smarsh®

ELECTRONIC COMMUNICATIONS COMPLIANCE SURVEY REPORT

2019

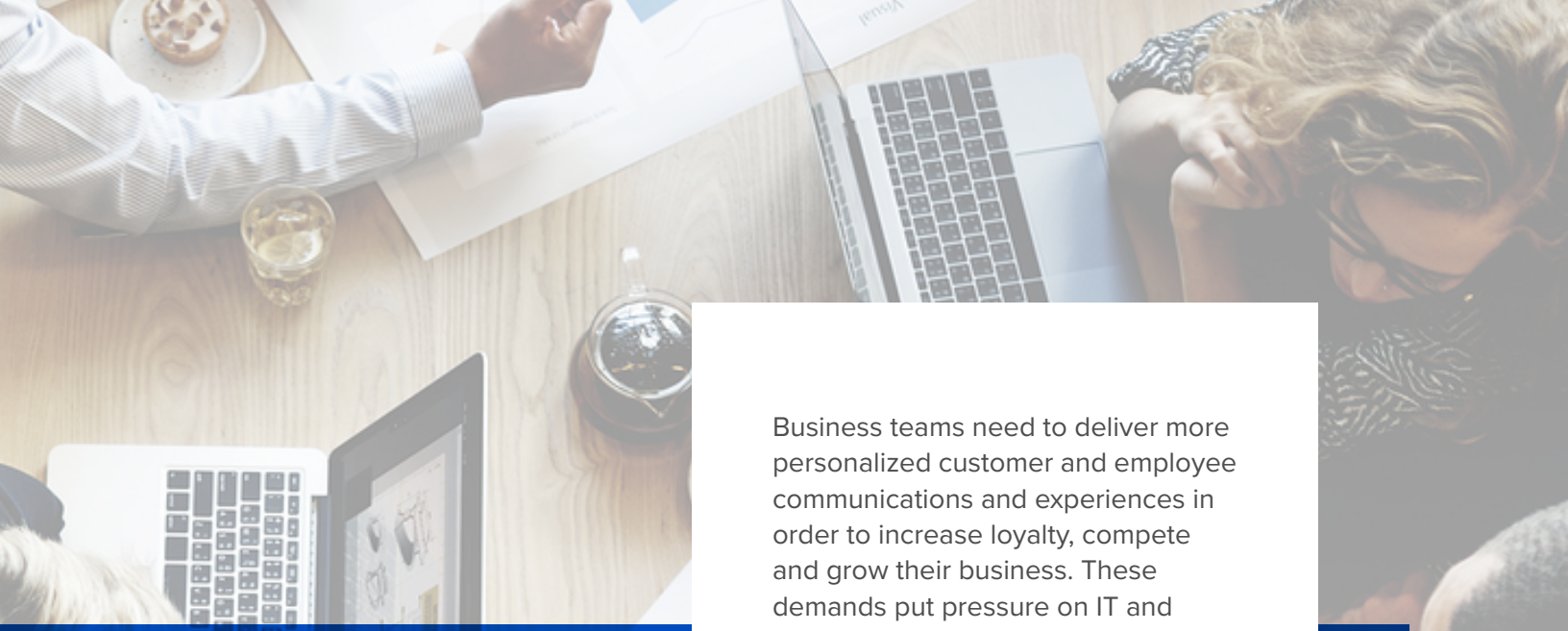


Table of Contents

Key Takeaways 3

Compliance teams have too few resources and can't keep up 4

Data volume, variety and velocity rapidly growing 5

Prohibition is no longer an option 6

01. Key Takeaway: To compete and grow, firms must embrace social, mobile and collaboration technologies 9

- Compliance Gap: Text/SMS messaging
- Compliance Gap: Collaboration tools
- Compliance Gap: Social networks

02. Key Takeaway: Like it or not, use of personal devices at work is now the standard 15

03. Key Takeaway: The archive is helping compliance move from a cost center to a value driver 16

Survey Methodology 18

Summary 19

Business teams need to deliver more personalized customer and employee communications and experiences in order to increase loyalty, compete and grow their business. These demands put pressure on IT and Compliance teams to expand the volume and variety of services they allow the organization to use.

Smarsh conducted a survey of financial services professionals responsible for the retention and oversight of electronic communications ("electronic communications compliance") to learn how these business requirements are impacting their ability to confidently manage risk.

For the purposes of this survey, "electronic communications compliance" refers to the supervision, protection and recordkeeping of electronic communications by an organization, as mandated in regulations such as SEC Rule 17a-3 and 17a-4, SEC Rule 204-2 and 206(4)-7, FINRA 2210, 2212-2216, 3110, 4511 and 4513, and CFTC Regulation 1.31. International regulations include MiFID (Markets in Financial Instruments Directive) II, the FCA's COBS 4, BCOBS2 and MCOB3, IIROC Rule 29.7, National Instrument 31-103 (Canada), the SFC Securities and Futures Rules and UMIR Policy 7.1.

About the Report

Data for this report was generated from a survey of over 300 IT and compliance leaders and practitioners, 81% who are personally responsible for Electronic Communication Compliance (ECC) and 6% who oversee ECC related activities.

81% Personally responsible
6% Oversee ECC
13% Not directly responsible for ECC

Respondents shared feedback on three key areas of electronic communication compliance:

- Compliance personnel
- Compliance policies, regulation and enforcement
- Systems, tools and processes

Key Takeaways

01. To compete and grow, firms must embrace emerging social, mobile and collaborative technologies

To hire the best talent and to communicate with a more sophisticated client and prospect base, employers must provide access to a growing number of applications for messaging, meetings and collaboration, or chase shadow IT. Respondents shared a few other interesting considerations about communication channels they are struggling to manage.

02. Like it or not, use of personal devices at work is now the standard

The trend of BYOD (Bring Your Own Device) has been an IT challenge for more than a decade but it now looks like there is no more debate. This year's results showed 74% of organizations allow employees to use personal devices at work.

03. Compliance is moving from a cost center to a value driver

Firms continue to make significant investments in compliance-specific technology and resources. The great news is that organizations are now getting more from those investments. More than 35% of respondents shared they leverage data from their archiving solution for non-examination purposes four or more times a year.

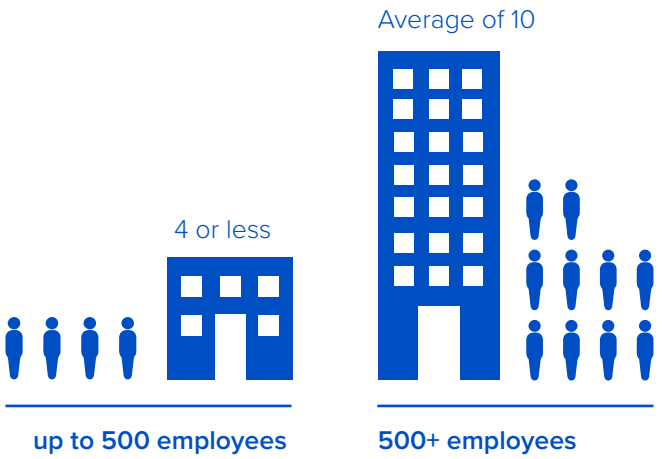
Compliance teams have too few resources and can't keep up

In this survey, organizations with up to 500 employees have four or fewer staff members performing supervision of electronic communications. Organizations with 500 or more employees had an average of 10 staff members doing work related to electronic communications compliance.

Yet, according to survey responses, 45% of respondents said that they are in constant catch-up mode, rather than proactive mode, when it comes to electronic communication compliance.

Without proper technology that automates the collection, preservation and review of increasingly diverse and growing volume, variety and velocity of data, organizations won't be able to fund a hiring plan that can keep pace with their business requirements.

COMPLIANCE STAFF MEMBERS



Top concerns related to electronic message compliance personnel:

- 45% feel they are constantly in catch-up mode rather than proactive mode
- 38% struggle to balance employee privacy considerations with oversight obligations
- 30% are concerned about personal accountability associated with electronic communications compliance

Data volume, variety and velocity rapidly growing

The massive scale utilization across every communication channel is staggering:

In its sixth edition of its "Data Never Sleeps" report, DOMO estimates that 1.7MB of data will be created every second for every person on earth by 2020[1]

According to Emarketer, the average person spends 55 minutes per day on their smartphones[2]

According to Time Is Ltd., employees are sending more than 200 Slack messages per week, with power users sending more than 1,000 per day[3]

While the volume of digital exhaust is overwhelming, managing risk is made even more complicated by how quickly business conversations shift from one channel to the next. An employee may start a conversation on LinkedIn, then move to email. A meeting will get booked using a meeting platform, and follow up or a quick reminder might be sent via chat. Attempting to prohibit the dynamic nature of these conversations could cause employees to circumvent the process, introducing additional risk in doing so.

Top concerns related to compliance policies, regulation and enforcement:

- 60% are concerned about fine-tuning supervision processes to find real risk
- 54% are concerned about understanding new and changing regulations for supervision practices across different types of messages and channels
- 40% are concerned about the complexity introduced by regulations or market dynamics (e.g., Brexit, GDPR)

1) https://www.socialmediatoday.com/news/how-much-data-is-generated-every-minute-infographic-1/525692/
2) https://www.emarketer.com/content/us-time-spent-with-mobile-2019
3) https://www.vox.com/recode/2019/5/1/18511575/productivity-slack-google-microsoft-facebook

Prohibition is no longer an option

Living the mantra of "if it can't be archived, it can't be used" is unrealistic, particularly as IT and Compliance teams must:

- Enable a workforce who want to use their preferred devices
- Meet the needs of a customer base that will only grow more tech-savvy as younger generations represent a larger portion of firm's revenue
- Reduce risks created by shadow IT, particularly as Software as a Service (SaaS) applications become more readily accessible
- Enable social and collaborative networks such as Microsoft Teams and Slack as sanctioned workplace communication channels

In parallel, the Compliance team must:

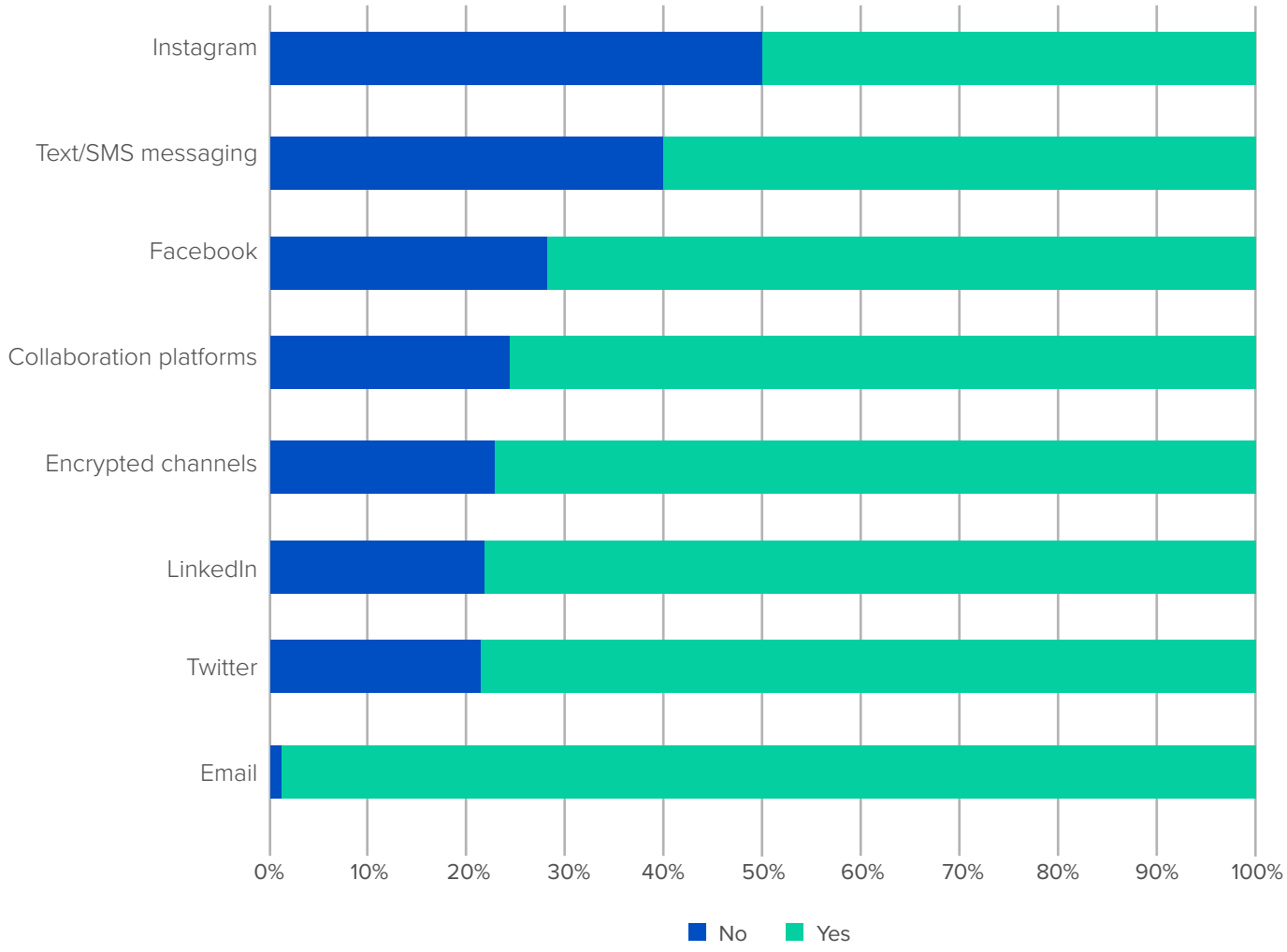
- Continuously update policy and written supervisory procedures to accommodate a higher volume of complex content from constantly-evolving channels
- Anticipate the likelihood that employees are using unauthorized technologies or channels
- Ensure they can respond to all data production requirements, beyond adhering to books and records obligations

Top concerns related to electronic message compliance systems, tools or processes:

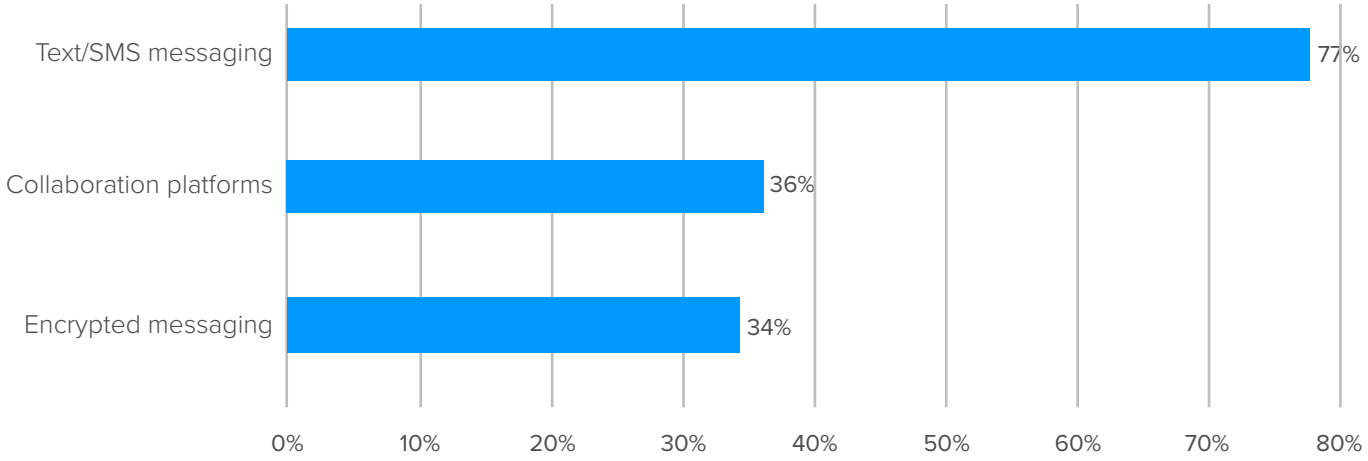
- Cyber security threats posed by the use of electronic messaging platforms
- Variety/volume of non-email communications channels (e.g., social media, text messaging)
- Variety/volume of mobile communications devices (e.g., smartphones, tablets)
- Security/capabilities of third-party vendors being used to manage data

Channels with the greatest compliance gaps

If allowed, is there an archiving/supervision solution in place?



Top three perceived sources of risk



01. Key Takeaway

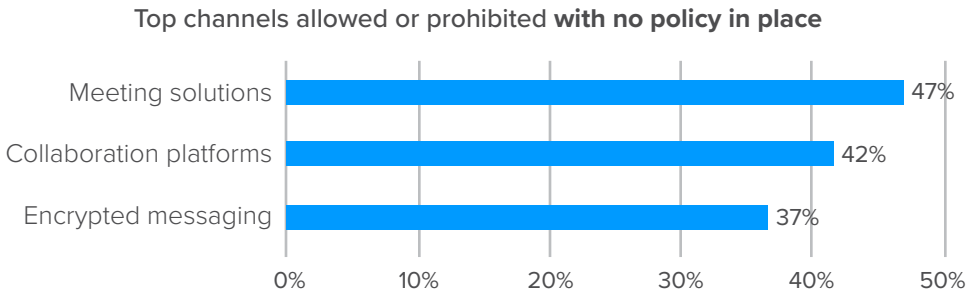
To compete and grow, firms must embrace social, mobile and collaboration technologies

To support their organization's ability to compete in tough markets, recruit the best employees and grow market share, the compliance team is under tremendous pressure to find solutions to capture, retain and monitor data associated with new communications applications and services, as well as adapt written guidelines around their usage.

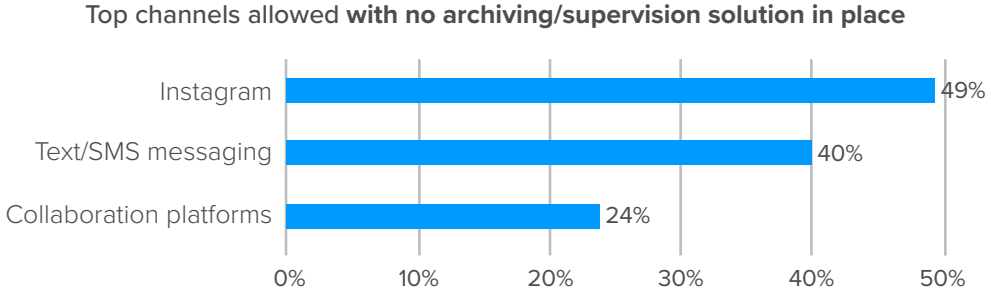
Business users continue to apply pressure to IT and compliance teams to support new social and collaborative networks, which are necessary to meet changing client demands as well as drive greater productivity across distributed teams.

As new, multi-modal networks (e.g. integrated voice, video, chats, application sharing, etc.) are requested or approved for use, compliance teams will need to keep pace with archiving and supervision standards. Survey data suggests that text messages, collaboration platform content and social media are primary sources of electronic communications compliance risk.

Nearly half of survey respondents (47%) have not established usage policies for meeting solutions, regardless of whether they allow or prohibit that channel for business communications. The same is true for collaboration platforms and encrypted messaging, where 42% for and 37% of respondents respectively have no usage policies in place for those channels.



While prohibition is not the answer, some firms face bigger challenges by allowing channels without archiving them: 49% who allow Instagram, 40% who use text/SMS messaging, and 24% who allow collaboration platforms, have no means of supplying associated communications data if required.



Compliance Gap: Text/SMS messaging

In December 2018, the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations issued a Risk Alert which stated "For purposes of this initiative, "electronic messaging" or "electronic communication" included written business communications conveyed electronically using, for example, **text/SMS messaging**, instant messaging, personal email, and personal or private messaging."[4]

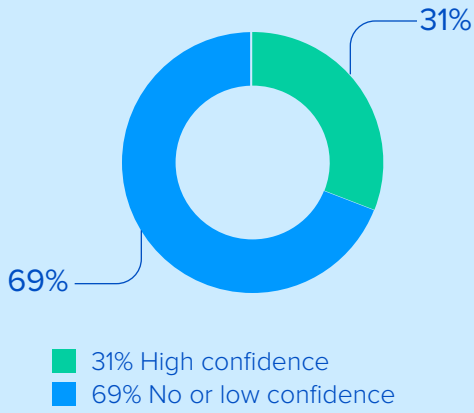
Despite the inclusion of these channels in the latest definition of electronic messaging, and the undeniable value of text/SMS messaging as a means of improving employee productivity and client communications, text/SMS messaging is a channel keeping compliance teams awake at night.

77% of survey respondents shared that this content type represents the greatest compliance risk – by far the most frequent response to the question, and **69% of respondents said they had low or no confidence** that, if examined, they could provide specifically-requested messages from SMS/text messaging channels within a reasonable time frame. Collaboration platforms came in a distant second, at 36%.

Beyond the confidence gap, the greatest risk is among the **40% of respondents who allow text/SMS messaging yet have no archiving or supervision in place**.

Yet, prohibition is clearly not an option: of those who said they don't currently permit text/SMS messaging, **54% have employees at their firms asking to use text/SMS applications** – by far the most requested channel.

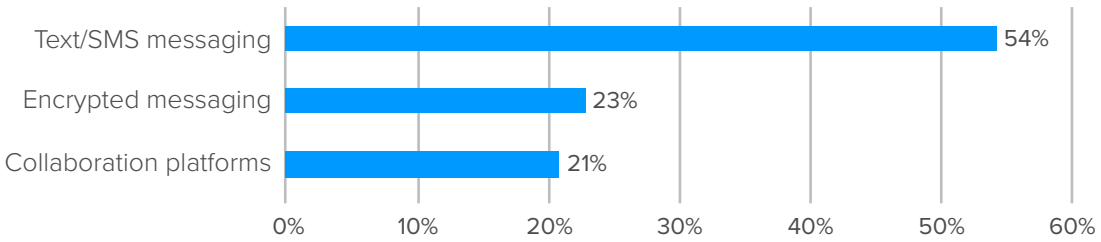
If examined, can you provide specifically-requested messages from SMS/text messaging channels within a reasonable time frame?



Pro Tip:
Providing access to text or SMS messaging can have a meaningful impact upon firm revenue and competitiveness. Firms are encouraged to archive text-originated content and develop the appropriate controls to drive the most value from these channels while managing the risk.

Suggested reading: *The Financial Firm's Guide to Compliant Text Messaging*

Top three prohibited channels requested by employees



4) https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf

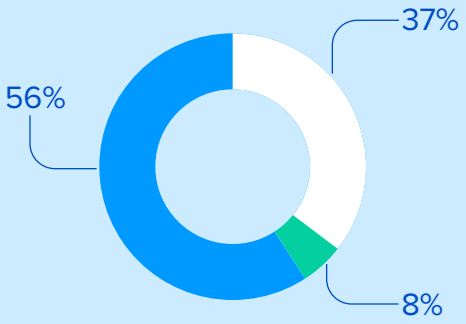
Managing the risk of encrypted messaging

Encrypted and ephemeral applications, including iMessage, What'sApp, WeChat and Snapchat, were not designed for business communications and can leave firms open to compliance vulnerabilities.

Of firms surveyed, **56% prohibit the use of these channels**, with written policies governing prohibition. Capture of these communications is problematic, though technology solutions evolve quickly. Although it is likely that some employees will find ways around those restrictions, it's important for firms to have a policy that clearly outlines whether channels are allowed or restricted. **37% of respondents did not have a written policy** governing the use or prohibition of these channels.

Interestingly, one-third of those surveyed said they were waiting for regulators to enforce regulatory guidance before they determine how they will provide support for use of those applications.

Encrypted channels compliance gap



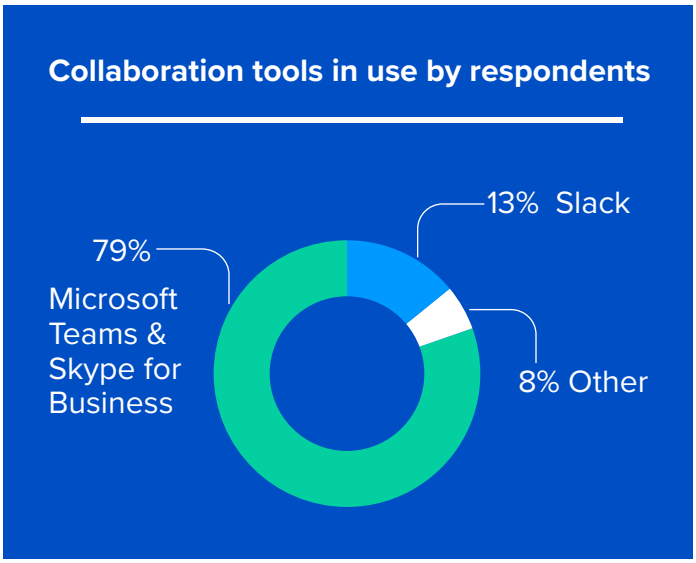
- 8% Allowed, written policy governing use
- 56% Prohibited, written policy governing prohibition
- 37% Allowed or prohibited, **no** written policy governing use

Pro Tip:
Until organizations have reliable technology solutions for compliant capture in place, they should evaluate alternatives to consumer applications which were not designed for business utilization. At the very least, firms must capture and archive all communication applications in use by employees..

Compliance Gap: Collaboration tools

According to a recent Gartner survey about Microsoft Office 365, Teams reflected the highest growth in adoption among Office 365 applications, with Microsoft now reporting that over 500,000 organizations are leveraging the platform. This is consistent with survey results which showed **79% of those respondents who allow the use of a collaboration platform have standardized on Microsoft products (Teams or Skype for Business)**.

Not to be outdone, Slack went through a very successful IPO in 2019, reporting over 600,000 clients; and 13% of respondents use it for their enterprise-wide collaboration platform making it the second highest collaboration platform in use.

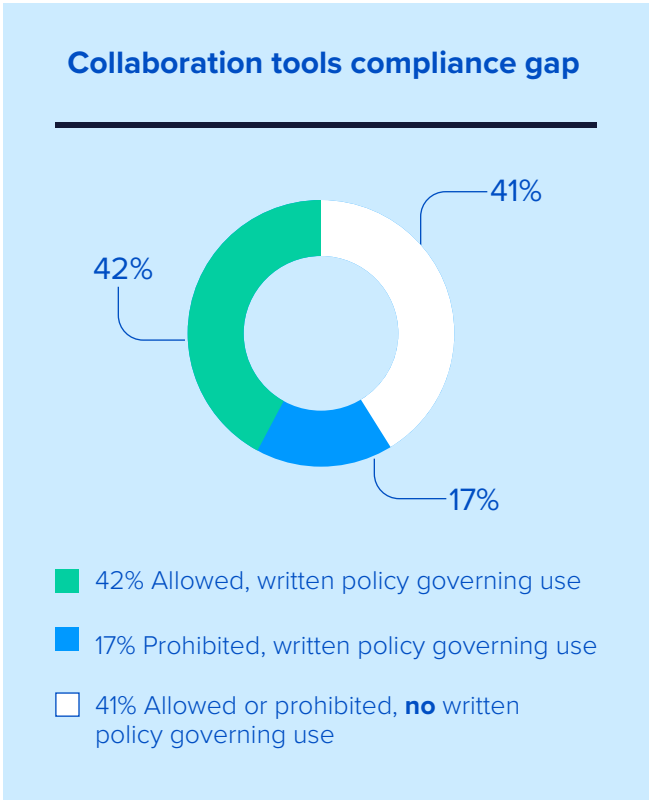


These channels are quickly becoming the "one stop shop" for a growing list of business applications, including instant chat, file sharing and storage, supporting diverse communication modes, including text, calls and video – with new integrations and capabilities being added every day. For example, through "auto upgrade" from Skype for Business to Microsoft Teams[5], Microsoft may be introducing a variety of new capabilities that Compliance teams should evaluate before enabling access to regulated users. It is critical to have a policy-driven lens around the use of these tools, given their dynamic nature.

Suggested reading: *Best Practices* for Stopping Risk, a guide to help you prepare strategies to tackle evolving forms of electronic communication.

A policy gap exists for the **41% of respondents who have no defined policy** to support usage or restriction, similar to the policy gap for encrypted messaging (37%).

Another concern is around the **17% of those surveyed who put policies in place prohibiting the channel**, assuming employees won't adopt a solution without understanding it falls within the restricted category.



Pro Tip:
The interactive nature of collaboration, along with the convergence of multiple communications tools like voice, video, app and document sharing introduce areas of potential risk that are not defined in policies written for email. Compliance teams should be active participants in the evaluation of features offered in new collaborative tools. Additionally, firms should take extra care in assessing interactive capabilities such as persistent chats that will complicate supervisory review in compliance tools designed for email and static messaging.

5) https://medium.com/@messageio/ready-to-auto-upgrade-skype-for-business-to-microsoft-teams-4c529a8ffc0

Where is collaboration taking place and what needs to be captured?

With the recent explosion in online meeting applications and successful market entries of companies like Zoom, it is clear that this is yet another emerging channel that requires compliance attention. And as platforms add modalities and capabilities, the meeting solutions and IM/collaboration platform categories are converging.

While some organizations use meeting solutions for live meetings, the platforms have evolved to support chat, file distribution, audio/video recording, and more.

Yet, of the nearly 42% who said they do have a policy governing use, less than a quarter (24%) of those have archiving or supervision processes in place associated with these applications. And, 33% of those surveyed say they allow the use of meeting applications without any restrictions or policy governing use.

Organizations will need to consider how to manage meeting applications that include live and recorded video and voice, as well as capabilities that have traditionally been included within unified communications solutions in order avoid gaps in their electronic communications compliance profile.

Which of these applications does your firm have a policy and retention or supervision strategy for?

- Microsoft Teams
- Slack
- Workplace by Facebook
- WebEx Teams
- Zoom

Pro Tip:
With regulatory guidance lacking for video meeting and unified communications capabilities, firms should be extra diligent to **1)** understand the native capabilities provided by each platform to capture content from each specific modality, and **2)** survey the ability of third-party solutions to fill the gaps

Compliance Gap: Social networks

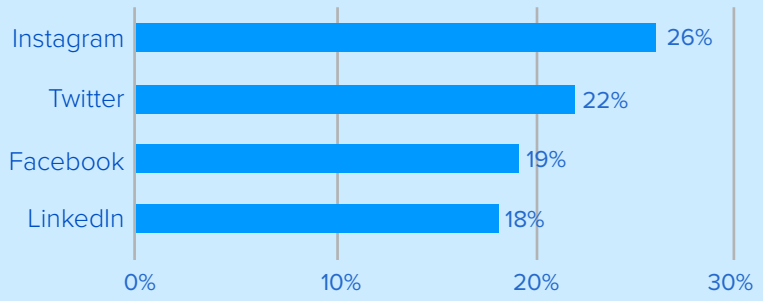
Leveraging social networks at work is a must for every organization. Marketing and sales teams, as well as human resources, are increasingly leveraging social media, including LinkedIn, Facebook, Instagram and Twitter, to amplify messages, connect with potential buyers and recruit employees.

It's also gotten the attention of regulators, who are casting wide nets around social channels. In the December 2018 Risk Alert from the OCIE, advisers are required to make and keep a copy of any communication that is circulated or distributed, directly or indirectly, to ten or more persons, "regardless of whether information is delivered in paper or electronic form, broker-dealers and investment advisers must reasonably supervise firm personnel with a view to preventing violations."

While the last six years have produced higher standards of social media compliance, with policy-creation and archiving on the increase, surprisingly, 44% of responders still prohibit the use of social networks, even though 10-14% of their employees are still requesting use of Twitter and LinkedIn.

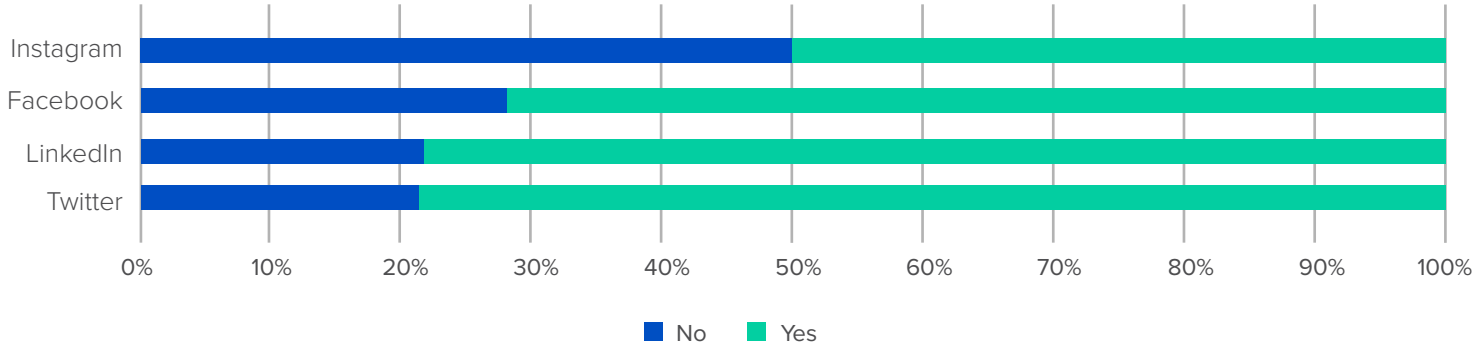
Suggested reading: *Texting and Social Media on SEC Radar*, Smarsh blog post by Marianna Shafir Esq.

Percentage of firms without policies for the following social channels



Pro Tip:
Don't assume that these channels are not being used or that employees understand the risks of using them, even in a very limited fashion. Involve the right stakeholders, including team members from marketing, sales, legal, HR, and IT departments; it's critical to create internal policies and processes that reflect today's evolving digital communications landscape, and to put solutions in place to capture the data from these channels at scale.

Social channel compliance gaps
If allowed, is there an archiving/supervision solution in place?



02. Key Takeaway

Like it or not, use of personal devices at work is now the standard

The past ten years saw the rise of Android and iOS mobile experiences, as well as an incredible growth of business-driven productivity applications brought to the mobile market. Research from Frost & Sullivan indicates that using portable devices for work tasks saves employees 58 minutes per day while increasing productivity by 34%[6].

In the past, teams would use prohibition of personal devices for work communications to cover their regulatory bases. Time and again, we've seen that this approach simply doesn't work. In fact, when asked about prohibited devices, **82% of responders who prohibit the use of devices for work communication felt little or no confidence they could prove adherence to their policy of prohibition**.

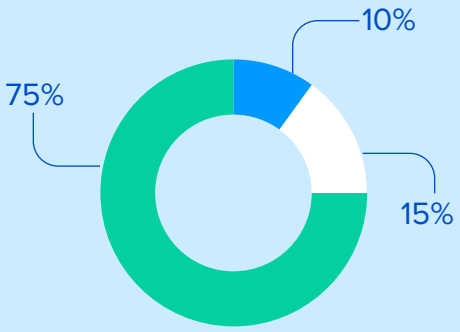
Today, firms have stopped trying to restrict employee demand for mobile devices in the workplace, and may appreciate the cost-savings that come with employees leveraging their personal devices. In fact, **75% of those surveyed allow a mix of personal and corporate-issued devices**.

While organizations have embraced BYOD, capturing and responding to all mobile business communication is not taken lightly by regulators. There is still a compliance gap associated with the applications running on those devices, in particular SMS/text messaging. Confidence that the organization is capturing and archiving all business communications sent via allowed mobile devices is not keeping pace. 44% of respondents lacked confidence in this area.

Suggested reading: *Managing Mobile Devices in the Workplace*

Pro Tip:
If the past few years have taught us nothing else, prohibition does not work, and in fact increases a firm's risk by effectively blinding it to the activities that will inevitably take place on commonly used prohibited channels. Organizations need to be able to support the latest mobility trends, whether they be BYOD, employer-provided devices, or a mixture of both — with the ability to capture a range of modalities (email, messaging, and collaboration applications). Without the right solutions in place to manage them, these mixed environments expose organizations to compliance and security risks.

What is the organization's policy on mobile devices



6) http://www.gscitsolutions.com/bring-your-own-device-byod-and-internet-of-things-iot-adoption/

03. Key Takeaway

The archive is helping compliance move from a cost center to a value driver

With the growing level of investment, not to mention an evolving threat landscape and the stakes of protection against it getting higher, the electronic communications archive must serve a growing need across the organization.

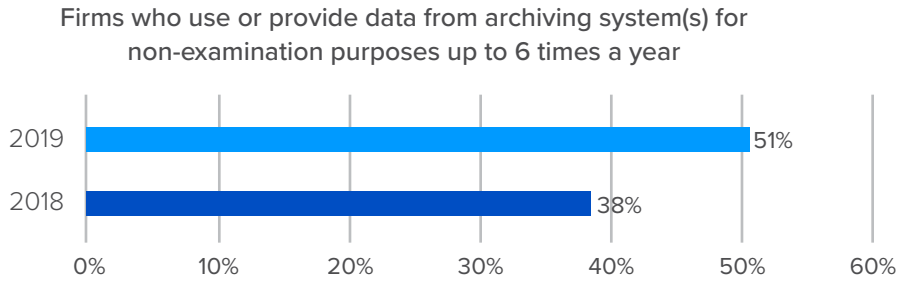
Compliance teams understand that much of what they do can help manage overall corporate risk alongside other departments including IT, marketing and HR. Data collected is now being leveraged far beyond audit/examination requirements, moving compliance from a cost center to a value driver.

The good news: when we compare 2018 and 2019 responses, we see increased leverage across all non-examination use cases being addressed with archived data. In particular, there was a **24% increase in the number of responders who say they leverage archived data to support legal discovery.**

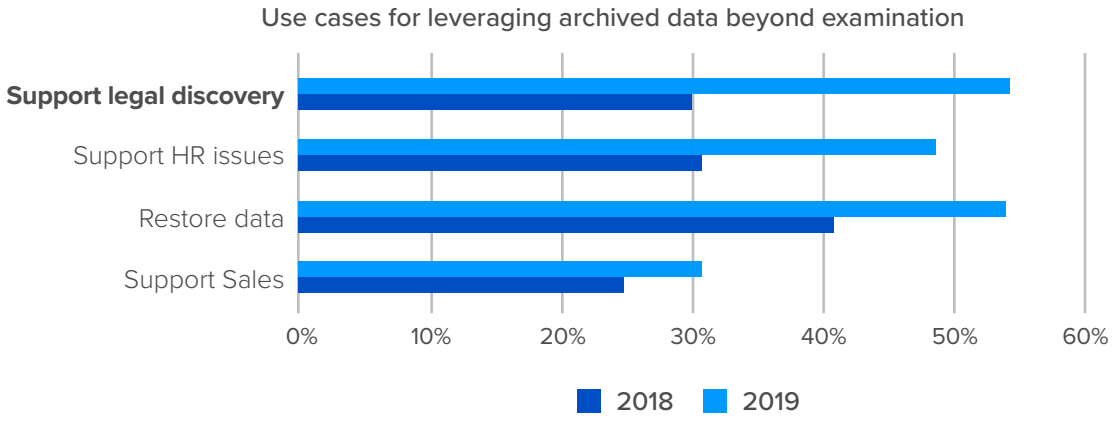
Beyond the improved identification of risks, firms are also recognizing that the creation of a centralized store of communications can also function as a revenue-building asset to the business, especially as providers leverage emerging artificial intelligence/machine learning capabilities. Stored communications can contain valuable insights into the needs and preferences of prospects and clients, and can be harvested to improve social media campaigns, messaging, and to equip sales teams with additional insights into their targeted firms.

Nearly half (47%) of respondents now believe that compliance is more than a cost/risk mitigation center; it can also contribute to top-line growth by maintaining valuable customer intelligence. This figure is up from prior year results, when an average of 39% of respondents in 2017 and 32% in 2018 provided use cases for archived data utilization.

Beyond restoring data, use cases included the support of HR or litigation issues, legal discovery or e-discovery requests, and even supporting sales and marketing efforts to generate new leads, analyze competitive activities or engagement behaviors.



Archived data can be incredibly effective to find potential violations of fraud, data privacy, human resources – as well as legal issues.



Six critical capabilities of an archiving and supervision technology system

1. Single platform for automated direct capture, ingestion, indexing, supervision and rapid retrieval across widest range of communications channels (email, IM, social media, etc.)

2. Search speed

3. Messages stay within native format (e.g., not converted into another content type, such as email)

4. Robust text message archival

5. Voice records archival

6. Examination/e-discovery assistance

*Responses based on which capabilities were essential when designing a comprehensive electronic message compliance program

Pro Tip:
Archiving data enables risk monitoring and the ability to document corrective actions taken. Leverage archive data to find early indicators of any wrongdoing such as the sharing of non-public information. Insider trading and anti-money laundering cases rely on proof of both the bad actions and the intent behind the actions; reinforcing the value and importance of capturing and archiving all electronic data. For example, Tweets can contain non-public information violating SEC rules, and LinkedIn posts can violate data privacy laws.

Survey Methodology

In 2019

Smarsh conducted a survey of 310 North America respondents who answered 36 questions from the following eight categories:

- Channels
- Archiving
- Devices
- Data production
- Supervision
- Compliance confidence
- Examination experiences
- Technology

Size of firms

Under 50 employees – **66%**

51-500 employees – **21%**

500+ employees – **13%**

Involvement with ECC

Under 50 employees – **66%**

51-500 employees – **21%**

500+ employees – **13%**

Types of firms

Broker-Dealer (BD)/financial network – **66%**

Registered Investment Advisor (RIA) – **39%**

Hedge fund – **15%**

Bank, Insurance or other – **12%**

Private equity firm – **7%**

Respondent Roles

Chief Compliance Officer – **26%**

Compliance department staff – **25%**

VP or C-level executive with compliance responsibilities – **13%**

Independent financial advisor – **10%**

Other, with compliance/supervisory responsibilities (please specify) – **10%**

IT support, DevOps or IT administration – **5%**

Branch or office manager – **5%**

VP or C-level executive in non-compliance role – **2%**

Compliance consultant – **2%**

IT security – **2%**

General counsel – **1%**

Survey Summary

Follow the lead of regulators and leverage technology to improve compliance and insights

Regulatory oversight is growing more sophisticated and the communications technology landscape continues to evolve. In 2020, many firms are planning ways to leapfrog competitors, unlock new market and customer opportunities, deepen understanding of customer preferences and behavior, and improve the overall positioning of the firm.

How can you manage the risk within your electronic communications, meet your regulatory obligations, and help pivot the compliance function from a cost function to one that helps grow the business? It starts with the ability to give employees the tools to communicate with customers and prospects using modern applications they want to use for conversations.

IT and Compliance teams need an aligned roadmap that allows them to:

- Embrace new and dynamic communication channels responsibly with use policies, and achieve efficient oversight across all channels with robust capture, archive and supervision technology
- Empower the mobile workforce while limiting the restrictions on message and collaboration applications on mobile devices they want to use

Archived data can efficiently strengthen compliance, recordkeeping, and e-discovery initiatives. Your records can be part of the best defense strategy, and they can also provide early warning signals of potential violations from channels that have evolved to offer new capabilities. The value of archived data can also be extended to use cases beyond regulatory examinations.

With cross-functional collaboration, the right technology and technology partners, and sound policies and procedures, you can help your firm stay ahead of the regulatory environment and grow its business.

About Smarsh

Smarsh helps financial services organizations get ahead – and stay ahead – of the risk within their electronic communications. Smarsh has established the industry standard for the efficient review and production of content from the diverse range of channels that organizations now use to communicate. With innovative capture, archiving and monitoring solutions that extend across the industry's widest breadth of channels, customers can leverage the productivity benefits of email, social media, mobile/text messaging, instant messaging/collaboration, websites and voice while efficiently strengthening their compliance and e-discovery initiatives.

A global client base, including the top 10 banks in the United States and the largest banks in Europe, Canada and Asia, manages billions of conversations each month with the Smarsh Connected Suite. The company is headquartered in Portland, Ore. with nine offices worldwide, including locations in Silicon Valley, New York, London and Bangalore, India. For more information, visit www.smarsh.com.