Moving Sensitive Communications to Signal or WhatsApp

Moving Sensitive Communications to Secure Messaging

Email and workplace chat platforms like Slack are not designed for sensitive communications. While convenient for daily operations, they create permanent, searchable records that are vulnerable to subpoenas, breaches, and surveillance. This guide explains when and how to move sensitive conversations to encrypted messaging platforms, primarily Signal and WhatsApp.

Concerns about Email and Slack

Why Email is Insecure for Sensitive Communications

Fundamental Vulnerabilities:

- Email travels between servers as plain text (encrypted "in transit" but viewable by Google, Microsoft, etc.)
- Messages are stored permanently on multiple servers (from senders and receivers)
- Subject lines are never encrypted
- Easy target for subpoenas and legal discovery
- Metadata (who, when, to whom) is always visible
- NOTE: Even "secure" email from Proton isn't encrypted if the recipients are Google or Microsoft users

When Email is Acceptable:

- Public communications (press releases, newsletters)
- Routine coordination that isn't sensitive
- Communications that you'd be comfortable being publicly disclosed

Why Slack/Teams Aren't Secure Channels

Critical Limitations:

- No end-to-end encryption (providers can read all messages)
- Complete message history stored on company servers (for paid accounts)
- Administrator access to all conversations
- Vulnerable to subpoenas, e-discovery, and data requests
- Often mistaken as secure due to business/professional use
- Compliance tools may monitor all activity

When Slack/Teams are Acceptable:

- General team coordination
- Project management discussions
- Non-sensitive organizational communications
- When transparency and searchability are priorities

Secure Messaging

What Makes Messaging Platforms Secure?

End-to-End Encryption (E2EE):

- Messages encrypted on your device
- Only the recipient can decrypt
- Service provider cannot read message contents
- Protection from server breaches and legal requests

Additional Security Features:

- Disappearing messages (auto-delete after set time)
- Screenshot notifications
- Minimal metadata collection
- Open source code (for verification)

Signal

Why Signal is Recommended

Technical Security:

- End-to-end encryption by default for all communications
- Trusted open source protocol audited by security researchers
- Minimal metadata collection (phone numbers encrypted)
- Disappearing messages for all conversations

Organizational Structure:

- Operated by Signal Foundation, a nonprofit
- U.S.-based but with strong privacy commitments
- Limited data to provide in response to legal requests (no messaging data and almost no metadata)
- Transparent about government requests (publishes reports)

Practical Features:

- Voice and video calls (also encrypted)
- Group messaging with admin controls
- File sharing (encrypted)
- Desktop applications available
- Relatively simple to use -- feels like a "regular" chat app

When to Use Signal

High Priority Scenarios:

- Campaign strategy discussions
- Legal strategy or attorney communications
- Confidential partner communications
- Internal discussions about sensitive operations
- Anything you wouldn't want leaked to opposition or adversaries
- Communications involving vulnerable individuals
- Financial or donor information discussions

Organizational Use Cases:

- Executive team sensitive discussions
- Board communications on confidential matters
- Crisis response coordination

- Incident response team communications
- Legal compliance discussions
- Sensitive conversation with external partners

Signal Best Practices

Setup and Configuration:

1. **Enable Registration Lock**: Prevents someone from registering Signal with your number
2. **Set Disappearing Messages**: Default to 1 week or 4 weeks for most conversations
3. **Enable Screen Security**: Blocks screenshots (on Android)
4. **Use PIN**: Protect account recovery with secure PIN

Operational Security:

- Create dedicated Signal groups for specific sensitive projects
- Name groups descriptively but not identifiably ("Project Alpha" not "Litigation Strategy")
- Regularly review group membership
- Use Signal for sensitive one-on-one check-ins
- Turn on disappearing messages

WhatsApp

Understanding WhatsApp's Security

What WhatsApp Does Well:

- End-to-end encryption using Signal Protocol
- Encrypted voice/video calls
- Enormous, global existing user base (easier adoption)
- Feature-rich (compared to Signal)
- Disappearing messages available

Critical Limitations:

- Owned by Meta (Facebook company)
- Collects extensive metadata (who you talk to, when, how often)
- Shares metadata with Meta for advertising/analytics
- Cloud backups not end-to-end encrypted by default
- Terms of service allow data sharing within Meta companies
- Subject to Meta's broader surveillance advertising business

Metadata Risks:

- Social graph mapping (who knows whom)
- Communication pattern analysis
- Geographic tracking
- Device information collection
- Contact list upload

Lower-Risk Scenarios (when it's ok to use WhatsApp):

- Communications with international partners where WhatsApp is standard
- Coordination that isn't highly sensitive but needs encryption
- Communities where Signal adoption would be a major barrier
- When the content is sensitive but metadata exposure is acceptable (it's ok to expose who you're talking to)

WhatsApp Risk Mitigation

If you must use WhatsApp:

1. **Minimize Metadata Exposure:**
   - Don't use it for highly sensitive contacts
   - Assume Meta knows you're communicating with this person
   - Consider what communication patterns reveal
2. **Secure Settings:**
   - Enable disappearing messages
   - Disable read receipts
   - Turn off automatic media download
   - Disable cloud backups (or ensure they're encrypted)
   - Enable two-step verification
   - Advanced Chat Privacy: Admins can turn this on, users can't save media to their device or export chats
3. **Behavioral Safeguards:**
   - Use for logistics, not strategy
   - If possible, move highly sensitive conversations to Signal
   - Don't use for communications involving vulnerable people
   - Assume metadata is being collected and potentially shared

---

Revision #1
Created 22 December 2025 19:48:50 by Josh
Updated 22 December 2025 19:49:29 by Josh