Disclaimer

The views and opinions expressed in this program are those of the speakers only and do not reflect the views or positions of any entities with which the speakers are associated.

CLE Credit

This program has been submitted for accreditation in all jurisdictions requested by Symposium registrants.

You will receive a follow-up email after Symposium with instructions for claiming your credit, along with a link to download program materials.

To claim credit for this session, you will need to write down the session-specific password that will be shared later in this hour.

Consilio

SYMPOSIUM 2025

Messaging Challenges

Encrypted, Ephemeral, and Everywhere

Agenda

- The Messaging Explosion
- Legal Landscape and Challenges
- Managing the Risk
- Collection Challenges
- Project/Production Workflows
- Final Thoughts
- Questions

The Messaging Explosion

Messaging Challenges: Chatter, Chatter Everywhere

The Messaging Explosion

- OTT Apps
  - Third-party applications on mobile devices (e.g., WhatsApp, Signal)
  - May or may not be extracted from the handset during a standard mobile device collection process
    - May be because of end-to-end encryption or another security setting
    - May be because data is stored in the cloud
- Varies from app-to-app and across devices and operating systems

The Messaging Explosion

- Encrypted Messaging
  - Properly implemented end-to-end encryption ensures it's impossible for anyone but the sender and recipient to read the messages
  - Pose a variety of technical challenges as discovery sources
- Ephemeral Messaging
  - Allows for the automatic deletion of sent messages after a set amount of time
  - For discovery, automatic deletion must be suspended, and past use may draw scrutiny – particularly in the absence of clear usage and retention policies
    - NOTE: As of the end of 2021, Signal had more than 40 million monthly active users, and many of them are using it for both private and professional communications

The Messaging Explosion

- Collaboration Tools
  - Diverse sources, containing diverse content, potentially stored in diverse locations
    - Thousands of public and private channels, millions of direct and group messages
    - Reactions, animations, links, embedded content from third-party sources, etc.
- Capabilities and tools for preservation and collection are typically tied to type of licenses
- Consider existence of structured data systems that integrate a chat feature in which evidentiary communications can be created (Mattermost, Slack, etc.)

Legal Landscape and Challenges

Messaging Challenges: Chatter, Chatter Everywhere

Legal Landscape and Challenges

- Existence of such a glut of communication methods have made it exponentially more difficult to comply with both statutory and common law duties of preservation; as well as lack of organization control and difficulty of monitoring company policy compliance

- Examples of Statutory Preservation Requirements:
  - *Securities Exchange Act Rule 17a-4(b)(4)*
  - *Investment Advisers Act Rule 204-2(a)(7)*
  - *Financial Industry Regulatory Authority Rule 4511*

- Federal and State rules against spoliation, data loss, etc.:
  - *FRCP 34, 37*
  - Demand letters in employment litigation (*Miramontes v. Peraton Inc*, No. 3:2021cv03019)

Legal Landscape and Challenges

- Reasonable Steps: Uncertainty around how hard and how proactively you must look for such communications
  - FRCP 37(e) requires that, before the application of curative measures or spoliation sanctions, there must be a showing that "a party failed to take **reasonable steps** to preserve" [emphasis added] evidence it should have preserved

- Possession, Custody, and Control
  - To what extent do employers " control" the messages and other data in their employees' personal accounts or on their personal smartphones and laptops?
  - Courts are still wrestling with this question
    - In 2022, one widely-discussed case applied a multi-factor analysis that looked at:
      - The language of the applicable company policies
      - The technical realities of the company's BYOD program
      - The general practices in the work relationship between employees and the company
    - That court found that the factors did not establish the defendant had "control over text messages on the personally-owned phones of its employees."
    - That court also argued that a company should not be compelled to extort its employees, through the threat of termination, into surrendering personal devices for collection.

Managing the Risk

Messaging Challenges: Chatter, Chatter Everywhere

Managing the Risk

- Ensure your organization has an approved list of applications and tools that users can use and make sure users are trained on their proper use (Mobile Device Management (“MDM”) tools can assist in tracking/identification of application use)
- Clearly define your usage policy and continuously monitor compliance against this policy
- Draft clear access guidelines, only those employees with a clear business case for using such applications should have access to them
- Ensure your litigation response protocols cover these applications and that your legal hold technology and response guidelines are up to the task
- Clearly define what type of communications ephemeral messaging applications should and should not be used for
- Issues of non-compliance should be addressed as a matter of priority, there is no substitute for good corporate governance
- The messages may no longer exist, but your legal obligations do

Collection Challenges

Messaging Challenges: Chatter, Chatter Everywhere

Collection Challenges

- Key Elements to Consider
  - What kind of matter is it? This will affect front-end processing decisions, facilitate review discussion points, and determine production requirements
    - Civil Litigation
    - SEC Subpoena
    - DOJ
    - Other Investigation
  - Is there a need to export the data for integration back into your company's archival system?
    - Important to discuss to fully understand processing options and their effect on review/production

Collection Challenges

- **Duty to protect personal data**
  - Created workflows that permit greater flexibility in the type and amount of non-promoted data retained by partner/provider

- **Where does data REALLY live?**
  - Advent of cloud computing means that data may not exist in traditional locations, or might live across multiple repositories
  - Cloud, computer, or phone collections may be in play

Collection Challenges

- From Devices
  - Huge variety of makes and models
    - Difficulty, cost, and time varies from model to model, from maker to maker, from operating system to operating system, and from update to update
  - Direct collection needs special tools; cloud backups are sometimes an option
  - Updates can mean changes in what's easy, what's hard, and what's possible
  - Stock applications typically captured; third-party may or may not be

- From the Cloud
  - Account access
  - Feature limitations depending on platform and license

- **From a regulated archive**
  - Some entities (particularly those in the Financial Services space) maintain regulated data archives to which messages/communications from business devices are automatically transferred. For those clients, collecting from the archive can therefore be a less intrusive alternative to in-person, or cloud-based mobile collections.

Collection Challenges

- Personal Mobile Device Workflow – Physical collection
  - Entire device must be collected
    - Extended downtime (3+ hours*)
    - Will collect the most data possible

- Personal Mobile Device Workflow – iCloud collection
  - Allows for a more flexible collection
    - Only possible for iPhones
    - Certain Categories can be excluded from collection
    - Greater sense of custodian agency

Collection Challenges

- Advanced Collections – ModeOne/Premium
  - Continuing the trend of more targeted collections
  - Can collect by participant and/or date range of communications.
    - iPhone/Android friendly
    - Ideal outcomes when used in appropriate situations, protects personal data.
    - Premium can target encrypted communications
    - Collection time is data dependent (may ultimately be longer than a traditional full forensic acquisition, depending on how “targeted” the queries are)

Collection Challenges

Supported Imaging Methods by Application

iPhone	Cellebrite Premium	ModeOne	Cellebrite UFED
Full File System Imaging	Y	N	N
Advanced Logical Imaging	Y	Y	Y
Collection Date Filtering	N	Y	N
Targeted Collection by Application	N	Y*	N
Targeted Collection by Contact	N	Y*	N

** Limited to supported apps*

Android	Cellebrite Premium	ModeOne	Cellebrite UFED
Full File System Imaging	Y	N	N
Advanced Logical Imaging	Y	Y	Y
Collection Date Filtering	N	Y	N
Targeted Collection by Application	Y	Y*	N**
Targeted Collection by Contact	N	Y*	N

** Limited to supported apps*

*** Can target high-level categories such as Contacts, Calls, SMS, MMS, Photos, and Files*

ModeOne Supported Applications for Targeting

iPhone		Android
iMessage	Installed Apps	SMS/MMS Messages
Contacts	Photos	Contacts
Calls	Videos	Calls
Voicemails	Locations	Gallery
WhatsApp	Recordings	Installed Apps
WeChat	Calendar	
LINE	Notes	
Viber	Safari History	
Kik		
Facebook Messenger		

** Can be targeted by contact number or email*

ModeOne Processing – Export Options

- DFES Standard: DAT file w/PDF
- PDFs should go through OCR to ensure all text data is captured.
- Most PDFs will contain attachments, but forwarded texts will also appear.
- DFES has communicated with Ops to better align on data handoff
- Other potential export options can be:
- UFDR
- RSMF
- Either of these options will be due to client or counsel request and should be communicated across all internal stakeholders.

Collection Challenges

- **From Reluctant Custodians**
  - Privacy expectations
    - Voiced and “hidden” privacy concerns can halt the collection process, or entrench resistance
    - If left unaddressed these fears will spread rapidly and evolve
  - Honest and open discussions are key
    - Use transparent processes, and overtly work to collect the minimal amount of data required
    - Collections staff should be specifically selected and trained to handle sensitive situations with empathy and compassion
  - Identify what data is relevant up front
    - Craft a workflow that targets relevant data, and can potentially avoid overcollection of sensitive and personal information
    - Work to make it as unintrusive as possible

Project/Production Workflows

Messaging Challenges: Chatter, Chatter Everywhere

Project/Production Workflows

- Investigations/Internal Analysis
  - Utilize Full thread export to quickly browse end-to-end conversations of the participant group
  - Extracted text enables key terms searching and highlighting
  - Array of mobile metadata fields allow for targeted searching of certain applications, participants, dates, etc.
  - Relationship threading allows for the threading of communications ACROSS chat/voice applications
- Regulatory inquiries
  - Flexibility required to comply with the production requirements of large regulatory bodies
    - DOJ: single item production
    - SEC: 24-hour unitization

Project/Production Workflows

- Litigation
  - Parties should include parameters for the searching and review of mobile data
  - Unitization format and Metadata should be confirmed in writing if possible

- Review workflow/Other considerations
  - Per-Day review
  - Single Item review with master thread as reference

Final Thoughts

Messaging Challenges: Chatter, Chatter Everywhere

Questions

Messaging Challenges: Chatter, Chatter Everywhere