WEBINAR BRIEF

Tackling the Challenges of Off-Channel Communications

Modernize e-discovery, overcome compliance hurdles and comply with DOJ requirements

smarsh | exterro

Introduction

In a world dominated by technological collaboration, financial services professionals communicate and move from channel to channel all day long. With regulators hyper-fixated on off-channel communications violations, managing the risks associated with "channel surfing" has become a modern regulatory challenge many firms are not equipped to handle.

> ### Before we dive too deep...
>
> Definitions matter and how terms are used across media is not always correct or aligned. To be clear, here is how we define off-channel communications.
>
> **Off-channel communications refer to the use of unofficial or unapproved digital tools for business-related interactions**

Off-channel communications have drawn significant attention from regulatory bodies like the SEC. From a regulatory perspective, the biggest concern hinges on a firm's ability to monitor for possible misbehavior within these unapproved channels. The SEC has heavily emphasized the need for robust control over approved communication tools that facilitate thorough investigations, regulatory interactions, e-discovery, and historical recordkeeping.

Off-channel communications violations have also caught the attention of the DOJ, making this a wider-reaching compliance issue that spans industries. The DOJ's interest around off-channel communications stems from growing concern over the use of personal devices and third-party messaging applications. Over the years, the DOJ has observed the use of these applications contributing preservation issues impeding investigations, informing the DOJ's latest guidance on their use.

This brief is based on a discussion from the webinar, "Overcoming Compliance Hurdles: Addressing Off-Channel Communications Records Management." Our panelists delved into the multifaceted challenges and implications of off-channel communications within business environments, with a focus on regulatory compliance and operational integrity.

Our panel of experts:

Robert Cruz
VP of Regulatory and Information Governance at Smarsh

Brad Harris
VP of Solutions at Exterro

Matt Kelly
Editor and CEO at Radical Compliance

The conversation highlighted three primary drivers for the proliferation of off-channel communications:

1. Rapid evolution and personal integration of new communication technologies
2. Client preferences pushing firms toward specific tools
3. Attempts by individuals to evade oversight and detection

This complexity is further amplified by the widespread adoption of remote and hybrid work models, making traditional monitoring and compliance more challenging.

Challenges in an evolving landscape

There's a seemingly endless variety of communications tools available today. Organizations must monitor their current collaboration technology stack and stay vigilant for new and unapproved tools circulating amongst employees. So, what do you do? Prohibit all new and existing tools outside your current list of permitted channels? Not if you want good employee morale, better communication with clients, or to stay ahead of the competition. Being too loose with channel restrictions is a recipe for disaster, but being too rigid is detrimental in other ways.

Our panelists agreed that consequence management and transparency with employees are key. There's also a great need to reiterate what employees can and cannot do when it comes to their business communications across different channels.

Finding the right balance

There is a great need to balance the focus between technology solutions and fostering a corporate culture that prioritizes the use of business communications channels. A balanced approach in this situation requires that an organization leverage technology to monitor communications while also instilling policies and training that underscore the significance of using approved platforms for business matters.

Firms should not consider this topic solely in terms of apps but also other tools, such as project management tools like Asana and ticketing systems like ServiceNow, Jira, Atlassian, or Confluence.

"You might be using your own phone to make dinner plans and that's okay. But you should not speculate about your client's market trading strategies with your coworkers on iMessage or Snapchat. [That's] not okay."

— Matt Kelly, Editor and CEO at Radical Compliance

With an evolving landscape of communication and technology, there's a fundamental shift across industries to embrace collaborative technologies that blend many functions — further complicating the task of supervision.

Strategies for managing off-channel communications

Overall, there is a critical need for companies to adapt their strategies, acknowledging that perfect control over communications is unattainable.

To stay ahead of regulatory change and mitigate off-channel risks, firms must:

- Embrace change by adopting technology to monitor communications
- Educate employees by instituting training and policies to encourage the use of approved channels
- Develop a corporate culture that underscores the importance of compliance and proper use of communication tools

"All of these various tools now are embedding the ability to chat with other users within these applications. So, I think about the challenge being much more broad than just about specific applications."

— Brad Harris, Vice President of Solutions at Exterro

To mitigate risks from off-channel communications, forward-thinking companies must blend technology solutions, cultural shifts, and policy enforcement to ensure compliance and maintain business integrity in a digital, decentralized work environment.

Actions speak louder than words

Exterro has been doing an annual survey of judges to solicit their thoughts on trends and directions, and their most recent survey of over 400 judges highlighted issues of data spoliation becoming more prolific, with text messages, mobile devices, and social media at the top of the chart.

Harris noted that "judges are becoming more aware of these types of issues, not only because litigants are bringing these issues to the court for resolution, but also just being aware to ask these types of questions."

This shift underscores the increasing complexity legal and compliance teams face in preserving data and responding to regulatory, privacy, and discovery requests. Something that cannot be overstated is the importance of choosing effective tools and strategies for data collection and preservation. Far too many firms experience the pitfalls of relying on methods that may fail to capture dynamic and collaborative data sources. Moreover, the multifaceted nature of the issue means various organizational functions such as legal, privacy, compliance, technology, and operational units will all need to be involved in managing it. The complexity of devising a comprehensive management strategy should not go unnoticed.

Furthermore, firms must watch and review regulatory enforcement trends. For example, the Securities and Exchange Commission's (SEC) approach to changing industry behaviors toward compliance through enforcement. The SEC has mentioned the need for firms to cooperate with regulators and proactively engage when issues are identified to mitigate risks and penalties.

In recent years, companies have adjusted to new regulatory realities and remote/hybrid work, including changes in approved communication tools and policies. The shift towards more controlled and compliant communication practices reflects an ongoing reevaluation of risk and compliance strategies in light of evolving technological and regulatory landscapes.

Implications for the Department of Justice's ECCP

In 2023, the DOJ updated its Evaluation of Corporate Compliance Programs (ECCP) to emphasize the importance of managing off-channel communications within corporate compliance frameworks. While the SEC has specific rules for financial companies to preserve all business communications, the DOJ's focus spans across industries, emphasizing the expectation for all corporations to rigorously adopt the guidelines, especially in handling off-channel communications and enforcing consequence management.

Matt Kelly, Founder of Radical Compliance, has written extensively on regulatory action, including SEC actions and US DOJ statements. He noted that the requirement to hire independent consultants to examine compliance programs could be "exacting and onerous" given their wide-ranging purview over surveillance programs, technologies used, training programs, records preservation, and how firms manage enforcement.

The updated guidelines emphasize the need for corporations to demonstrate diligent management of off-channel messaging risks to satisfy DOJ expectations without strictly mandating the prohibition of such apps. Our panelists advocated for clear communication of policies to employees. They underscored the significance of implementing effective consequence management practices, including financial penalties for policy violations, to ensure compliance. Additionally, Harris indicated that one of the more significant implications of the focus on off-channel will be to pull different disciplines within an organization into these discussions.

"Do more senior executives get harsher penalties because they should know better? Do lower-level people who are repeat offenders also get harsher penalties because they're repeat offenders? That is going to be onerous for a lot of companies."

— Matt Kelly, Editor and CEO at Radical Compliance

"It's not just your compliance department, your legal department for litigation, your cybersecurity team for cyber breaches. These various disciplines are gaining knowledge and awareness of these activities."

— Brad Harris, Vice President of Solutions at Exterro

Generative AI could be the future of litigation

Firms should understand the inevitable integration of generative AI in communication platforms (e.g., Copilot in Microsoft Teams) and how this impacts their business moving forward. The DOJ's interest in how companies manage unapproved communication tools is not a trend, and firms must make greater efforts for control.

Advanced technologies could prove highly useful for litigation and regulatory responses. AI's potential to improve discovery processes by identifying communication gaps and unapproved message exchanges is going to be game-changing. On the flip side, if companies do not enhance their compliance and discovery practices in response to evolving technology, they are destined to fall behind.

What are firms doing to address off-channel communications risks?

Companies must take proactive measures to address off-channel communications risks. Within financial services, firms are adapting to mitigate risks associated with non-compliant communication practices.

It starts with policies

Implementing clear policies regarding acceptable communication tools and conducting thorough IT surveillance to detect unauthorized channels is a must. It is also very important to instill awareness among employees about the consequences of policy violations.

Additionally, information sharing and capturing across different organizational disciplines to enhance regulatory response and preparedness for litigation and privacy challenges is a necessity. Understanding behavior patterns, embracing technological advancements in approved tools, and maintaining vigilance over off-channel communications are critical. The key is a collaborative effort integrating policy, technology, and training to effectively manage and mitigate the risks of non-compliance.

It's worth noting that the selection of communication tools must consider the ability to create and preserve historical records for defensibility purposes. Lastly, experts highly recommend data mapping as an ongoing exercise, engaging various organizational disciplines to identify and mitigate potential regulatory risks posed by shadow IT applications.

If firms stop looking forward, they will fall behind

Being innovative or future-focused does not mean adopting new technologies and permitting new channels nonstop with little or no regard for regulatory requirements. That would open the organization to huge fines for infractions. However, being too rigid in processes and collaboration technology can act as a hindrance to progress, not a protection from regulatory risk. The balancing act is not about technology or regulations directly, it's about communication. Firms must understand that permitting and prohibiting channels should be based on whether the use of a channel improves internal and/or external communications. If the answer is yes, then that channel must be vetted to ensure employee use remains compliant within legal and regulatory requirements.

This brief is in partnership with Exterro.

exterro®

Exterro provides busy legal and IT leaders powerful technology solutions to navigate complex data risks successfully. Built on the industry's only data risk management platform, our software suite gives organizations the power to manage the interconnected requirements of e-discovery, privacy compliance, data governance, digital forensic investigations, and cybersecurity response operations all in one place. Our software is used by thousands of industry-leading businesses, government agencies and law firms across the world.

877-398-3776 | www.exterro.com | 𝕏 @Exterro | Exterro | Company/exterro

smarsh®

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

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

Brief - 07/24

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