# 6 Keys for Effective and Defensible ESI Collections

## Description

If youâ??re involved in digital forensics, litigation support, or legal operations, developing a defensible strategy for collecting electronically stored information (ESI) is non-negotiable. The volume, velocity, and variety of data in modern environments, from Slack messages to mobile devices, demand a more intentional approach to ESI collection.

In a recent EDRM webinar, Pinpoint Labs Jon Rowe and Jamie Beasley joined Brett Burney of Nextpoint Law Group to share best practices based on real-world experience. These six keys outline how to prepare, execute, and validate a precise and defensible collection strategy thatâ??s both practical and future-ready.

### 1. Plan ESI Collections With Intent and Structure

A vague request like â??grab the mailboxâ?• is no longer sufficient. A legally defensible and technically accurate collection starts with structured planning. Key planning actions include:

- Identifying all data sources (local drives, SaaS platforms, mobile apps)
- Mapping custodian responsibilities and systems
- Documenting workflows, legal hold status, and collection scope

â??Defensibility starts with preparation. Without a clear map, your collection risks missing key data or over-collecting irrelevant noise,â?• shared Rowe.

Planning ensures the right people, tools, and data are aligned from the beginning, mitigating downstream delays and legal risk.

### 2. Use Supervised Self-Collection to Balance Scale and Control

While traditional self-collection raises defensibility concerns, supervised self-collection (when paired with oversight and validated tools) is a scalable and defensible solution.

Tools like Pinpoint Labsâ?? Harvester and SafeCopy tools help organizations to:

- Remotely assist custodians during collection
- Maintain control and chain of custody
- Script automated collections with defined filters (dates, file types, locations)

â??Itâ??s not about cutting corners. Itâ??s about using smart tools to meet real-world constraints without sacrificing integrity,â?• said Burney.

This approach is especially useful in large enterprises or remote environments where direct IT collection may not be feasible.

**3. Prioritize Privacy and Compliance in Mobile and Cloud Collections**

Todayâ??s data isnâ??t just on hard drives. Itâ??s in pockets and clouds. Mobile phones, Microsoft Teams, Google Drive, and WhatsApp contain critical information that must be collected correctly and ethically. Modern collection tools should:

- Offer private previews before data leaves the device
- Respect jurisdictional privacy rules (e.g., BYOD environments, GDPR)
- Provide targeted collection options by app, date range, and contact

â??When people know they have visibility into whatâ??s being collected, cooperation goes up and defensibility follows,â?• commented Beasley.

Planning for mobile device forensics and cloud data access from the start is essential in complex cases.

**4. Redefine Custodianship in the Age of Collaboration and AI**

Custodianship used to mean a personâ??s laptop or inbox. Now, itâ??s shared documents, department-owned data, and even AI-generated content. For a complete and contextual ESI collection:

- Consider all contributors to dynamic content (e.g., Google Docs, Microsoft Loop)
- Map out system-generated data sources like logs or AI outputs
- Identify who is accountable, not just who authored the content

This evolution is essential for investigations that involve collaborative platforms or cloud-native files.

**5. Embed Defensibility Into the Process, Not Just the Output**

Audit trails, error logs, and hash verification are not optional. Theyâ??re the foundation of defensibility. Invest in tools built to:

- Log every action in real-time
- Capture snapshots of job parameters
- Generate chain-of-custody reports automatically

â??Defensibility means you can show your work (every setting, every exclusion, every file hash) and show it immediately, not weeks later,â?• said Rowe.

Regulatory teams, opposing counsel, and judges expect this level of detail. Youâ??ll also want this information if any questions arise.

**6. Filter Early to Save Time, Money, and Review Headaches**

Pre-collection filtering isnâ??t about cutting corners. Itâ??s about collecting with purpose. Strategic filtering improves data quality and lowers the cost of review. Common tactics include:

- Indexing content before collecting to test keyword sets
- Collecting broadly but filtering by file types, dates, or sources before upload
- Retaining raw collections in a staging environment for reprocessing if needed

â??Cast a wider net on the device, then apply smart filters post-collection. Youâ??ll save time, avoid rework, and still maintain control,â?• said Beasley.

Early filtering also supports Legal Hold optimization and data minimization strategies, both of which reduce risk.

## Final Takeaway: Align Collection With Your End Goals

Whether youâ??re preparing for litigation, responding to a regulatory request, or conducting an internal investigation, your ESI collection strategy must align with the review and production phase from day one.

By applying these six keys (planning rigorously, supervising collections, protecting privacy, expanding custodian scope, ensuring defensibility, and filtering early), youâ??ll be better equipped to handle todayâ??s data complexity with confidence and clarity.

---

Want to learn more about Pinpoint Labsâ?? approach to defensible collections? Visit our product overview.

**Date**
04/20/2026
**Date Created**
08/20/2025