibited from use entirely. This should be prescriptive, recognizing that video meetings can easily take on a casual, informal feel outside of the familiar norms of in-person business meetings.

While policy infractions are independent of the method of delivery, video does create some unique conditions. One example is the mandated use of backgrounds to avoid any unintentional display of offensive material. Alternatively, a policy to not use the camera function except when speaking can minimize the risk of something embarrassing being shared with your customers.

Content inspection/surveillance practices - In addition to the supervision of regulated users, firms should also periodically inspect conferencing for code of conduct or IP policy infractions. A good place to begin is with client-facing video meetings. Recordings should be reviewed prior to publishing or sharing that information with clients or prospects.

2. User training

Each conferencing technology provides a unique set of features and enables access to only a subset of these features for capture. Therefore, user training on acceptable and prohibited use policies is imperative. For example, if the firm prohibits the use of files subject to NDAs within conferences, that needs to be explicitly addressed in training programs and regularly monitored by the compliance team.

Training should also address the appropriate use of security and privacy features within each platform. These include the use of waiting room features, the importance of not sharing user-specific access codes, and training for meeting organizers to carefully manage distribution and attendee lists. This is to ensure that ethical wall or other policy violations are not created.

3. Selecting the appropriate capture technologies

There are different options available for capturing content from conferencing technologies. It is important to consider these alternatives in more detail.

Capturing content from conferencing technologies: the alternatives

There are alternatives to using a specialized content capture solution. Some businesses choose to explore the native features within the communications tools or to build their own solutions.

1. Native features:

There are differences between out-of-the-box functionality and specialized capture solutions for conferencing technologies. Most important are the mechanisms provided by each to capture the unique conversational content, context and metadata that are produced by the multi-modal platforms.

Every tool is different, and none are specialized to meet the unique requirements of highly regulated firms. If attempting to capture content directly via web conferencing providers, firms should consider the following:

- Level of access available via back-end APIs
- Events that are accessible for capture
- Amount of accessible historical content
- Storage technology used by the provider to ensure immutability
- Data security and privacy
- Notification procedures for API updates and enhancements

2. In-house solutions:

Some businesses with large IT development resources have chosen to develop their own connections to web conferencing content sources as a strategy to reduce cost. While this may be suitable for some, businesses should consider the following:

- If IT is a core part of the business strategy
- How many communication channels are currently supported
- At what rate new channels are added
- Who will provide support for maintenance and disruption in the capture of data flows
- Where the content will be archived, and if that archive can scale

3. Specialized third-party capture solution:

This is often considered the safest and most comprehensive option. The solution must have the capability to capture communications in full context so firms can leverage their rich metadata and see how conversations start and develop. When content can be sent directly to a robust data archive, communications can be accessed and understood alongside other communications sources such as IM and collaboration content. Some table stakes capabilities are outlined here:

- Ability to capture direct and group chat content
- Capture of voice content for platforms such as Zoom
- Ability to send content directly to an archive for retention and further analysis

✓

Web conferencing technology is not just a featured component of a communications strategy; it is essential to conducting business. All businesses that are required to — or would like to — manage and monitor communications must have a way to capture that content and enforce related policies.

For businesses that are not in the IT industry, taking on these challenges may be more onerous than they anticipated, and they may be unable to keep up with regulatory requirements. Likewise, relying on the native features some technologies offer may leave gaps that increase a business's risk exposure.

For most, the best course of action is to rely on a specialized provider. A fully managed content capture solution allows organizations to fully adopt web conferencing technologies without the increased concern about risk exposure.

Chapter 3 - Conferencing Technologies References:

1) https://venturebeat.com/2020/04/02/zooms-daily-active-users-jumped-from-10-million-to-over-200-million-in-3-months/

2) https://learnbonds.com/news/top-3-us-web-conferencing-apps-hit-over-70-market-share/

3) https://www.bluejeans.com/blog/video-conferencing-usage-during-coronavirus-outbreak

4) https://finance.yahoo.com/video/zoom-competitor-8x8-sees-spike-195401644.html

5) https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/09/remote-work-trend-report-meetings/

Chapter 4 - Mobile

70% of employees' phones will be replaced by mobile devices

88% of employees use mobile phones for work while on personal time

91% of mobile users keep their smart phone within arm's reach

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

Now that mobile devices are integral to the workplace, regulated organizations have had to decide how to approach their mobile strategy. They must ensure their ability to enforce policies and meet regulatory requirements governing the capture of electronic communications.

In the most tightly controlled model, companies supply their employees with mobile devices. 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, both policy enforcement and content capture are a concern.

To address these compliance concerns, do businesses have to use two different technology solutions? 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.

Firms should not have to deal with multiple niche vendors in order to satisfy their regulatory obligations. Nor should they need to buy "good enough" solutions that may open the door to legal and compliance risk. Compliance departments should be looking for a specialized solution that can cover potential exposure and empower them to create, manage and coordinate policies across platforms and devices.

The benefits of enabling mobile communications

The benefits of a mobile strategy include not just voice and text but mobile-tethered communications as well. Since voice is covered in a later chapter, the focus will be on text and mobile-tethered apps in this chapter.

Considering that over 90% of text messages receive a response, it is hard to deny that this should be a key component of a company's communications strategy. Aside from the obvious convenience that mobile devices provide, they also offer flexibility to your workforce. Allowing employees to work in various settings using a mobile device enables them to rapidly respond to customers and prospects. This increases customer satisfaction and loyalty. It also drives in-house productivity among colleagues.

As employees choose mobile communications over email, mobile-tethered applications such as WhatsApp and WeChat have increased in popularity. Due to demand, these apps now support end-to-end-encryption protocols to provide secure mobile communication channels between employees and customers. With this security in place, these apps have become preferred informal communication channels to maximize real-time critical and confidential financial decision-making.

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 end up holding information that becomes relevant to the discovery process. This could be voice, text messages or more intensive content delivered through mobile-tethered applications. In many cases it is 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-tethered applications 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 is 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 GDPR, the 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 is 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 to understand lengthy asynchronous chat discussions. The use of emojis and other unique features offered by WhatsApp or WeChat, for example, also lengthen and complicate the review process.

The risks associated with mobile technologies

Mobile devices have become a common and crucial tool in the workplace. An employee's ability to engage with clients and customers from anywhere in the world and at any time has allowed businesses to reach new heights in productivity, collaboration and responsiveness. These benefits have also created compliance risks for industries where all forms of communication need to be captured and retained for regulatory purposes.

Concerns about risk exposure have prompted some businesses to use blanket prohibition policies where mobile devices are concerned. The 2019 Smarsh Compliance Survey revealed that 60% of firms prohibit the use of mobile devices for business purposes. Keeping in mind that 91% of people always have their smartphone within reach, this makes policy enforcement a nearly futile task.

Other businesses attempt to restrict the use of specific mobile device features, allowing voice and text but not mobile-tethered applications, for example. These approaches have two distinct risks: 1) the high likelihood that employees that will either disregard or be unaware of them, and 2) that policies are either poorly defined or not actively monitored for compliance.

For firms that have strong policies in place there is still the risk that they are not capturing the right information. Text and mobile-tethered applications present a unique syntactical context that allows us to express emotion in an otherwise flat exchange. The use of images and emojis can be of enormous importance in uncovering behaviors. Many solutions on the market today are unable to capture and preserve this context.

Mitigating the risks of mobile technologies

There are five critical things businesses can do to mitigate the risks posed by mobile devices:

1. Actively develop mobile device governance

Existing mobile device or communication policies need to be reviewed by all stakeholders and employees. 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 whose role is to:

- Assess the existing mobile environment
- Refresh policies per user group
- Update policies as new apps and functionalities are deployed
- Examine the latest trends and benchmarks

2. Stay on top of mobile capture requirements

Capturing mobile-based content, including its unique metadata, emojis and GIFs, enables firms to more effectively adhere to regulatory guidance on digital communications. This was most recently highlighted in FINRA's 2019 Exam Findings and Observations.[2]

3. Capture content the right way

It is vital that organizations capturing mobile communications can do so in native form, complete with full context and metadata. This means being able to capture text content direct from mobile carriers such as AT&T, Verizon and U.S. Cellular, to name but a few in the U.S. alone. It is important to be able to capture all the message types — SMS, MMS, RCS, for example — in order to fully understand the sent and received communications. Similarly, if BYOD applications such as CellTrust are activated, these communications should also be captured directly from the source in their native format for proper information governance.

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 not wait until an investigation is taking place to learn that employee messages are violating policies. 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 retraining employees are integral steps for staying in front of risks.

DID YOU KNOW?

Over 18 million texts are sent every minute.[3]

Capturing mobile communications: the alternatives

Businesses that have not yet decided 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:

1. Prohibition policies:

Policies range from prohibiting all mobile devices to prohibiting just mobile-tethered apps. Businesses thinking about prohibition policies have several considerations:

- How likely it is that their workforce will comply with the policy
- What the response will be from their clients, including those who demand to communicate over text
- If the policy is prescriptive enough, including outlining the consequences of policy violations
- Whether the policy has been informed by all the stakeholders
- If the policy enables employees or inhibits their productivity

2. Custom-built or licensed connectors:

Some businesses take on each new communication 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. They will either contract a third party to develop a connection to the content or license an off-the-shelf (OTS) product to provide the same capability. Organizations leaning toward this strategy should consider the following:

- Who will provide support for maintenance and potential disruption in the captured data flows
- For OTS products, if they can 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 new channels are added
- Where the content will be stored, and if it can be scaled

a. **Text to landline:** Firms that know they must include text as part of their communications strategy but are still wary of increased risk exposure 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 employees will share their personal numbers to move conversations to their mobile device.

b. **Forensic device collection:** Many firms continue to rely upon forensics tools like Cellubrite that 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.

c. **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.

d. **Specialized, automated third-party capture vendors:** 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 allow 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. It provides firms with the maximum flexibility to respond to change without disrupting vital communications.

✓ In a world where bankers, brokers and asset managers are conducting business remotely, the demand for communication on mobile devices has increased exponentially. While this has been an abrupt transition for some, FINRA has indicated that it will continue to focus on ensuring that a firm's recordkeeping and supervisory processes stay active in this new environment. Similarly, the UK's Financial Conduct Authority (FCA) expects all companies to meet their regulatory obligations despite the crisis.

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-tethered applications offer, and employees are inclined to oblige.

Businesses that still rely on prohibition policies are not only stifling productivity, they are 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.

Chapter 4 - Mobile References:

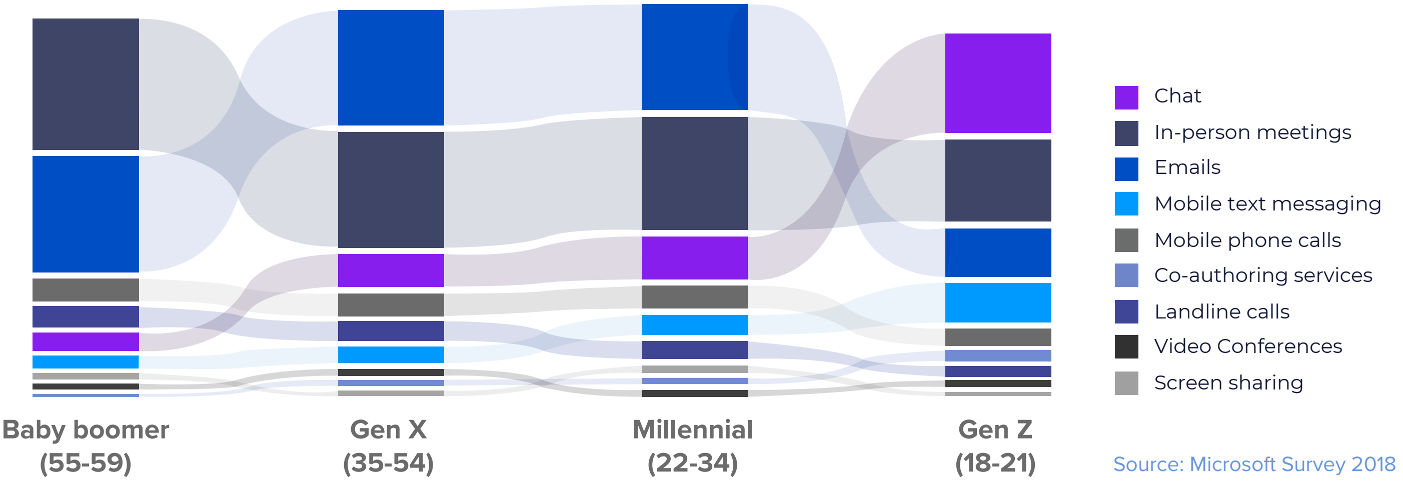
1) https://www.gartner.com/en/marketing/insights/articles/tap-into-the-marketing-power-of-sms, https://www.business2community.com/infographics/email-marketing-vs-sms-marketing-stats-infographic-02021390

2) https://www.finra.org/rules-guidance/guidance/reports/2019-report-exam-findings-and-observations/digital-communication

3) https://www.domo.com/learn/data-never-sleeps-7

Chapter 5 - Voice

The generational divide



Source: Microsoft Survey 2018

Regardless of the generation, in-person meetings remain a constant preference in the way we communicate. With remote workforces becoming the new normal, people are filling the face-to-face gap by using video and voice chat internally and with clients.

In an unprecedented move, many banks (including Bank of America, Citigroup, Goldman Sachs and JPMorgan Chase) are allowing their traders to execute trades from home. However, regulatory obligations still apply. This can be a challenge considering the variety of communication methods that are available while working from home.

Historically, the ability to capture and govern voice data in tools like Skype for Business, Teams and now Zoom has been especially challenging. The answer has been merely to disable this functionality. This is no longer realistic.

For many years, Smarsh has witnessed the growing demand for voice to be included as an integrated channel of compliant communication. This enablement is not only to provide a more collaborative and productive work environment, but also to harness the additional insights that voice content can provide.

Key regulations surrounding the capture of voice content:

On January 3rd, 2018, MiFID II went into effect in Europe. Some European countries, for example the UK, had already mandated that voice content be captured. However, MiFID II solidified the requirement for all European Union states to capture voice communications.

Article 16(7) states: *“Records shall include the recording of telephone conversations or electronic communications relating to, at least, transactions concluded when dealing on own account and the provision of client order services that relate to the reception, transmission and execution of client orders.*

“Such telephone conversations and electronic communications shall also include those that are intended to result in transactions concluded when dealing on own account or in the provision of client order services that relate to the reception, transmission and execution of client orders, even if those conversations or communications do not result in the conclusion of such transactions or in the provision of client order services.”

In the U.S., the requirements have a few more dimensions. Financial services compliance is a much broader topic than recordkeeping and supervisory practices related to communications. Firms are also focused on meeting mandates outlined by the SEC and FINRA, and within the Dodd-Frank Act. These mandates involve market transparency, anti-money laundering and anti- bribery, as well as a variety of other risk categories. Dodd-Frank requires that firms maintain voice records for monitoring programs for a 5-year period.

FINRA 4511 books-and-records rules do not explicitly refer to voice recordings. It is noted only that records obligations include “communications relating to their ‘business as such,’ and include … customer account ledgers, securities records, order tickets and trade confirmations.” Voice is simply viewed in this context as another communications source.

One notable exception with FINRA is Rule 3170, otherwise known as the “Taping Rule.” This requires firms to supervise voice recordings when the firm or specific individuals have had past disciplinary issues that warrant closer inspection.

Beyond these wide-reaching regulations, there are other areas where the capture of voice communications is necessary. For example, in the UK the Senior Managers Regime holds senior staff accountable for the actions of their employees. Being uninformed of staff activities could result in dire consequences.

The benefits of enabling and capturing voice content

Monitoring voice calls for client satisfaction has been a longtime common practice in financial services. Organizations have typically administered this process through a traditional method: calls are recorded on a standalone platform, and then randomly chosen calls are listened to as a way of ascertaining client satisfaction. The reason only a small, randomly picked sample of calls is listened to is because of the sheer amount of time and resources this process takes. But by using this non-comprehensive method, important information is likely being missed. Newer capture and archiving technologies are capable of collecting and analyzing a large amount of this data, if not all of it, with fewer resources.

Capturing and analyzing voice data from client calls and sales pitches also enables businesses to detect potentially missed buyer-intent signals. Comparing this data across hundreds of calls could provide insights that inform sales approaches and product development. In addition, analysis of internal voice communications can provide businesses with a clear picture of effective collaboration between teams and the efficiency of specific projects and functions.

The unique challenges of capturing voice content

Voice technologies are well entrenched within financial services firms. These are most typically managed by telephony specialists that have dealt with multiple generations of PBX systems, trading turrets and early attempts at solutions for “unified communications.” For many firms, captured voice content has been managed within specialized platforms. While each of these voice-specific platforms offers rich feature sets, they also come with high licensing and support costs, complexity, and dated, inflexible on-premise architectures. This lack of flexibility becomes a challenge as firms look to embrace voice features within today’s collaborative platforms.

Capturing voice content: the alternatives

Siloed communications capture

For too long, many regulated firms have captured and stored voice communications through single-purpose, siloed products. These products were designed at a time when telephony teams were consumed by codecs and had to wrestle with voice and audio data extraction from legacy PBX systems. Operating these systems has required highly specialized expertise, which only rarely intersects with other communications domains such as email and instant messaging. As a result, electronic communications and voice content have remained fragmented — despite the promise of today’s “unified” communications. This highlights the need for a single pane of glass solution.

However, bringing voice and e-communications into a single unified compliance operation has been hampered by three main challenges:

1. Voice has been dealt with separately for a reason. Despite the convergence in technology, “voice” represents a technically diverse spectrum of channels that must be captured
2. Most incumbent enterprise archives were built for email and not for voice
3. Firms have had a hard time finding cost-effective and reliable methods to bring voice calls into their supervision workflows

Working with a siloed voice recorder and archive presents challenges for downstream compliance and e-discovery operations. The primary challenge is that many of the incumbent recorders can’t record voice from modern sources such as Microsoft Teams and Zoom. Even if they could, these voice calls are part of a larger ecosystem that includes collaboration through file sharing, group chats and meetings. Having separate archives would mean a disconnect between these channels of communication. Maintaining the context would be nearly impossible.

Addressing voice recordings reactively

A key difficulty in dealing with the capture and playback of voice recordings is the massive volume of information that is typically contained within each record. It becomes an insurmountable task to spot potential infractions among such magnitude of recordings. Simply put, the signal/noise ratio is not cost effective for some firms to ingest large volumes of historical voice content into high-performing content platforms. This is particularly the case if that voice recording is needed only for a specific event, such as e-discovery. In order to meet this scenario, AI/ML approaches are gaining traction in allowing firms to construct light indices over voice repositories in order to surface potentially responsive content. Once uncovered, that voice content can either be delivered to a case managed within an archive or directly to a legal review platform.

An integrated capture and archive solution

Considering the richness of collaboration offered by tools such as Microsoft Teams, Zoom and Slack, voice is just one aspect of their functionality. However, when you combine multiple features/ modalities of communications from multiple vendors, then you really begin to see the complexities this can introduce for a compliance or investigations team. The ability to have all electronic communications, including voice, in a single, easy to search archive reduces effort while also increasing productivity. It allows for the consolidation of supervision and e-discovery workflows across all communications in use by the business.

Additionally, recent improvements in the accuracy of transcription technologies enable firms to use voice files indexed in conjunction with transcripts to improve review efficiency. For example, an indexed transcript can be used to identify a potential policy infraction. Once that infraction is surfaced, a compliance supervisor can listen to the accompanying recording for additional context into that potential issue. This coupling of the transcript and voice file also allows for the voice recording to be tagged at the spot in the recording that contains the infraction. This can greatly reduce the manual effort required to review voice files.

Staying compliantly productive

It is key to select a voice capture and archiving vendor that understands the real challenges and burden placed on financial institutions when it comes to regulatory requirements. There is a balance between enabling the best of breed productivity tools and remaining compliant.

Given the complexity and data volume associated with new collaboration and conferencing technologies, the selection of the appropriate compliance technology platform is more important than ever. Firms need to have a unified view of their employees and the content sources they are using. This is in order to address the requirements outlined in MiFID II and elsewhere.

Voice and other electronic communications should be indexed, normalized and enabled for high-speed search — not only within the platform itself, but also in a manner that can feed other downstream applications. These applications include content surveillance and AI/ML tools that can help firms gain further visibility into risk and opportunities for service enhancement.

The collaboration, chat and conferencing technology spaces are exploding, especially considering the increase in remote workstations. Vendors like Microsoft and Zoom are introducing new voice-centric features into their collaboration tools every day. Today we are already capable of seeing a live transcript during a Microsoft Teams voice call. The ability to capture all this rich content is now more essential than ever.

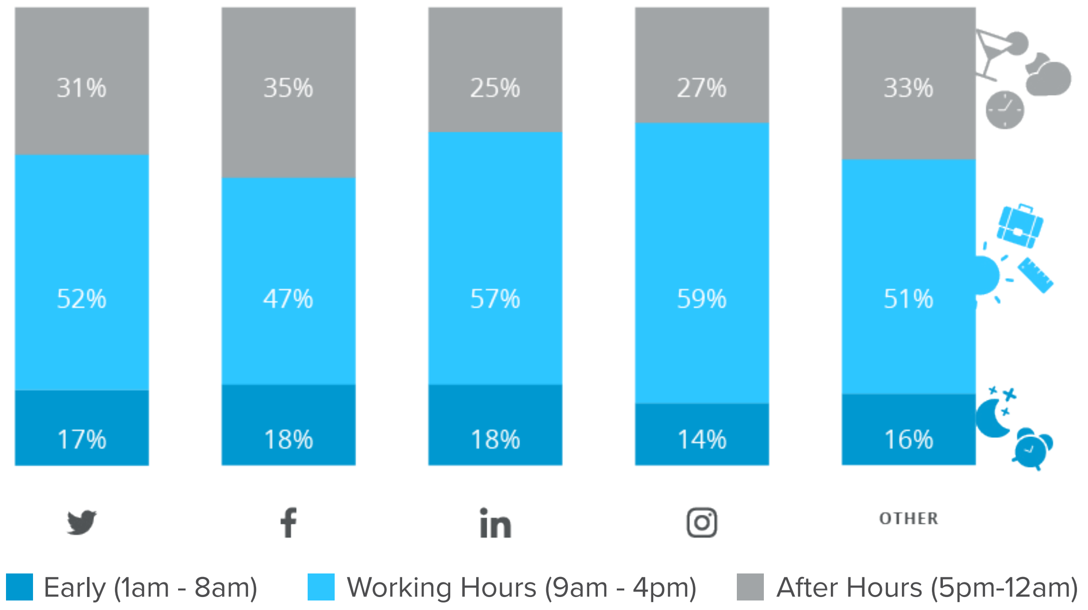
Firms have a choice between managing voice capture and playback with a mature, telephony-centric platform versus an integrated approach to voice. Where any one organization falls comes down to flexibility and innovation versus specialization and the familiarity of managing the voice legacy environment.

Flexibility will come by having the controls in place to embrace new voice-enabled features across all communications sources. This includes the growing use of voice assistants such as Alexa, Cortana and Google Assistant in the workplace. Innovation will come in the ability to unify voice alongside other messaging and collaborative data. This will enable firms to better understand the needs of their customers and respond to the dynamics of the markets they serve.

Chapter 6 - Social Media

Maintaining an active social media presence is now table stakes across most industries. More firms than ever are engaging clients and prospects on LinkedIn, Twitter, Facebook and other social networks.

The topic of social media is more than simply a question of enabling the appropriate level of social access to registered broker-dealers and financial advisors. "Always on" millennials are estimated to comprise half of the U.S. workforce today, and with them come the familiar social tools they are accustomed to using. These employees spend the majority of their online social media time during work hours. They may not always be aware of the line between the business and personal nature of the content they are posting, even if they indicate "tweets are my own."



Hootsuite[1]

This goes beyond an issue of demographics, however, as was highlighted by Elon Musk and his $20M tweet that ran into issues with the SEC and its Fair Disclosure Rule. Executives and any client-facing employees are only one inappropriate post or inebriated tweet away from causing damage to the firm. Businesses can reap all the benefits of social media. However, establishing guardrails that keep these activities from increasing risk exposure is paramount.

The days of social media being confined to the marketing team and company-sponsored websites are over. Every organization should be pursuing a company-wide initiative to integrate social media tools into all aspects of the business. They should also ensure that they have sufficient controls in place to manage this expansion in social media content.

For financial services, the use of social media can be broken into three distinct areas: social marketing, social selling and social advocacy.

Social marketing encompasses the broad areas of publishing content, customer service and social advertising.

Social selling relates to the empowerment of agents and advisors. It enables them to connect and engage with their clients, watching and listening for money-in-motion events to trigger sales opportunities.

Social advocacy provides the opportunity for all employees, specifically non-regulated employees, to champion company messages and act as brand advocates.

The benefits of enabling social media communications

Firms must consider two big-picture goals when using social media as part of an overall communications strategy: how it can increase revenue and how it can decrease expenses. Exploring both of these areas can help quantify social media objectives and measurements.

From a revenue perspective, social media can improve the way that businesses target specific life events for sales opportunities. It can also identify referral and cross-promotion opportunities. Many firms' customers want to use social media to communicate quickly and on the go. All these activities can lead to an increase in revenue with unparalleled efficiency.

Enabling registered reps and advisors to use social media to engage clients and prospects has clearly demonstrated these benefits. According to Putnam's Social Media Survey.[2]

- **92%** of reps and advisors who use social media for business say that it has helped them acquire new clients, up from **49%** in 2013
- **57%** indicate that social media has helped them initiate contact from referrals from existing clients
- **90%** of advisors say that social media plays a key role in their marketing efforts, up from **23%** in 2014

This data is also supported by Hootsuite research indicating that registered reps who use social media earn more than their colleagues who don't. "Simply creating a social profile is not enough. Zero percent of the advisors who have only a passive presence on social media gained new assets through social channels. Compare that to the highest achievers. They brought in average new assets under management of $15.3 million. Eighty percent of those high achievers pay for a premium level of service on a social network, rather than sticking only to free tools."[3]

In addition, social media can be a powerful tool for decreasing marketing and advertising expenses. The traditional mass dispersion technique can be replaced with targeted advertising to specific demographics. This approach reduces the volume of unsuccessful marketing materials. It is also considerably less expensive than traditional advertising. Furthermore, social media can be utilized as a recruitment tool and as an advocacy platform, which has been proven to boost job satisfaction and decrease employee turnover.

The unique challenges associated with social media content

The single most common challenge with social media that the financial services industry faces is how to remain compliant across all channels and conversations. While regulatory bodies have each issued their own specific guidance (for example, FINRA 11-39 and 17-18, SEC 204-2 and IIROC 11-0349), the common goal is to protect the investor.

Determining how social media can be used, such as which features to enable and which to disable, can produce a variety of interpretations of these rules. Some firms will limit the use of social only to specific actions like sharing one's LinkedIn profile. Others will conduct supervisory pre-review to inspect content before delivery and before hitting an immutable archive. Understanding the boundaries, therefore, is critically important and challenging.

One indisputable aspect is that any social media content that is allowed to be used for business purposes needs to be captured and archived by financial services firms. This can be difficult, especially for firms with multiple active corporate social media accounts and employee accounts.

Another challenge many businesses face is how to determine corporate policy regarding the use of social media by the organization as a whole. As previously referenced, social selling and social advocacy can be powerful forces for a firm's brand. However, it is not always easy to ensure employees are staying on message. While a social media policy should be common practice, businesses may also want to consider how best to enforce that policy. Tools that allow businesses to control access to social media features produce alerts, execute remediation actions, and moderate content are all factors that need to be considered.

The risks of enabling social media

There are inherent risks in allowing employees to use social media, which include both intentional and unintentional policy violations. These can span from a relatively minor entanglement issue to an incredibly serious compliance violation, including:

Regulatory compliance risk

While FINRA, SEC, MiFID II and other regulatory rules generally do not distinguish one communications source from another, there are specific considerations that apply to social media. FINRA Rules 11-39 and 17-18 both call out specific requirements for links to third-party sites, distinguishing personal communications as well as testimonials and endorsements. Suffice it to say, the choice of the appropriate method for social capture is vital to demonstrating adherence to pre- and post-archiving policy controls.

Data privacy risk

As with other sources, social content collection needs to tie to stated business or regulatory purposes that are outlined in policies. Complying with GDPR and CCPA obligations can be significantly more complex if firms allow users to co-mingle personal and business usage on a single network, such as Twitter.

DID YOU KNOW?

More than 511,000 tweets are sent *every minute.*[4]

InfoSec risk

Given its popularity, social media will remain a security target. Security risks common to social media include scams and identity theft. Exposures are also created by location sharing, as well as the use of schemes launched from bogus, unauthorized company sites. It is worth noting that FINRA recognizes cyber espionage as the single largest threat to financial firms.[5]

Discovery review risk

Courts have been consistent in stating that social media is simply another form of electronically stored information (ESI). It is subject to the same preservation and production requirements as any other responsive content. The discovery review risk of social media arises from its asynchronous, interactive nature. Capturing retweets, likes, shares and comments on initial posts can be critical to defending your firm in litigation. In fact, the Sedona Conference, a discovery industry advisor, emphasized the importance of capturing interactive social content with the appropriate tools that maintain conversational context.[6]

Internal policy risk

The reality of social media is that people are not always thinking of their firm's market dynamics when posting about a product or service. This could include comments that are misinterpreted as endorsements, tarnish their employer's brand or inappropriately disclose company confidential information. Without the appropriate tools in place to enforce policies, this could result in lengthy, resource-intensive audits, heavy fines and other sanctions for non-compliance.

Mitigating the risks of social media

There are four essential tools that businesses can use to mitigate the risks posed by social media:

1. Access controls

There are two methods for controlling the information posted on social media: 1) allowing read-only access, or 2) allowing selective access based on business need.

Keeping up with market-moving tweets and LinkedIn profiles can have a lot of business value. That said, unmanaged access can lead to productivity loss and compliance risks. By permitting read-only access, businesses can curb the loss in productivity while still providing their employees with access to the information.

Some businesses need to access a subset of social media features to conduct their work effectively. Social sellers need to be able to connect with clients and exchange messages. Social recruiters need to exchange messages with candidates. Social support teams must be able to respond to incoming tweets. However, social media also comes with unwanted features like job search capabilities and inappropriate content. With selective access, businesses can allow the features necessary for job performance, while blocking those that are not.

2. Alerts

There are two main concerns regulated businesses have with the use of social media: brand-damaging content and compliance violations. Products that allow businesses to build lexicon policies that search for keywords or regular expressions like social security numbers are power tools to combat these issues. When implemented, they proactively detect compliance risks, alert the employee attempting to post the content, and block the post. When the alerts are displayed, they provide the user with the explanation for why their post violates the policy, which helps to educate them for future postings. In highly regulated industries this is a crucial tool to help prevent the release of confidential information that carries serious legal and regulatory repercussions.

3. Remediation

Even when a business's protocols fail and something that violates their policy has made it onto social media, there is a way to mitigate the situation. While some damage may have already been done, the content does not have to live on in perpetuity. Remediation tools allow businesses to remove posts, comments or likes that violate their policy. For highly regulated industries, this tool, combined with a sophisticated capture solution, can both mitigate compliance violations and produce a record of corrective action.

4. Moderation

There are tools that provide businesses with the ability to manage all their social media accounts on one platform and set permissions at the employee level. They can also automatically detect and remove unwanted content. Businesses should consider a solution that allows manual moderation of content. Manual moderation allows employees to write a post, script a comment or initiate a like, but requires that it be reviewed prior to allowing it on social media. This workflow gives employees the tools to be productive using the most modern social platforms, without increasing the organization's risk exposure.

Capturing social media content: the alternatives

Regardless of industry, all businesses are concerned with the risks of allowing their employees to use social media. For highly regulated industries they must consider not only abuses of internal policies, but regulatory compliance violations as well. In the absence of controls to mitigate these risks, businesses must be able to show that they electronically captured violations and executed appropriate corrective actions. There are several options available for capturing or managing social media content for compliance purposes, including using a specialized capture solution. Here are some of the most popular:

1. **Prohibition policies:** Many businesses, especially those in non-regulated industries, use prohibition policies to manage social media usage. Some choose to prohibit the use of social media altogether, while others only prohibit certain channels or certain actions within channels. Businesses thinking about this strategy have several considerations:

    - How likely it is that their workforce will comply with the policy
    - If the policy is prescriptive enough
    - Whether the policy has been informed by all the stakeholders
    - If the policy enables employees or inhibits their productivity
    - If the policy is defensible to regulators (if regulatory obligations apply)

2. **Native features:** One of the key differences between out-of-the-box functionality and specialized capture solutions relates to *how* each captures content. The mechanisms provided to capture the unique conversational content, context and metadata that are produced on social channels must be carefully inspected. Each channel is different, and none are specialized to meet the unique requirements of highly regulated firms. If attempting to capture content directly via social media platforms, businesses should consider all the following:

    - The level of access via back-end APIs
    - What events are accessible for capture
    - How much historical content is accessible
    - What storage technology is used by the provider to ensure immutability
    - Data security and privacy
    - Notification procedures for API updates and enhancements

3. **Screen scraping and user data downloads:** A variety of rudimentary approaches to content capture exist, most of which are not suitable to the ongoing needs of regulated firms. Screen scraping can provide some utility in cases such as highlighting incidents of fraud or some other point-in-time event. However, the use of a screen grab is only slightly more useful than taking a picture of a social wall with your cellphone. Both fail to capture the interactive nature of social media. Similarly, relying upon users to download activities from a social network introduces opportunity for misuse or user error.

4. **Specialized, custom built or licensed connectors:** Some businesses take a one-off approach to each new communication channel that needs to be supported. They narrow their focus to thinking about capturing content from individual channels, rather than taking a broader view that encompasses all social media channels. This leads them either to contract a third party to develop a connection to the content source or to license an OTS product that provides the same capability. Businesses contemplating this strategy should consider the following:

    - Who will provide support for maintenance and disruption in the capture data flows
    - For OTS products, if they can continue to meet the needs of the business as the channels release updates and enhancements
    - How many other communication channels are currently supported
    - At what rate new channels are being added
    - Where the content will be archived, and if that archive can scale

The safest and most enduring of these specialized solutions for regulated organizations are automated capture technologies that provide social media connectors *alongside* support for other communication channels.

From baby boomers to millennials, society has fully embraced social media. Businesses that have failed to do the same are falling behind and potentially risking exposure. Modern businesses are using social media to increase their revenue with reduced overhead expenses while providing their customers the communication experience they've come to expect.

Even in highly regulated industries, with tools on the market to control access and usage, the adoption of social media doesn't have to carry increased risk. What all businesses must consider, however, is how they are going to manage the growing volume of communications and variety of channels.

Social media is undoubtedly a powerful tool for businesses. That said, managing the maintenance and addition of new channels while ensuring continued regulatory compliance is often too much to take on. For these reasons, a fully managed capture solution is highly recommended — preferably one with additional controls to manage, moderate and remediate content.

Chapter 6 - Social Media References:

1) https://hootsuite.com/research?businessSize=all&industry=all

2) https://www.putnam.com/advisor/business-building/social-media

3) https://blog.hootsuite.com/social-media-financial-services/

4) https://www.domo.com/learn/data-never-sleeps-7

5) https://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/corporate-espionage-risk-management-for-financial-institutions/

6) https://thesedonaconference.org/publication/Primer_on_Social_Media

Chapter 7 - What's Next

Capturing communications data comprehensively, natively, and with full context is a necessary component of protecting and advancing your firm. Where and how to store that information, how to monitor it and how to retrieve it are all aspects of what's next that we will consider in this chapter.

Captured content feeds downstream business processes

For firms in industries with regulatory retention requirements (e.g., financial services, healthcare, energy, utilities, government), the approach to capturing communications proactively and inclusively is vital in order to meet recordkeeping obligations.

Many industries also have archiving requirements that follow the spirit of SEC 17-a4. These state that a firm's communications must be stored to "minimize deterioration and prevent loss," as noted by the FDA CFR Title 21, Sec. 820.[1] Or, they require firms to develop procedures that "prevent unauthorized modification or deletion" of electronic requirements, as outlined by the United States Department of Energy Order 243.1B.[2] There are ongoing concerns over data breach, ransomware and other InfoSec threats. As a result, captured content must also be delivered to archiving locations with the appropriate security controls, chain-of-custody protections and third-party attestations.

Aside from those with explicit regulatory requirements, other firms are increasingly re-examining their ability to capture and store emerging content sources such as Microsoft Teams, Slack and mobile device content. They recognize that those networks are increasingly delivering information that is important to their business and acknowledge that they do satisfy their own internal records criteria. That realization is causing them to rethink the method of capture they utilize in order to satisfy their internal records retention policies.

Proactively capturing content and delivering it to a purpose-built, centrally controlled records archive also helps firms meet their information governance objectives. This includes:

- The ability to define retention policies that correspond to the value or risk of that data
- Enabling the systematic disposition of data that no longer has value to the business
- Implementing the controls and response to data privacy requirements, like enabling firms to respond to Rights of Access requests under GDPR, CCPA and similar mandates

One final aspect that firms should consider when examining how and where captured content is delivered is the need for that content for e-discovery and investigative work. Firms that employ reactive methods of discovery, such as the on-demand collection of content when faced with litigation, are increasingly arriving at the conclusion that these methods are not efficient.

Reactive content capture is also expensive and presents multiple points of failure. Firms cannot afford to wrestle with mobile carriers for historical phone records. They cannot afford the resources to use screen scraping, user downloads or a forensics tool to collect and deliver dynamic content to an email-oriented legal review tool every time litigation happens.

Choosing the appropriate capture and archiving technology is important. Organizations must be able to capture content securely. Then it must be delivered to archiving systems that can play back the unique content, context and metadata of each source. This will save firms time and legal review cost and remove many of the uncertainties of reactive methods of e-discovery.

The next network

Ultimately, processes and technologies to capture communications content will continue to be dynamic and evolving. Demographic changes mean that there will always be a new set of tools introduced to the business. These will reflect both employee familiarity and shifting client demands. Here are some of the dynamics of which firms should stay apprised:

Messaging/chat is attached to every application

The number of applications, devices and forums in which individuals can engage with clients will grow exponentially. Voice and video enablement will closely follow. Text-only tools are soon to become the dial-up, answering machine and floppy disks of the next generation.

Conferencing and collaboration tool features evolve in near real-time

The suddenly prolific use of virtual meeting tools has forever altered its pace of innovation. Existing market leaders will be joined (or supplanted) by others offering unique capabilities to improve productivity, speed up information retrieval and improve methods for API access required by regulated firms.

AI and ML continue to proliferate content

Sources will increasingly embed AI advances in the forms of virtual assistants, bots and decisioning engines within content sources.

The use of auto-classification technologies will grow

Firms will continue to embrace approaches to automate the classification of content in order to reduce the burden of assigning policies to multiple content sources manually.

Litigation and regulatory action will catch up, eventually

The big case involving collaboration or conferencing technology is bound to happen and will shake firms into taking the risks associated with these platforms seriously. It is better to be prepared than be forced to react.

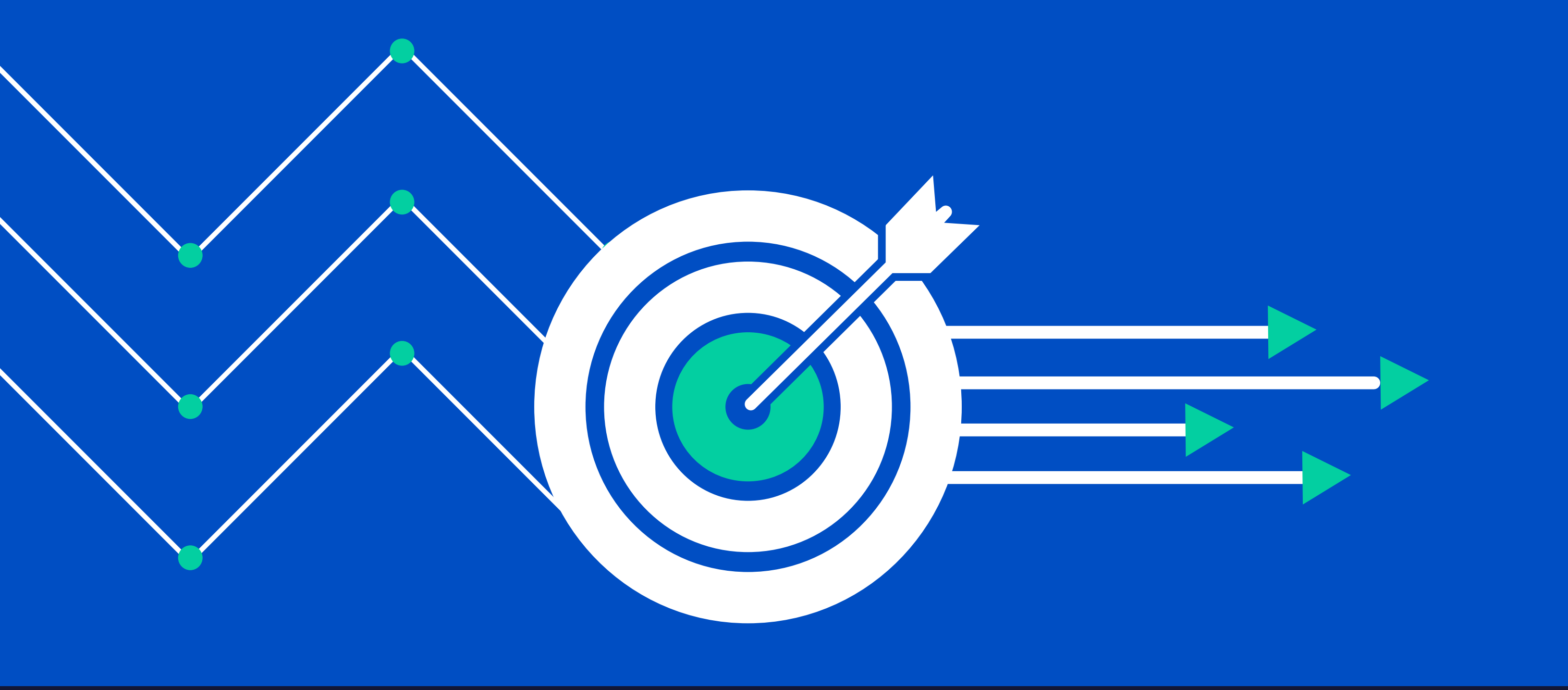
Physical to mobile to virtual

Let’s face it, you are the office. We have largely proven the ability to transition from a physical presence to a remote presence. There have been some growing pains and unforeseen challenges, but we appear to be emerging stronger as a result. What we thought would not happen until 2030 took place in the first three months of 2020. The next step, in some unknown form, is to have the ability to simply communicate and work wherever you are, untethered to a specific device or location. This is an intimidating concept, but one that is likely to arrive much sooner than we can imagine.

Chapter 7 - What's Next References:

1) https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?fr=820.180&SearchTerm=record%20retention

2) https://www.directives.doe.gov/directives-documents/200-series/0243.1-BOrder-b/@@images/file



Chapter 8 - Conclusion

It all starts with capture...

In an era of considerable uncertainty, businesses need an element of control. World events have caused firms to quickly react to the needs of a suddenly remote workforce. Absent other guidance, many will resort to using the communications tools with which they are familiar. These include chat, social, conferencing and mobile applications, some of which are better suited than others for use by a regulated firm.

At the same time, IT teams are seeking to leverage established technology standards. This might involve taking advantage of Microsoft Teams as part of their investment in the Microsoft 365 platform, or in combination with Slack, Zoom and other department-level favorites. Meanwhile, regulatory obligations remain a constant, data privacy laws are developing and potential policy infractions such as Slack bullying and textual harassment are entering the lexicons of HR and legal investigators.

To gain control, many firms are now extending their due diligence efforts to proactively inspect new communications tools before they permit their use within their firms. Increasingly, compliance teams are working closely with security, legal, IT and business stakeholders to weigh the benefits of new communications and collaboration tools against the risks.

Since each new tool is unique, risk mitigation must encompass a variety of factors. These include policy updates, user training and the availability of technologies that allow firms to automate policy enforcement to a level that satisfies the firm’s risk thresholds.

Fortunately, the right technology solution and partner for capturing complete and comprehensive communications data plays a vital role in this risk mitigation strategy.

The way forward with specialized capture technology

Specialized capture technology is designed to connect with all the networks in use by your business, today and tomorrow. With a solution like this, content is ingested directly and comprehensively from the source. Messages are captured in their original format, within fully threaded conversations and with all associated metadata. This level of visibility paints a complete picture of any interaction in question. And with a specialized capture solution, your business will stay prepared for inevitable new platforms and content types.

Specialized solutions also enable compliance teams to be proactive about risk. They can take advantage of ethical walls, feature blocking and data loss prevention capabilities and disclaimers, for example, as part of a comprehensive compliance program.

An equally important consideration for firms is the technology vendor they choose as a partner. The vendor must have strong partnerships and agreements with the electronic communications sector. They must consistently develop these relationships as new tools emerge. They should be experts in the area of compliance, to stay on top of evolving regulatory and legal needs.

Ultimately, a specialized, comprehensive and automated capture solution is good for business. Organizations can better manage compliance and other corporate risk because of the ability to quickly and thoroughly react to investigations or requests. Workers are empowered to safely use the communications tools and devices that they prefer, resulting in improved productivity and agility.

An additional bonus of using advanced capture technology is the wealth of business insight inherent in the data it collects. This information can help drive growth and provide a competitive advantage. Compliance teams, CCOs and other stakeholders can plan for potential challenges and how business strategy must adjust to meet them. With old tools and incomplete data sets, firms miss out on getting the full potential from their communications information.

The importance of a compliance program that can evolve with your business

Whichever option your organization chooses, it is crucial that your compliance program takes into consideration new channels, technological advances and emerging and evolving uses for captured data. While there are many unknowns, the proliferation of communications data is a trend that shows no sign of slowing down. Developing a strong communications compliance program — especially one that offers automation of key tasks — helps to protect and enable your organization.

Smarsh Products Overview

The Connected Suite™

The Smarsh Connected Suite provides everything your organization needs to achieve compliant productivity. Comprised of Connected Capture, the Connected Archive and seamlessly integrated Connected Apps, these industry-leading solutions from Smarsh empower your organization to face the evolving regulatory landscape with confidence.

Connected Capture™

Smarsh Connected Capture comprises content capture and management solutions across email, social, mobile, IM & collaboration and voice channels, available on-premise or in the cloud. Key differentiators of Connected Capture include the following:

Breadth of supported content

With support for 80+ communication channels out of the box and APIs for custom channels, Smarsh is the only provider that captures and manages such a wide variety of content.

Native, contextual capture

Smarsh captures content the right way. Unlike competitor solutions that flatten communications to email format, Smarsh captures all content natively in threaded conversational context. This includes point-in-time snapshots of joins, leaves, edits, deletes, comments, attachments and other events. Smarsh is also able to unify user identities across channels, giving businesses a full view of an employee's interactions.

Policies and alerts

With Smarsh Connected Capture, you can create lexicon policies to flag keywords, phrases and regular expressions and send real-time alerts to protect your sensitive information. Advanced capabilities such as ethical walls, feature blocking, redaction, remediation and disclaimers are also available for certain channels. These channels include Skype for Business, Webex Teams, Microsoft Teams, Cisco Jabber, Facebook, LinkedIn and others.

Once captured, your communications data can then be sent seamlessly to the Connected Archive — our secure, context-aware data store — or to any existing archive, application or data lake.

Connected Archive™

Smarsh has been the leading provider of archiving solutions for the past two decades. We have developed deep industry expertise serving clients of all sizes and complexity, from small businesses to the world's largest banks and government entities. With these distinct needs in mind, the Connected Archive comes in separate editions, each with a unique set of capabilities tailor-made to help you succeed. Unlike others' legacy solutions, Smarsh archiving solutions retain communications in their native format — with full conversational context — for the most effective possible review experience. Built for scale and to weather regulatory change, our archives grow and evolve seamlessly alongside your organization.

The Professional Archive

The Professional Archive is our comprehensive and user-friendly compliance platform built for small and mid-size organizations. Inclusive of capture, archive, supervision and e-discovery capabilities across 80+ communication channels, the Professional Archive will deliver unparalleled efficiency at your organization. A single pane of glass solution, the Professional Archive empowers you to efficiently review and search all of your electronic communications in one place. Support for new channels is continually being added, so your organization can implement innovative communication and collaboration technologies and stay ahead of regulatory change.

The Enterprise Archive

The Smarsh Enterprise Archive is designed for global enterprises with complex security, data privacy and regulatory obligations (including GDPR) and positions your organization for the future. It uses modern, web-scale technologies to ingest, search and export content orders of magnitude faster than legacy archives. All of your content is retained in full conversational context, helping you to reduce costs and increase productivity with the industry's most effective and efficient review experience. The Enterprise Archive is built to scale as your data volume grows, with no impact to platform performance.

The platform has been architected for the highest possible availability, with no single point of failure. As the only cloud-native archive, the Enterprise Archive protects your data with global "triple-active" configuration. Redundant copies of all data are stored across three availability zones. This means that customers benefit from high data availability and disaster protection at all times, with zero downtime or data loss for drastically lower risk and expenses.

The Enterprise Archive can be hosted on your choice of leading cloud infrastructures (Azure or AWS) almost anywhere in the world. It is also fully enabled to feed downstream applications for enhanced analytics, surveillance and business insights.

Connected Apps™

Smarsh offers two applications that integrate directly with the Connected Archive: Supervision and Discovery. These applications empower your organization to meet your compliance and legal challenges head-on. Both Supervision and Discovery applications come in Professional and Enterprise editions. Each one comes with a specialized set of capabilities and workflows. Enterprise Supervision can also be purchased as a stand-alone application. Smarsh Supervision and Discovery Apps both leverage the unique way that the Connected Archive preserves and displays communications data as threaded conversations — complete with metadata — for ultimate review effectiveness.

Supervision™

The Supervision App is a purpose-built solution designed for today's communications and regulations. The Smarsh customizable policy engine applies granular filters to employee communications to surface policy violations while reducing false positives. Your team can then collaborate on the efficient review of a high volume and variety of archived data, all retained in full conversational context. Our advanced reporting helps you to satisfy evidence of your supervision to auditors. Your organization can also gain vital insights from your supervised data through our open APIs and the ability to integrate our Supervision App with third-party applications.

Discovery™

The Discovery App is specifically designed to enable your organization to collect, preserve, review and export all of your electronic communications data on demand. Integrated with the Connected Archive, the Discovery App retains all your communications in their native format across 80+ channels complete with conversational context and metadata. You can then quickly and efficiently find and analyze essential content using powerful search, case management, legal hold and review tools. In addition, you can use the Smarsh Discovery App to extract insights from your data to make informed strategic decisions. Our open APIs enable you to easily share content with internal or external parties.

Solutions to meet the evolving needs of your business

Smarsh has architected its solutions specifically to be able to support your business as it evolves. Our products are equipped with open APIs for the ingestion, enrichment and export of content, meaning you can take advantage of integrations with third-party applications. Partnerships with the latest content sources and elastic scaling capabilities help you to stay one step ahead of risk within your communications. Additionally, flexible deployment options enable alignment of your capture and archiving solutions with your business's IT strategy as it develops. With Smarsh, your compliance team can meet regulatory obligations and enable your business today, and in the future.

For more information about our products, visit www.smarsh.com or contact your sales representative.

Additional Resources

Smarsh offers many valuable resources related to communications capture and your compliance program. Visit www.smarsh.com to find these tools and more:

- **Report:** Learn how other organizations are managing compliance in the Annual Electronic Communications Compliance Survey
- **Video:** More on how Smarsh handles capture for the enterprise
- **Blog:** What's next for compliance technology?
- **Assessment:** How is your firm managing compliance and productivity across mobile devices?
- **Guide:** Global Regulatory Communications Compliance Guide for Financial Services

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

☎ US: 1-866-762-7742 | UK: +44 (0) 20 3608 1209 www.smarsh.com @SmarshInc SmarshInc Company/Smarsh