CORPORATECOUNSEL

Mitigating Off-Channel Communications: A Guide for In-House Counsel and Compliance Professionals

August 20th, 2024

By Ken Koch, BDO USA, and Tim Nagy, Mayer Brown

Off-channel communications—those that occur outside of approved corporate systems—can pose a considerable challenge for regulatory compliance, data security and overall business integrity.

The rise of digital communication tools has transformed how employees interact within organizations. However, with the convenience of third-party apps like WhatsApp, WeChat and personal text messages comes significant compliance risks. Off-channel communications—those that occur outside of approved corporate systems—can pose a considerable challenge for regulatory compliance, data security and overall business integrity. This article delves into the complexities of off-channel communications, exploring employee behaviors, storage of communications, and strategies for in-house counsel and compliance/risk professionals to consider in addressing this pervasive issue.

The Problem: Employees Are Using Third-Party Communication Channels to Conduct Business

Off-channel communications refer to the use of unauthorized or unmonitored platforms for business-related communications. Despite policies dictating the use of corporate communication tools, employees often resort to personal messaging apps for various reasons, including convenience, speed and familiarity. This can expose organizations to significant risks, including:

- Regulatory Noncompliance: Regulatory bodies including the SEC, CFTC, HHS, FDA, FCC, FTC, FERC, NERC, and others mandate that companies maintain comprehensive records of business-related communications. Failure to do so can result in hefty fines and legal penalties. (See, e.g., Press Release, U.S. Securities and Exchange Commission, Sixteen Firms to Pay More than $81 Million Combined to Settle Charges for Widespread Recordkeeping Failures (Feb. 9, 2024), https://www.sec.gov/newsroom/press-releases/2024-18; Release No. 8599-22, Commodity Futures Trading Commission, CFTC Orders 11 Financial Institutions to Pay Over $710 Million for Recordkeeping and Supervision Failures for Widespread Use of Unapproved Communication Methods (Sept. 27, 2022), https://www.cftc.gov/PressRoom/PressReleases/8599-22).
- Data Security Threats: Using unmonitored platforms increases the risk of data breaches. Sensitive business information may be exposed to unauthorized access, leading to potential data loss or theft.
- Reputational Damage: Noncompliance and data breaches can significantly damage an organization’s reputation, eroding trust with clients, partners, and stakeholders.

- Operational Inefficiencies: Managing multiple communication channels without a centralized system can lead to inefficiencies and hinder effective communication within the organization. It can also impact completeness and timeliness in responding to a document request or subpoena.

Understanding Employee Communication Behaviors

Employees today have access to a myriad of communication tools, from corporate emails and internal messaging platforms to third-party apps like WhatsApp and WeChat. Despite clear policies, employees may use off-channel communications for several reasons:

- Convenience and Familiarity: Personal messaging apps are often more user-friendly and familiar, making them an easy choice for quick communication.

- Perceived Efficiency: Employees might believe that these apps allow for faster and more efficient communication, particularly in fast-paced environments.

- Accessibility: With the rise of remote work and BYOD (Bring Your Own Device) policies, employees are increasingly using their personal devices for work purposes, often toggling between personal and professional communications.

Understanding these behaviors is crucial for developing effective strategies to manage off-channel communications. It’s important to recognize that employees are not necessarily acting out of malice or disregard, but rather out of a desire to perform their jobs more efficiently—they want to get things done. Sometimes, the complexity of enterprise-level systems and the way they are deployed within a company can increase the time it takes to complete work, and that can stifle enthusiasm and the sense of urgency employees may have had at some point. Gaining real insight into the psychology of how employees communicate can guide the development of policies and solutions that address the root causes of off-channel communications.

Where Are the Communications Stored?

Understanding where and how communications are stored is crucial for compliance. Also, there are dozens of configuration options for how long those communications are stored. It’s critical to understand these variables in designing and implementing a compliant program. Here’s an overview of common platforms with default configurations:

- WhatsApp: On iPhones, without iCloud enabled, messages are stored locally on the device. When iCloud backup is enabled, messages are backed up to the user’s iCloud account. For Android devices, WhatsApp messages are saved in the internal storage under the “WhatsApp/Databases” directory. Cloud backups can be configured to Google Drive for Android or iCloud for iOS. This means that if these communications are not backed up to a company-managed cloud service, they could be lost if the device is damaged or data is deleted.

- WeChat: Messages are stored locally within the app’s data directory on both Android and iOS devices. WeChat does not store chat data on its servers unless explicitly backed up by the user. This local storage can be problematic if the communications need to be retrieved for compliance or legal reasons and are not properly backed up.

- SMS and iMessage: SMS messages are stored on the device itself and can be backed up to cloud services like iCloud for iPhone users. iMessage data is encrypted and stored within Apple's ecosystem. However, if these messages are not part of the company's archiving system, they might not be captured for compliance purposes.

Addressing the Issue: What Can We Realistically Do to Solve This Problem?

Solving the problem of off-channel communications involves a multi-pronged approach, integrating policy, technology, and culture change. Spoiler alert: it's not easy.

Policy Development and Enforcement

- Clear Communication Policies: Establish and enforce policies that specify approved communication channels. Document procedures for capturing and archiving communications from all permitted channels. These policies should be clear, concise, and communicated effectively to all employees. Regular updates and reminders can help ensure that everyone is aware of the current policies.

- BYOD Policies: Clearly define guidelines for BYOD usage to ensure that personal devices used for business communications comply with company policies and regulatory requirements. This includes installing monitoring and archiving software on personal devices used for work purposes, ensuring that all business communications are captured.

- Exceptions: in some cases, there may still be situations where communications occur in a third-party channel. Ensure there is policy to address the treatment of those messages when they occur and have a mechanism in place to get those communications into the company system.

Technological Solutions

Effective technology solutions are essential for managing off-channel communications. Here are some key components to consider:

- Real-Time Capture and Archiving: Ensure the technology can capture messages in real time and archive them securely. This prevents any data loss and ensures all communications are stored in compliance with regulations.

- Advanced Search and Retrieval: The solution should offer advanced search capabilities, allowing for quick retrieval of specific communications from multiple channels. This is crucial for compliance audits and legal investigations.

- Compliance with Regulatory Standards: Ensure the technology complies with relevant industry regulations regarding data retention and privacy. This is critical for avoiding fines and ensuring that all business communications are legally compliant.

Unfortunately, there is no individual software platform that addresses everything organizations need. Here are a few different categories of software that will certainly help you contribute to an effective policy.

- Unified Communication Platforms: Implement platforms that integrate with popular messaging apps to capture and archive communications in real time. These platforms ensure all communications are recorded and stored securely, accessible for compliance and legal review. The platform should be user-friendly to encourage adoption and should integrate seamlessly with existing systems.
- Mobile Device Management (MDM): Use MDM solutions to enforce security policies, manage app usage, and ensure compliance. These solutions can control which apps are installed on devices, monitor communications, and ensure all business-related messages are archived. MDM solutions can also provide remote wiping capabilities to protect data if a device is lost or stolen.
- Archiving Solutions: Deploy archiving software that integrates with various communication platforms to securely store and easily retrieve messages. These tools ensure that all business communications are captured and stored in compliance with regulatory requirements. The archiving solution should support e-discovery processes and provide advanced search capabilities for quick retrieval of specific communications.

Corporate-Issued Devices vs. BYOD: Do We Revert Back to This Now?

Returning to corporate-issued devices can enhance control over business communications, but is not a standalone solution. Here’s why:

- Enhanced Control and Monitoring: Corporate-issued devices allow better implementation of MDM solutions and compliance monitoring. They ensure that all installed apps and communications are subject to the company’s policies and monitoring systems.
- Employee Resistance and Dual Usage: Employees may still prefer personal devices for convenience, leading to continued use of off-channel communications. Clear policies and continuous monitoring are crucial. Additionally, companies must ensure that corporate-issued devices are user-friendly and meet the employees’ needs to reduce the temptation to use personal devices.

Mitigating Security Threats and Data Breaches

Implementing compliance technologies can significantly mitigate security threats and data breaches associated with off-channel communications:

- Enhanced Security: Unified communication platforms and MDM solutions offer robust security features, including end-to-end encryption and secure data storage, reducing the risk of data breaches. These features ensure that business communications are protected from unauthorized access and tampering.
- Real-Time Monitoring: Advanced monitoring tools can detect and prevent unauthorized access, ensuring that sensitive business information remains secure. Real-time alerts can notify compliance teams of potential breaches or policy violations.

- Data Loss Prevention (DLP): DLP technologies help prevent the unauthorized transfer of sensitive information, protecting against data leaks and breaches. These technologies can automatically block or flag suspicious activities, providing an additional layer of security.

Employee Training and Awareness

- Continuous Training: Regularly train employees on the importance of using approved communication channels and the potential risks of off-channel communications. Emphasize the legal and regulatory consequences of non-compliance. Training should be engaging and interactive, using real-world scenarios to illustrate the risks and best practices.
- Compliance Culture: Foster a culture of compliance where adherence to communication policies is encouraged and rewarded. Leadership should demonstrate compliant behavior and reinforce the importance of following established guidelines. (Compare with J.P. Morgan Securities LLC, Exchange Act Release No. 93807 (Dec. 17, 2021) (supervisors responsible for implementing and ensuring compliance with policies and procedures used their personal devices to communicate firm business.))

Effectiveness of 'Honor Statements'

"Honor statements," where employees sign documents committing to follow policy and specifically avoid third-party channels for business communications, can be part of the solution. However, their effectiveness can be limited if not supported by other measures:

- Reinforcement through Training: Employees need continuous training and reminders about the importance of compliance and the risks associated with off-channel communications. Honor statements should be part of a broader educational initiative.
- Monitoring and Enforcement: Without monitoring and enforcement, honor statements alone are unlikely to be effective. Companies must implement technology solutions to ensure compliance and detect violations. This could include, for instance, surveilling for a disproportionately low number of messages associated with a particular custodian on approved channels and keyword searches.
- Cultural Integration: Honor statements should be integrated into the company's culture of compliance. Leadership should model the behavior expected from employees and regularly communicate the importance of adhering to approved communication channels.
- **Culture, Culture, Culture: Tone at the Top Remains a Key Element**

Fostering a culture of compliance has tangible benefits, including improved regulatory adherence, enhanced trust, higher employee engagement, and operational efficiencies. However, it also presents challenges:

- Leadership Commitment: Strong leadership is crucial for setting the tone and engaging employees. Leaders must demonstrate their commitment to compliance through their actions and decisions.

- Continuous Effort: Cultural change is an ongoing process that requires regular monitoring and adjustment. It’s not a one-time initiative but a continuous effort to align behaviors with the organization’s values and policies.

Impact to the Company

Cost-Benefit Analysis: This All Sounds Expensive. What Is the ROI?

Investing in compliance technologies and fostering a culture of compliance involves significant costs, but the long-term benefits outweigh these expenses. Key benefits include:

- Avoidance of Fines: Prevent hefty fines and legal fees associated with regulatory breaches. Regulatory fines for non-compliance can be substantial, and avoiding these penalties can save companies millions of dollars.
- Operational Efficiency: Streamline communication processes and reduce the administrative burden on compliance teams. Efficient communication platforms and monitoring systems can free up resources and allow compliance officers to focus on more strategic tasks.
- Reputation Management: Build trust with stakeholders by demonstrating a commitment to compliance. A strong reputation for regulatory adherence and data security can enhance relationships with clients, partners, and investors.
- Mitigation of Security Threats: Enhanced security features reduce the risk of data breaches, protecting sensitive business information and ensuring business continuity. Preventing data breaches also avoids the associated costs of remediation, legal consequences, and reputational damage.

Conclusion

Addressing off-channel communications requires a holistic approach that integrates policy, technology, and cultural change. By combining clear communication policies, advanced technological solutions, continuous training, and a strong compliance culture, organizations can effectively manage the risks associated with off-channel communications. This comprehensive strategy not only ensures regulatory compliance, but also enhances overall communication practices within the organization.

Implementing these measures will require an investment of time and resources, but the long-term benefits—ranging from avoiding regulatory penalties to improving operational efficiencies and protecting the company’s brand and reputation—are significant. In-house attorneys and compliance professionals play a crucial role in driving these initiatives, ensuring that their organizations are well equipped to navigate the complexities of modern communication landscapes while maintaining a compliant environment and protection of secure data.

Ken Koch *is principal and the forensics practice market leader at BDO USA in Washington, D.C. and* **Tim Nagy** *is a financial markets regulatory & enforcement partner at Mayer Brown in Washington, D.C.*

Reprinted with permission from the August 20th, 2024 edition of Corporate Counsel © 2024 ALM Global Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 877-256-2472 or asset-and-logo-licensing@alm.com.