



# What Does a NextGen E-Discovery Playbook Look Like?



You've exchanged information with your clients via text messages.  
You've collaborated with your colleagues on Microsoft Teams or Skype for Business.  
You've seen the court cases referencing the use of social media. So, as technologies for communications and collaboration continue to move away from email and static documents, how should a firm adjust its e-discovery playbook? That's the question we aim to tackle in this brief guide.

# What Does a NextGen E-Discovery Playbook Look Like?



## Common Questions

Every new communications and collaboration technology is different, each with its own unique set of capabilities to create, modify, preserve, and share content. However, we find that e-discovery managers seeking to update their e-discovery playbooks inevitably stumble upon the same crucial questions.

### These are just a few to keep in mind:

- 1 How can you match custodians to all of their content sources?
- 2 What methods are available to collect and preserve these content sources?
- 3 How can legal teams review rich, dynamic collaborative content?
- 4 How can metadata and conversational context be delivered for production?

## 1 How can you match custodians to all of their content sources?

**Answer:** Data mapping needs to be re-shaped as “identity mapping”

**Explanation:** Every e-discovery manager has experienced the challenge of mapping the content source, owner, and access method to each custodian. Now, add the complexity of screen and buddy names and the challenge of recognizing that “ThatGamerDude” on Twitter is actually a person of interest with an existing identity in your company’s corporate directory structure. Now, multiply that complexity by 30 to 40 different content sources that are being used by that custodian to do their job. In short, you can’t map this universe in real time. As a result, NextGen Playbooks are increasingly calling for the creation and on-going mapping of identities – from users to all the content sources that they have been authorized to conduct business over so that firms can stand ready whenever that person appears on a custodian list.

### Next steps:

- Inventory all communications and tools that employees are authorized to use to conduct business
- Capture all screen names, buddy names, identifiers used by each employee
- Update identity mapping on a quarterly basis, and as new tools are authorized

## 2 What methods are available to collect and preserve these content sources?

**Answer:** Every new content source is unique, requiring its own method of collection

**Explanation:** Social media, text messaging and mobile applications, and collaborative content from sources like Microsoft Teams and Slack all behave differently, and each was designed with its own set of capabilities to capture content from the source. Some have full APIs, others none at all. Some can be captured by third party technologies or forensic services, while others may require a time-consuming service request to retrieve historical content, as is the case with mobile carriers. A few make it even more complex with the use of encryption and other methods to protect user privacy. What is clear is that rudimentary methods such as screen scraping or snapping a picture of someone's Facebook wall may not always withstand court scrutiny.

### Next steps:

- Update records retention policies to reflect cost, complexity, and uncertainty of reactive collection
- Clarify policies: employees cannot use anything that cannot be reliably captured
- Legal teams should be engaged when new content sources are evaluated for business use to ensure that a reliable, defensible method of collection has been vetted, documented and can be added to the NextGen E-Discovery Playbook

NextGen E-Discovery Playbooks need to start and end with good information governance.

In *Commonwealth v. Mangel*, the Superior Court of Pennsylvania disallowed into evidence a social media post presented by the prosecution as a simple screen shot.



### 3 How can legal teams review rich, dynamic collaborative content?

**Answer:** Review needs to respect native context and metadata

**Explanation:** The legal review tools in use by most firms today were designed when the predominant form of electronically stored information (ESI) was email and scanned documents. That world was linear and static – a document that may have been preceded by or followed with a similar document with different version number or time stamp; an email that may have a follow-up reply or forward. Unfortunately, today’s social and collaborative technologies are dynamic, context-sensitive, and multi-dimensional: a conversation happening over a series of tweets, a chat room where individuals join, leave, edit content and interact via video, whiteboards, or voice – and sprinkled with added context in the form of emojis. None of those active, interactive elements translate well into a static review environment. In fact, most review platforms continue to use conversational threading to figure out who said what, who participated in an event, or who may have taken an action that led to the issue in question. This is not effective.

#### Next steps:

- Examine existing review tools ability to preserve native attributes of each content source
- Incorporate ‘events’ (join/leave, content edits, etc.) into review workflow to account for dynamic, collaborative platforms
- Evaluate new review solutions that preserve non-text based content sources

NextGen E-Discovery Playbooks must call for the use of modern review technologies that are focused on understanding the data – not just how to improve the review rates of documents.

### 4 How can metadata and conversational context be efficiently delivered for production?

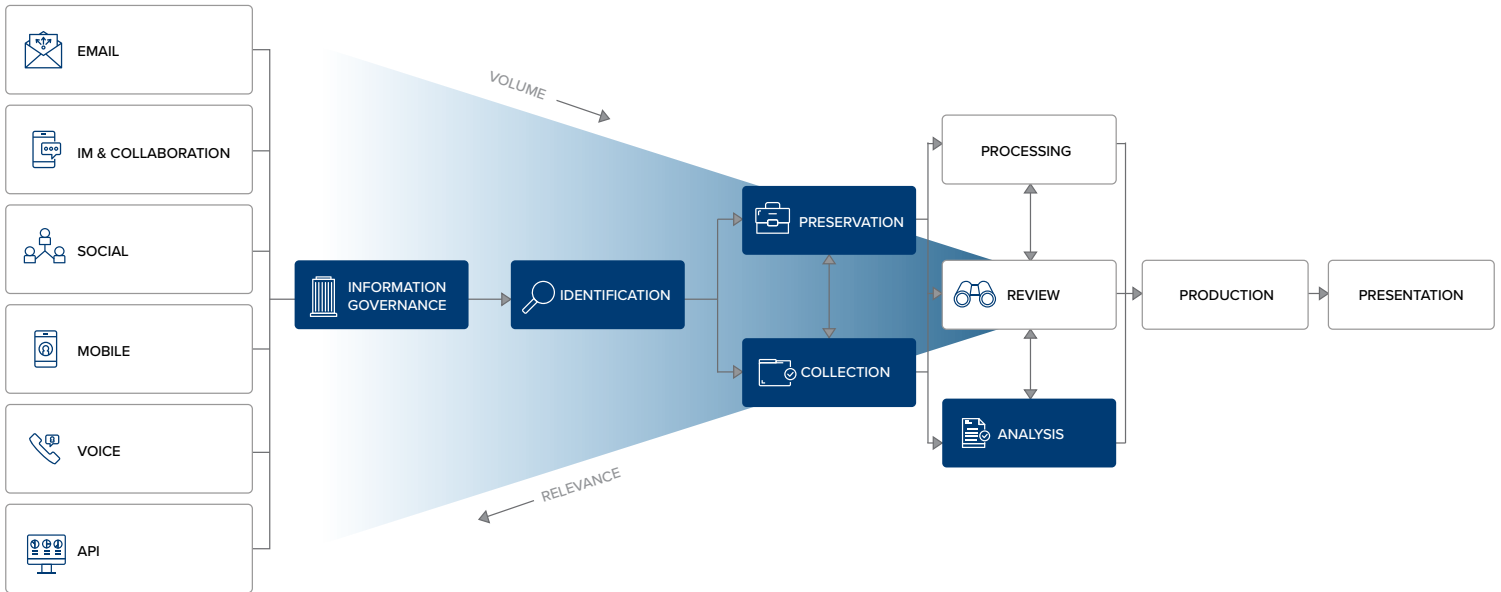
**Answer:** E-discovery throughput needs to be redefined

**Explanation:** Firms have traditionally evaluated the performance of an e-discovery platform and efficiency of workflow in terms of ingestion and export rates. However, the reality of new content sources has fundamentally changed the equation. Metadata and event information preserved as ‘objects’ can impose new burdens on systems designed primarily for email and document payloads – even more so if those systems were designed for operation on-premises. As firms think about these rich new sources of content, they need to re-examine their assumptions for ingestion rates and times, as well as their ability to export content, context, and metadata so that it is not creating a bottleneck for the next step in their e-discovery workflow.







#### Next steps:

- Examine ingestion and export rates of all content attributes encountered in legal review
- Understand non-email and file integration capabilities of e-discovery analysis and production tools

NextGen E-Discovery Playbooks need to acknowledge that the shift away from email and documents is nothing short of a redefinition of the basic unit of work. The task is no longer about finding a needle in a haystack. It’s about finding multiple unique needles in multiple unique haystacks.



## Components of a NextGen E-Discovery Playbook

- 
**Governance:** ensuring your policies are updated to define acceptable and prohibited business uses for each network, as well as to define the role for e-discovery professionals in the evaluation of new communications tools
- 
**Identification:** ensuring that identities can be proactively mapped between custodians and content sources
- 
**Preservation:** definition of preservation methods to be used for non-IT and non-custodian controlled content sources, including social media and mobile applications
- 
**Collection:** outline of the methods to be employed to collect from each content source, whether it be dependent on the native content source provider, 3rd party technologies or forensic services, or internal IT staff
- 
**Review:** assessment of current review technologies to address unique content modalities from each new network, including voice, video, whiteboards, join/leave/modify events, emojis, and other non-text information
- 
**Analysis:** similar to above, assessment of whether existing analytics or predictive coding technologies can process new content sources, or if reviewed data can be exported to third party applications at required throughput

The update to your existing e-discovery plans will depend on numerous factors including the volume and variety of communications, collaborative channels, and applications your organization employs for both internal and external communications, your internal policies, as well as your e-discovery patterns.

In altering your e-discovery plan, your ultimate goal should be the minimization of risk. While it's not possible to eliminate all forms of risk entirely, a thoughtful attempt at updating your e-discovery efforts should help properly position your firm to both mitigate known risks and react appropriately to risk that may be uncovered down the line.



Smarsh® helps organizations get ahead – and stay ahead – of the risk within their electronic communications. With innovative capture, archiving and monitoring solutions that extend across the industry’s widest breadth of channels, customers can leverage the productivity benefits of email, social media, mobile/text messaging, instant messaging/collaboration, websites and voice while efficiently strengthening their compliance and e-discovery initiatives.

A global client base, including the top 10 banks in the United States and the largest banks in Europe, Canada and Asia, manages billions of conversations each month with the Smarsh Connected Suite. Government agencies in 40 of the 50 U.S. states also rely on Smarsh to help meet their recordkeeping and e-discovery requirements.

The company is headquartered in Portland, Ore. with nine offices worldwide, including locations in Silicon Valley, New York, London and Bangalore, India. For more information, visit [www.smarsh.com](http://www.smarsh.com).

