The Hidden Risks of Modern Messaging

Key Risks, Stats, Legal Challenges, and Best Practices for Modern Legal Teams

Modern communication channels are an essential part of business operations. Organizations need governance that ensures these communications are properly retained, preserved, and managed when legal, regulatory, or compliance obligations arise.

Regulatory actions by the DOJ & FTC against the destruction of evidence have led to strict preservation guidance.

58% ***of publicly listed companies now ban apps with ephemeral messaging entirely,*** compared to only **33%** of private organizations.

63%

of compliance executives were not monitoring business communications occurring on personal messaging apps like WhatsApp, despite increasing regulatory scrutiny.

$2 B+ in fines

have been imposed by SEC and CFTC tied to employees using WhatsApp, Signal, texts, and other off-channel messaging platforms for business communications that were not properly preserved.

59%

of surveyed firms have banned WhatsApp and similar apps due to regulatory scrutiny. The SEC and CFTC have levied billions in fines against major financial institutions for using unapproved off-channel apps, such as WhatsApp and Signal, where business communication is difficult or impossible to archive.

75%

of employees use WhatsApp or other messaging apps to share sensitive business data, and **71%** admit to sending critical company information through those platforms.

Understanding Their Differences

Encrypted Messaging		Ephemeral Messaging
Messages are protected through encryption so only authorized parties can access the content	Definition	Messages are automatically deleted after a set period or once viewed
Privacy and security	Primary Purpose	Temporary communication and reduced message retention
Limited visibility and collection complexity	Main Legal Concern	Loss of discoverable evidence
Yes, unless manually deleted or retention policies apply	Can Messages Persist?	Often no, as messages may disappear automatically
Signal, WhatsApp, Microsoft Teams, Apple iMessage, Telegram (in Secret Chats mode)	Examples	Snapchat, disappearing messages in Slack or Microsoft Teams, WhatsApp's Disappearing Messages feature

Encrypted Messages

What legal teams need to know

Encrypted messaging platforms secure communications in transit and at rest, making unauthorized access difficult. While encryption improves privacy and cybersecurity, it can complicate preservation, collection, review, and monitoring obligations.

Common Legal Challenges

- Difficulty accessing message content during investigations
- Limited centralized retention controls
- BYOD and personal-device complications
- Cross-border privacy and data transfer concerns
- Metadata gaps during collection
- Shadow IT and unsanctioned app usage

Best Practices

- ✓ Implement approved communication policies
- ✓ Use enterprise-managed messaging platforms
- ✓ Define retention and preservation procedures
- ✓ Maintain audit logs and access tracking

- Potential Legal risks
- Failure to preserve communications during litigation
- Regulatory scrutiny over inaccessible records
- Delayed eDiscovery response timelines
- Incomplete productions due to inaccessible data

- ✓ Conduct employee training on acceptable use
- ✓ Coordinate legal, compliance, and IT governance

Ephemeral Messages

What legal teams need to know

Ephemeral messaging systems automatically delete communications after a designated timeframe. While useful for reducing unnecessary data accumulation, these tools create substantial discovery and preservation risks if not governed properly.

Common Legal Challenges

- Automatic deletion of potentially relevant evidence
- Inability to reconstruct conversations
- Limited retention visibility
- Preservation failures during legal holds
- Inconsistent user-level settings
- Difficult forensic recovery
- Potential Legal risks
- Spoliation allegations
- Court sanctions for deleted evidence
- Regulatory penalties
- Adverse inference rulings
- Increased investigation costs

Best Practices

- ✓ Disable auto-delete during legal holds
- ✓ Establish defensible retention schedules
- ✓ Monitor disappearing-message settings
- ✓ Document preservation efforts thoroughly
- ✓ Restrict use for regulated or high-risk matters
- ✓ Regularly audit messaging compliance

When Encryption + Ephemerality are Combined

The Highest-Risk Scenario

Some platforms combine end-to-end encryption with disappearing messages, creating major preservation and discovery concerns.

Why

This Creates Elevated Risk

- Communications may become inaccessible and automatically deleted
- Legal teams may lack visibility into active conversations
- Preservation windows can be extremely short
- Organizations may struggle to demonstrate defensible compliance

Example Risk Scenarios

Legal Hold Violation

An employee subject to a legal hold continues using disappearing messages on an encrypted platform. Relevant communications are automatically deleted before preservation occurs and this leads to:

- Potential spoliation claims
- Regulatory scrutiny
- Increased forensic costs
- Possible sanctions or adverse inference findings

Governance Checklist for Legal Organizations

Policy & Compliance

- [ ] Define approved messaging platforms
- [ ] Establish retention requirements
- [ ] Create legal hold escalation procedures
- [ ] Restrict unauthorized applications

Technology Controls

- [ ] Enable enterprise retention settings
- [ ] Archive business communications where possible
- [ ] Monitor deletion settings and user activity
- [ ] Coordinate IT-security oversight

Employee Training

- [ ] Train employees on preservation obligations
- [ ] Educate staff on legal hold requirements
- [ ] Reinforce acceptable communication practices
- [ ] Provide reporting channels for policy violations

Taking Ephemeral and Encrypted Messages in Stride

Encrypted and ephemeral messaging are now central to modern business communication. For legal teams, the challenge is no longer whether these tools exist, but whether governance, preservation, and compliance strategies can keep pace with how employees actually communicate.

Consilio

© 2026 Consilio. All rights reserved.