MINTZ

eDiscovery for the Modern Company Using IM and Chat Applications

October 31st, 2023

The webinar will begin shortly

SPEAKERS

MICHELLE N. LIPKOWITZ
Member, Litigation & Managing Member, DC Office
Washington D.C.
MNLipkowitz@mintz.com // +1.202.434.7448

Michelle is a seasoned litigator with a multifaceted practice that encompasses complex commercial litigation, white collar defense, and government investigations. She has extensive experience with shareholder, construction, product liability, and contract disputes as well as consumer class actions and criminal defense matters. She regularly provides counsel on highly sensitive matters, often assisting with crisis management and strategies for handling the press for clients across a broad spectrum of industries.

JOHN B. KOSS
Managing Director, E-Data Consulting Group
Boston
JBKoss@mintz.com // +1.617.210.6855

As the Managing Director of Mintz's Chambers & Partners globally- and nationally-ranked E-Data Consulting Group, John's practice focuses exclusively on counseling clients on information governance and the utilization of technology and artificial intelligence to manage large data matters. John has particular experience advising clients in the life sciences, pharmaceutical, and healthcare industries facing commercial litigation, corporate M&A activity, antitrust inquiries, and government investigations.

TROY CAHILL
General Counsel and Corporate Secretary
LaserShip and OnTrac Logistics
Washington DC
TCahill@ontrac.com // +1.703.348.7680

Troy D. Cahill serves as General Counsel for OnTrac Logistics, Inc. and LaserShip, Inc. Prior to joining OnTrac/LaserShip's legal department, Troy was in private practice with Akin Gump where he focused his practice on appellate litigation before the Supreme Court of the United States and federal courts of appeals. Troy served as staff counsel to the Supreme Court of the United States, Office of the Clerk from 2002 to 2006.

Why Do We Care?

SEC Charges 11 Wall Street Firms

SEC Charges 11 Wall Street Firms with Widespread Recordkeeping Failures

Press Release

SEC Charges 11 Wall Street Firms with Widespread Recordkeeping Failures

Firms admit to wrongdoing and agree to pay penalties totaling $289 million

FOR IMMEDIATE RELEASE
2023-149

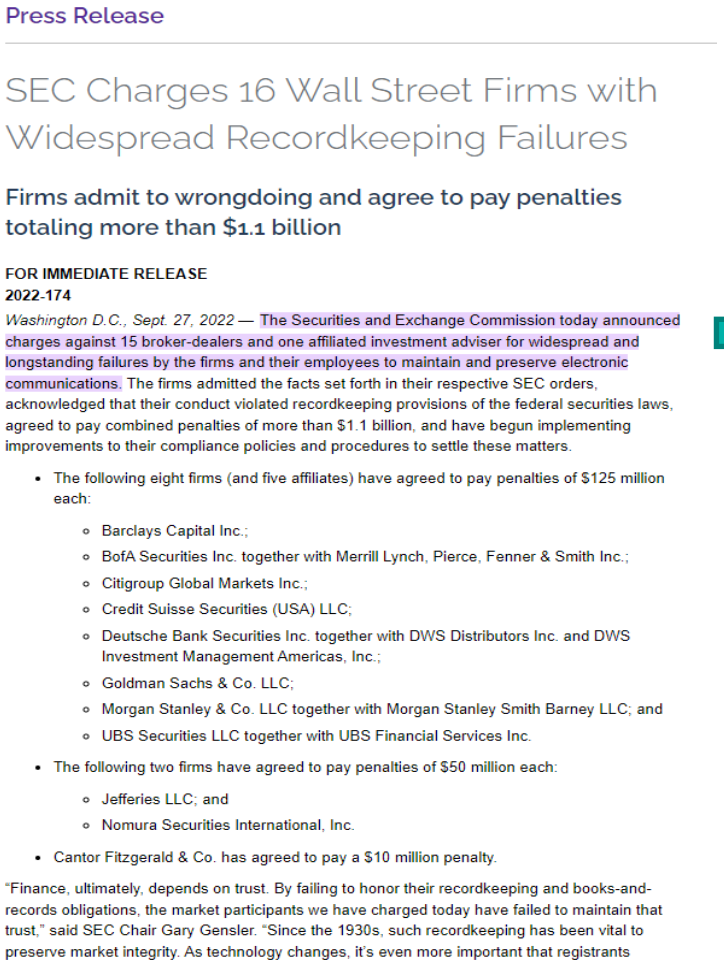
Washington D.C., Aug. 8, 2023 — The Securities and Exchange Commission today announced charges against 10 firms in their capacity as broker-dealers and one dually registered broker-dealer and investment adviser for widespread and longstanding failures by the firms and their employees to maintain and preserve electronic communications. The firms admitted the facts set forth in their respective SEC orders. They acknowledged that their conduct violated recordkeeping provisions of the federal securities laws, agreed to pay combined penalties of $289 million as outlined below, and have begun implementing improvements to their compliance policies and procedures to address these violations.

- Wells Fargo Securities, LLC together with Wells Fargo Clearing Services, LLC and Wells Fargo Advisors Financial Network, LLC agreed to pay a $125 million penalty;
- BNP Paribas Securities Corp. and SG Americas Securities, LLC have each agreed to pay penalties of $35 million;
- BMO Capital Markets Corp. and Mizuho Securities USA LLC have each agreed to pay penalties of $25 million;
- Houlihan Lokey Capital, Inc. has agreed to pay a $15 million penalty;
- Moelis & Company LLC and Wedbush Securities Inc. have each agreed to pay penalties of $10 million; and
- SMBC Nikko Securities America, Inc. has agreed to pay a $9 million penalty.

“ Firms admit to wrongdoing and agree to pay penalties totaling $289 million..”

SEC Charges 16 Wall Street Firms

SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures



Press Release

SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures

Firms admit to wrongdoing and agree to pay penalties totaling more than $1.1 billion

FOR IMMEDIATE RELEASE
2022-174

Washington D.C., Sept. 27, 2022 — The Securities and Exchange Commission today announced charges against 15 broker-dealers and one affiliated investment adviser for widespread and longstanding failures by the firms and their employees to maintain and preserve electronic communications. The firms admitted the facts set forth in their respective SEC orders, acknowledged that their conduct violated recordkeeping provisions of the federal securities laws, agreed to pay combined penalties of more than $1.1 billion, and have begun implementing improvements to their compliance policies and procedures to settle these matters.

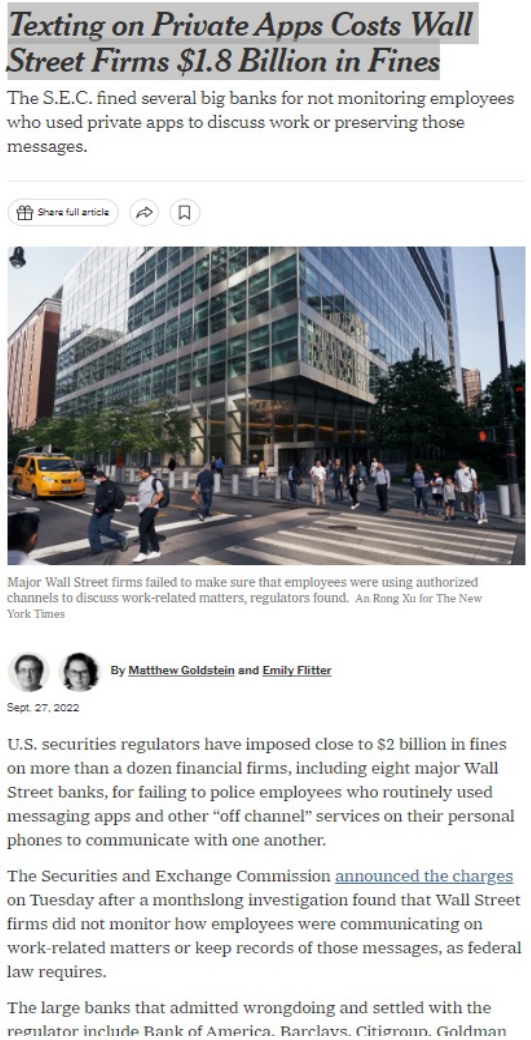
- The following eight firms (and five affiliates) have agreed to pay penalties of $125 million each:
  - Barclays Capital Inc.;
  - BofA Securities Inc. together with Merrill Lynch, Pierce, Fenner & Smith Inc.;
  - Citigroup Global Markets Inc.;
  - Credit Suisse Securities (USA) LLC;
  - Deutsche Bank Securities Inc. together with DWS Distributors Inc. and DWS Investment Management Americas, Inc.;
  - Goldman Sachs & Co. LLC;
  - Morgan Stanley & Co. LLC together with Morgan Stanley Smith Barney LLC; and
  - UBS Securities LLC together with UBS Financial Services Inc.
- The following two firms have agreed to pay penalties of $50 million each:
  - Jefferies LLC; and
  - Nomura Securities International, Inc.
- Cantor Fitzgerald & Co. has agreed to pay a $10 million penalty.

"Finance, ultimately, depends on trust. By failing to honor their recordkeeping and books-and-records obligations, the market participants we have charged today have failed to maintain that trust," said SEC Chair Gary Gensler. "Since the 1930s, such recordkeeping has been vital to preserve market integrity. As technology changes, it's even more important that registrants

" Firms admit to wrongdoing and agree to pay penalties totaling more than $1.1 billion.."

Texting on Private Apps Costs Wall Street Firms

Texting on Private Apps Costs Wall Street Firms $1.8 Billion in Fines



Texting on Private Apps Costs Wall Street Firms $1.8 Billion in Fines

The S.E.C. fined several big banks for not monitoring employees who used private apps to discuss work or preserving those messages.

Share full article

Major Wall Street firms failed to make sure that employees were using authorized channels to discuss work-related matters, regulators found. An Rong Xu for The New York Times

By Matthew Goldstein and Emily Flitter

Sept. 27, 2022

U.S. securities regulators have imposed close to $2 billion in fines on more than a dozen financial firms, including eight major Wall Street banks, for failing to police employees who routinely used messaging apps and other "off channel" services on their personal phones to communicate with one another.

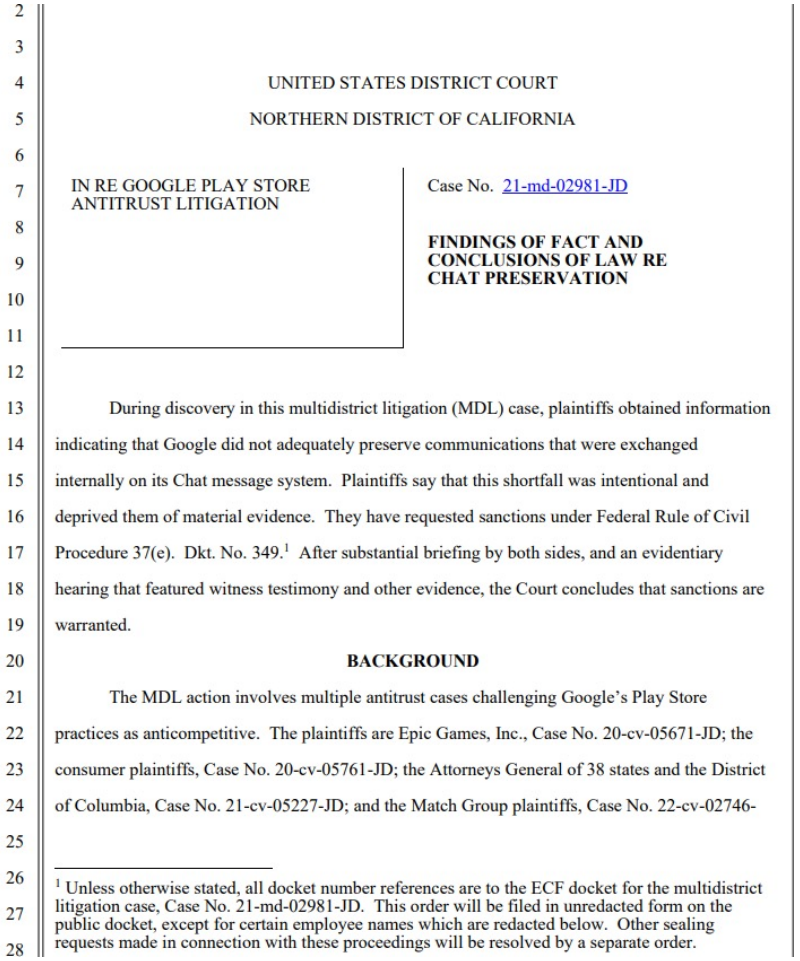
The Securities and Exchange Commission announced the charges on Tuesday after a monthslong investigation found that Wall Street firms did not monitor how employees were communicating on work-related matters or keep records of those messages, as federal law requires.

The large banks that admitted wrongdoing and settled with the regulator include Bank of America, Barclays, Citigroup, Goldman

"The SEC fined several big banks for not monitoring employees who used private apps to discuss work or preserving those messages..."

Google Sanctioned for Failure to Preserve Internal Chat Messages

Google Sanctioned for Failure to Preserve Internal Chat Messages



UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE GOOGLE PLAY STORE ANTITRUST LITIGATION

Case No. 21-md-02981-JD

FINDINGS OF FACT AND CONCLUSIONS OF LAW RE CHAT PRESERVATION

During discovery in this multidistrict litigation (MDL) case, plaintiffs obtained information indicating that Google did not adequately preserve communications that were exchanged internally on its Chat message system. Plaintiffs say that this shortfall was intentional and deprived them of material evidence. They have requested sanctions under Federal Rule of Civil Procedure 37(e). Dkt. No. 349.[1] After substantial briefing by both sides, and an evidentiary hearing that featured witness testimony and other evidence, the Court concludes that sanctions are warranted.

BACKGROUND

The MDL action involves multiple antitrust cases challenging Google's Play Store practices as anticompetitive. The plaintiffs are Epic Games, Inc., Case No. 20-cv-05671-JD; the consumer plaintiffs, Case No. 20-cv-05761-JD; the Attorneys General of 38 states and the District of Columbia, Case No. 21-cv-05227-JD; and the Match Group plaintiffs, Case No. 22-cv-02746-

[1] Unless otherwise stated, all docket number references are to the ECF docket for the multidistrict litigation case, Case No. 21-md-02981-JD. This order will be filed in unredacted form on the public docket, except for certain employee names which are redacted below. Other sealing requests made in connection with these proceedings will be resolved by a separate order.

"Google did not adequately preserve communications that were exchanged internally on its Chat message system..."

District Court Cuts Litigants No Slack

District Court Cuts Litigants No Slack for Failing to Produce Instant Messaging Data

"It is crucial that attorneys are mindful...and understand the preservation and collection pitfalls…"

Corporate Instant Messaging Data Resulting in Default Judgment

April 26, 2023 | Spring 2023 Vol. 67 #2

By John B. Koss

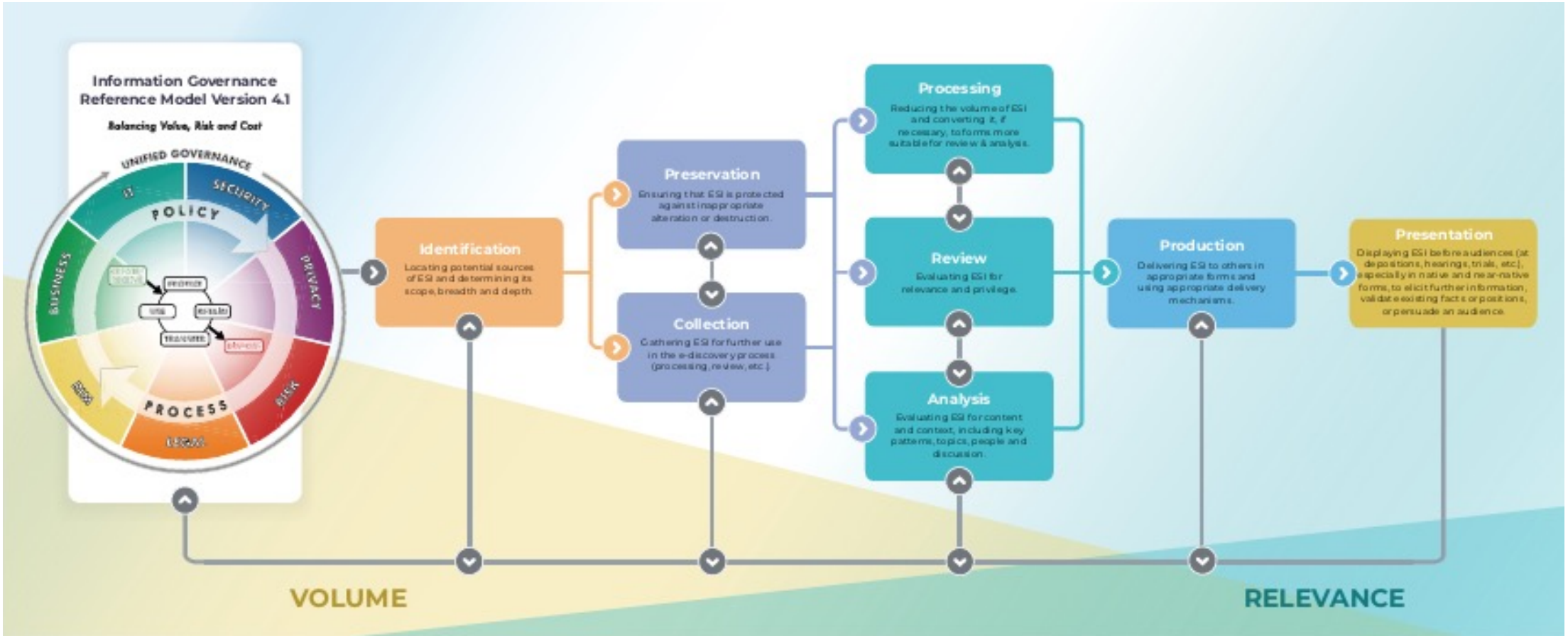
With the rapid emergence of COVID and the resulting rush to accommodate remote work, many corporations swiftly implemented corporate instant messaging applications such as Slack. Slack is a cloud-based instant messaging application that allows users to communicate on a one-to-one basis or in larger groups in dedicated "channels," which are permissioned chat groups that can be commissioned for corporate teams, departments, or parties outside an organization.

While applications like Slack can facilitate remote collaboration and feel familiar to younger workers used to social media messaging, some of their unique features, including the way in which Slack organizes and catalogues individual and group messages as well as programmatic options for identifying, searching, and preserving communications, create strategic risks when such data is implicated in civil discovery. It is crucial that attorneys are mindful of these unique characteristics and understand the preservation and collection pitfalls associated with applications like Slack before advising clients and attempting to collect data to meet discovery obligations.

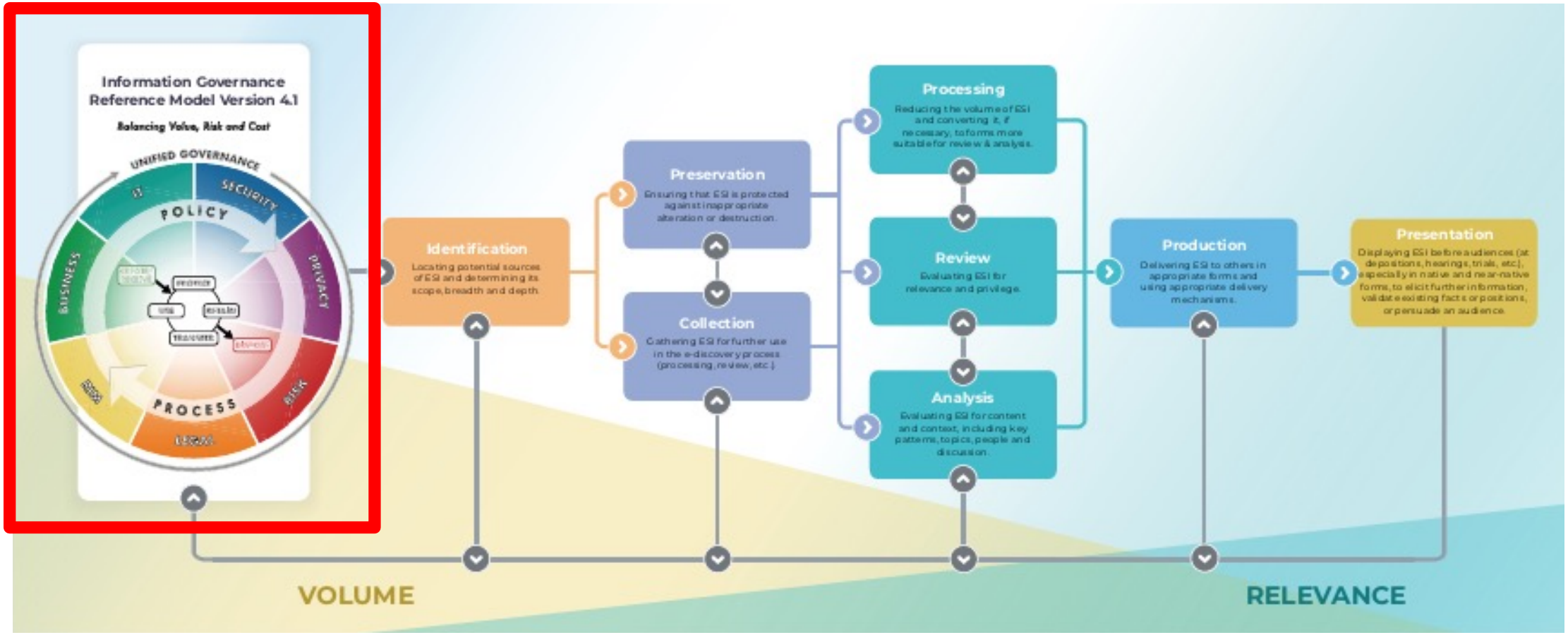
The importance of this messaging evidence and the litigation risks of failing to properly preserve, review, and produce it were on full display in a recent decision issued by the United States District Court for the District of Massachusetts in the matter of *Red Wolf Energy Trading, LLC v. BIA Capital Management, LLC*, 19-cv-10119-MLW, 2022 WL 4112081 (D. Mass. Sep. 8, 2022). In this case, the Court entered default

What the Legal Department Should Know

Overview: The E-Discovery Lifecycle



Phase I - Information Governance for IM/Chat App Data



IG- Internal Practice & Policy

- What are the permissible IM and chat apps at your organization?
- What does the permissible use policy say about the scope and employee use of these apps?
- What is the retention schedule for these permissible apps?
- How is your organization managing shadow IT/impermissible application use?
- How does your organization regulate employee use of personal devices/cell phones for business purposes?
- What does your organization policy say with respect to “control” of such devices?
- How are employee privacy concerns and issues addressed?

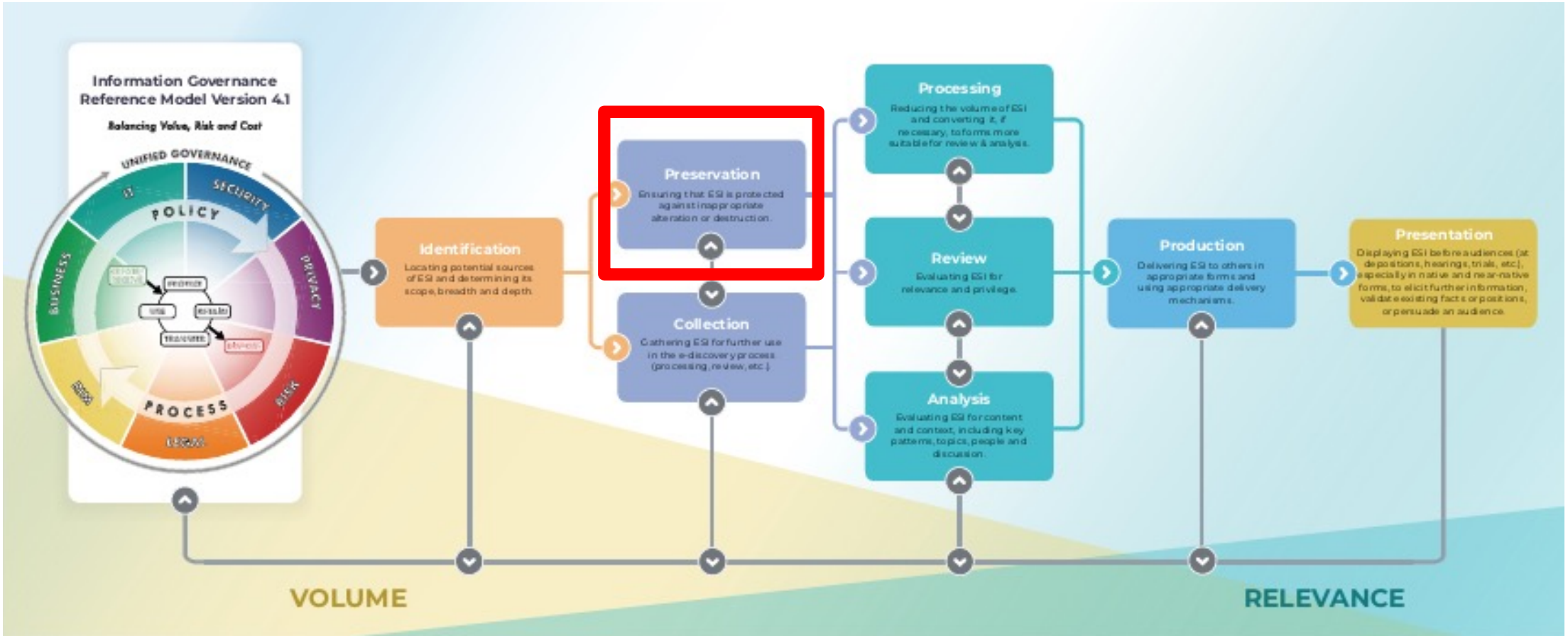
IG – Collaboration with Compliance

- Are you in a regulated industry that has retention requirements for certain communications data?
  - If so, assume all IM/chat app data is subject to those retention requirements.
- Even if no such regulations exist, assume IM/chat app data will be considered in scope by all federal agencies in response to document requests or demands.
  - FTC, SEC, DOJ, State AGs all consider such data relevant and discoverable to the same extent as more traditional hardcopy and email communications.
- Do privacy statutes or regulations apply to the IM/chat app data to be collected?
  - E.G., GDPR or CCPA.

IG- Collaboration with IT

- Understand the subscription models that your IT Department has in place for each IM and chat app.
  - E.G., is your Slack app subscription Pro, Business+, Enterprise Grid?
- Where does IM and chat data reside?
  - E.G., Teams messaging typically resides across O365.
- How does you IT Department regulate corporate content/business use of personal devices/cell phones?
  - E.G., BYOD Policy, use prohibition, hybrid approach?
- Where are the servers hosting the data geolocated?
  - P.S., the “Cloud” is not the answer.

Phase II – Preservation of IM/Chat App Data



Scope of Preservation

- To the extent IM/chat app data is in scope for your matter, how broadly should data be preserved? Should a hold be placed at all?
  - Here, knowing the subscription level and corporate location of this data is key.
- What information can IT provide with regards to the use of these apps by certain users?
  - Can you identify specific apps used by each employee or department?
  - Within an individual's app usage, can specific channels, groups, or locations where an employee had access/communicated be identified and individually preserved?
- Or, does preservation require broader capture based on subscription or search limitations?

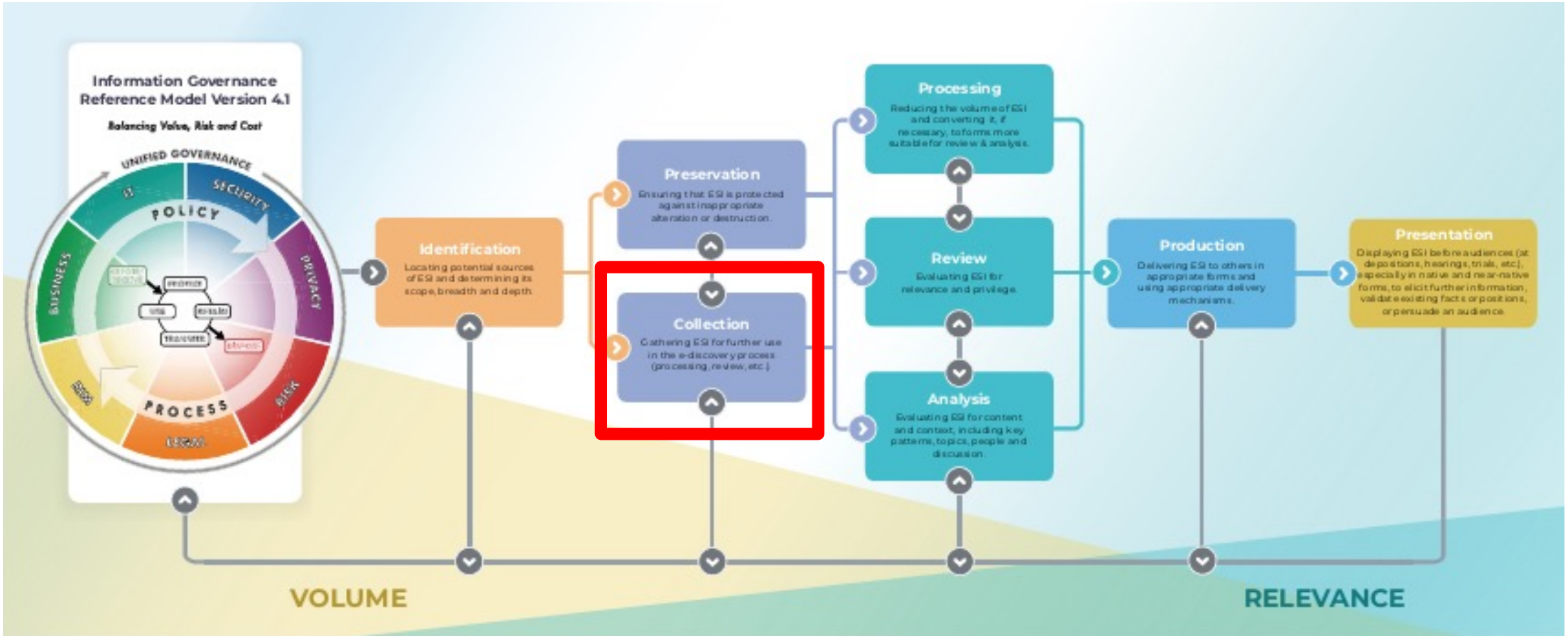
Method of Preservation

- What options are available for the organization in terms of placing a legal hold across identified IM/chat app data?
- Are programmatic legal holds possible/available/workable?
- What does/does not reside in the employee mailbox or other sources that might already be under legal hold based on their location within your overall infrastructure?
- Can a legal hold be placed on individual users or channels?
- How can these preservation steps be documented and monitored?
- What are the costs of the chosen preservation approach?

Personal Device/Non-Corporate App Data

- Generally, BYOD and personal devices do not back up data to your organization's corporate IT infrastructure outside of email, calendar, contacts, and other remotely-accessed applications.
- This means that most personal texting (e.g. SMS, iMessage) all resides exclusively on the personal device (or archived in iCloud backups).
- The same is true for and social media/chat application data (WhatsApp, Signal, Telegram, WeChat).
- Accurately capturing this data typically requires obtaining a full forensic backup.
- When should a preservation copy of a personal device be made?
- Should iCloud backups be included in the forensic collection?

Phase III – Collection of Chat/IM App Data



Scope of Collection

- As with preservation considerations and questions previously discussed, collection can be equally tricky and premised on the limitations of the corporate systems and policies in place.
- Ideally, IM/chat app data will be collected as narrowly as practicable, but this will depend on your organization's particular applications and settings.
- Discuss with outside counsel (if applicable) what might be in-scope and make sure that complete relevant dataset is included in capture.

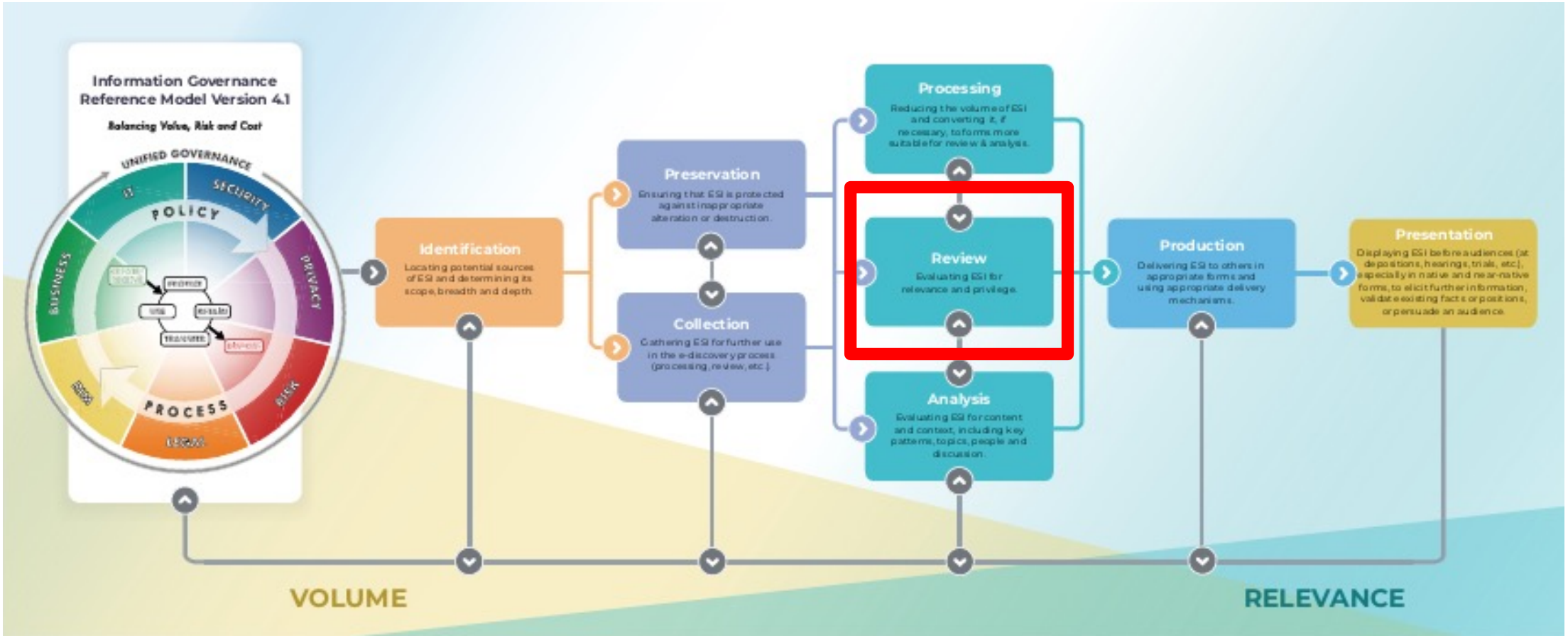
Method of Collection

- It is important to understand the technical components of your specific IM/chat applications to ensure that all relevant messaging and data is collected correctly and in full.
  - E.G., MS Teams messaging may include data across O365 and requires attention to each component.
- Are your internal IT resources capable of conducting an appropriate collection of these data sources or should a forensic/outsourced resource be used?
  - Collection of these data sources is very different than email or other more traditional sources of discovery and may require specific tools or workflows.

Personal Device/Non-Corporate App Data

- Assuming a preservation/backup image of a personal device/cell phone has been created, that image can be systematically mined for potentially relevant IM/chat data.
- Specific messages, contacts, senders/recipients, and/or dates can be extracted from the image.
- Once identified, potentially relevant data can be extracted and processed into most document review tools.
- Work with your technical expert to ensure collected data is processed correctly to preserve relevant metadata fields that may assist with review and analysis further down the line or be required for production.

Phase IV – Review of IM/Chat App Data



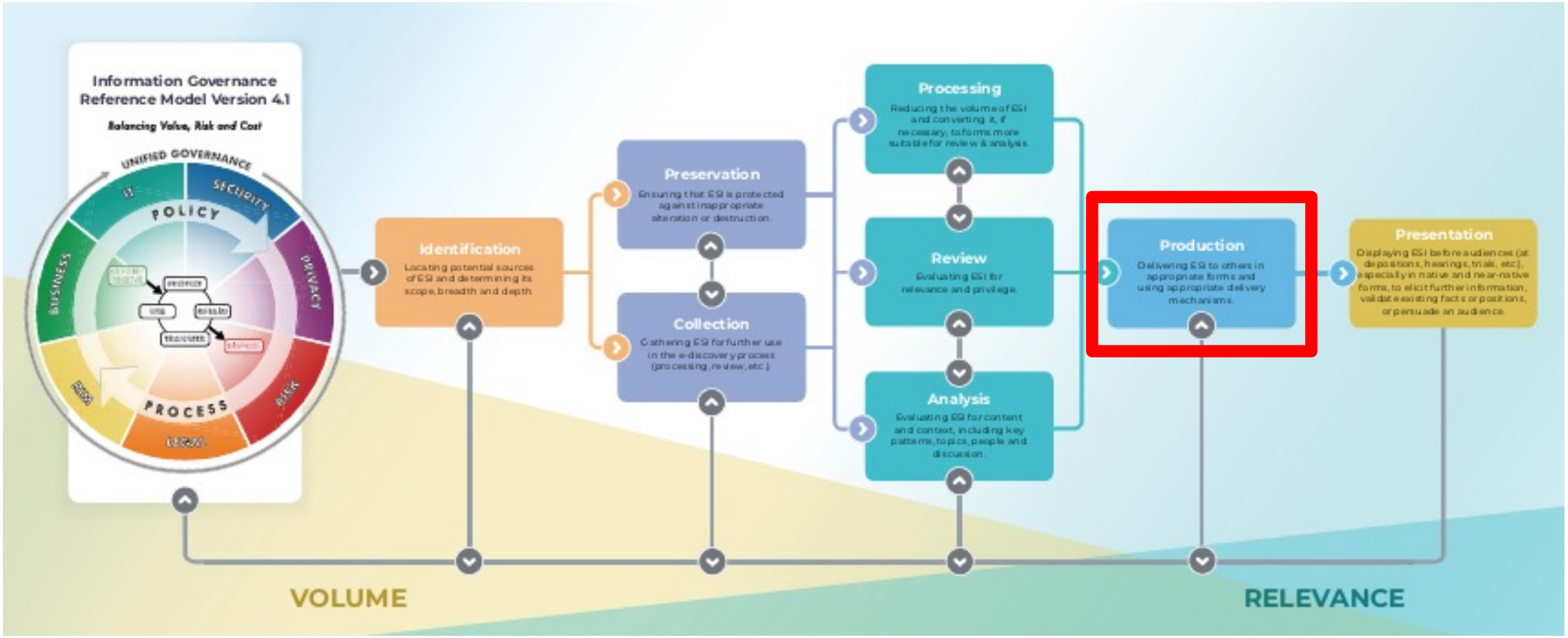
Best Practices for Review of IM/Chat App Data

- If a full collection of an application instance in the only option, work with a technical expert to determine how to process and analyze the data in the most cost efficient and practical manner.
- Understand the ability of your particular review tool to utilize search terms or other analytics to zero in on potentially relevant portions of communications or channels.
- Once relevant IM/chat app data is best reviewed in a document review application that allows for coding and tracking data in full “families” or groups.

Best Practices for Review of IM/Chat App Data

- Most review applications allow for messages to be processed in customizable time periods or in full sets.
- Work with outside counsel or your relevant internal resource to determine what format and sequence make sense for your particular matter.
- Make sure privilege considerations are factored into review timing and workflow.
  - Typically, the membership of IM/chat app channels and the involvement of various members at various times can be determinative of privilege.

Phase V – Production of IM/Chat Data



Production Format of IM/Chat App Data

- What is the agreed-upon format for the production of Chat/IM data?
  - Is there an ESI protocol or government production specifications for your matter?
  - What are the specific requirements of that protocol/specifications?
  - Has all required metadata been identified and included in the production load files?
- Screen grabs or screenshots do not generally comply with discovery rules or government production requirements.
- What cadence of communications is appropriate for production (i.e., individual messages, daily, weekly, something else?)

Production Considerations Relating to IM/Chat Content

- Date range agreements on relevance may allow for wholesale removal of certain portions of chats or channels.
- Consider also, how to handle redactions/removals of irrelevant information being mindful of general prohibition of deletion of “irrelevant” data/messages intermingled with “relevant” communications.
- Metadata analysis (and membership of channels) may be required to determine privilege for any group or channel that contains members of the legal department.
  - Typical analysis of role/involvement applies, by large membership or participants in the group or channel may complicate the analysis.
- Also, keep an eye out for PII/PHI that may also require redaction.

Special Considerations for Internal Investigations

Special Considerations for Internal Investigations

- Does your internal investigation require analysis of IM/Chat app data?
- How can this data be reviewed with existing internal applications and software?
  - How can IT make this data available for informal analysis/fact gathering?
- What is the potential that your internal investigations arguably triggers a duty to preserve?
- Will some or all of the collected data be retained outside of the native IM/chat app, or will it be deleted?
- If a full backup is required to preserve all content, should that be done at the internal investigation phase?

Special Considerations for Government Investigations

Special Considerations for Government Investigations

- Assume that all sources of corporate communications are within the intended scope of informal and formal document requests.
- Often IM/chat data is the most sought-after evidence given the likelihood for damaging evidence or off-the-cuff remarks.
- If no production specifications accompany the government information request, consider what format might be strategically the best approach.
- Take steps to identify and preserve IM/chat app data as soon as practicable to ensure no inadvertent data loss, especially if legal hold capabilities are not built into your applications or subscriptions.

Final Thoughts and Speaker Takeaways

Actionable Takeaways

- Keep A Clean House
  - Confirm that corporate policies are current and address the use and management of corporate IM/chat App data.
- Knowledge Is Power
  - Make sure the Legal Department understands all potential sources of corporate IM/chat App data and has a clear understanding of preservation and collection options and workflows.
- Be Proactive
  - Engage actively with outside counsel to develop a preservation and collection approach that is consistent with both internal capabilities and production expectations.

Actionable Takeaways

- Good Things Do Not Come To Those Who Wait
  - To the extent IM/chat App data may be implicated, address those data sources with haste and review the questions posed in this slide deck to ensure readiness.
- Personal Devices Should Not Be Ignored
  - If employee text message/chat app data resides on personal devices and may become relevant to a litigation or investigation, best practice suggests taking a preservation image as early as possible for implicated devices.
- There Is Nothing To Fear But Failing To Plan
  - IM/chat app data is no different than other more traditional communication evidence, if proactive and responsible steps are taken at each phase of the e-discovery lifecycle.

Helpful Links

- In re Google Play Store Antitrust Litigation, No. 21-MD-02981-JD, 2023 WL 2673109, at *10 (N.D. Cal. Mar. 28, 2023).
- https://bostonbar.org/journal/district-court-cuts-litigants-no-slack-for-failing-to-produce-corporate-instant-messaging-data-resulting-in-default-judgment/
- https://thesedonaconference.org/publications
- https://thesedonaconference.org/sites/default/files/publications/6_Ephemeral_Messaging_1.pdf
- https://edrm.net/resources/data-sets/

MINTZ

Questions?