Custodianship in a Collaborative Age

By Greg Buckles – www.eDiscoveryJournal.com

September 21, 2023

Has collaborative ESI broken the traditional concept of custodianship? Putting aside collaborative messaging ESI, collaborative 'documents' or workflows may challenge the traditional possession, custody or control tests for admission of evidence in legal proceedings. Beyond authentication, practitioners should assess and adapt their eDiscovery workflows in light of these new ESI types and sources.

> **Rule 901**. Requirement of Authentication or Identification (a) General provision.—The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.
>
> **Rule 34(a)(1)** specifies that parties may only request the production of documents or electronically stored information (ESI) "in the responding party's possession, custody or control."
>
> **Rule 30(b)(6)** Notice or Subpoena Directed to an Organization. In its notice or subpoena, a party may name as the deponent a public or private corporation, a partnership, an association, a governmental agency, or other entity and must describe with reasonable particularity the matters for examination.

What has changed?

Traditional ESI – based on 1 to 1 document to custodian relationship. A single custodian created or possessed a single piece of ESI. Copies were transmitted with email or other container context. Custodians authenticate ESI as evidence based on their possession, custody or control. Changes tracked as whole document versions.

Collaborative ESI – Can be created within the shared workspace or as collaborative components embedded in personal repositories. Shared workspaces are generally controlled by administrators, policies and architectural features. Shared workspaces are generally based on topics, projects, departments or other broader concepts. Collaborative ESI can be stored in a wide variety of locations depending upon the applications, systems, content type and other factors.

Possession Then and Now

Corporate business usage of email took off in the mid-1990s with the advent of webmail. However, it was almost exclusively printed to paper/image in civil litigation until the early 2000's. Federal prosecutors and regulators demanded large volumes of native ESI during the waves of criminal corporate financial and energy scandals of that era. The first draft of The Sedona Principals was published in 2002, defining Electronically Stored Information and paving the way for the 2006 and later amendments to the Federal Rules of Civil Procedure.

It is my assertion that eDiscovery rules, technology and common practices have continued to treat ESI content and repositories as simplistic extensions of a custodian's physical filing cabinet. Email is seen as a digital version of physical correspondence, even when it now contains dynamic content, embedded actions and other extended functionality connected to external systems and entities.

The transition from enterprise email, file shares and workstations to cloud based global platforms such as Microsoft 365 and Google Workspace means that ESI is no longer 'possessed' by custodians or corporations. These cloud platforms provide retrieval mechanisms, but customers can no longer physically access the storage or content on demand.

Who has Control in the Cloud?

Many cloud platforms support customer supplied encryption for security, privacy and protection of ESI. This prevents the platform hosts and external parties from accessing the encrypted content. Does that constitute the legal definition of 'control' if a custodian has limited retrieval or access capabilities to the full context and metadata of their ESI?

The advent of 'modern attachments' stored in SharePoint libraries, Teams channel mailboxes and other shared repositories poses distinct challenges to the concept of singular custodianship. Modern attachments are essentially just a sharing link with access permissions to ESI on a variety of shared storage. Depending on access rights, the shared document, spreadsheet or other ESI may have been completely revised or even created by multiple individuals. So who is the custodian? Are they the custodian of only the content that they have contributed to the final version? Are they the custodian of the version that existed the moment that the access link was sent?

Custodial approaches

Administrative custodianship – One approach is to designate corporate administrators or retrieval specialists as the 'custodians' of collaborative platforms such as Teams, Dropbox and web wiki's. These 'super users' understand the system policies, technologies and retrieval methods used to preserve, collect, process and produce this shared ESI. While this approach supports chain of custody and overall system authentication as a potential Rule 30(b)(6) witness, it does not provide the parties access to the business context of why and how the ESI was created. The 'custodianship' is divided between the eDiscovery/technology process and the fact/contributor witnesses.

Repository owner custodianship – Most Teams channels, workspaces or other collaborative portals have a business owner or moderator whom manages access, organizes content and has the best knowledge of the overall repository. This approach supports efficient authentication of larger collections of ESI relating to the scope. As with the Administrative custodian, this custodian may not have knowledge about specific items, collaborator roles or even content creation workflows.

Item creator custodianship – In this approach, ESI is associated with the original creator of the collaborative ESI. They generally have the most knowledge regarding the ESI purpose and context.

Final editor custodianship – The 'modified by' metadata field can sometimes be used to assign custodianship based on the last contributor to have modified the ESI. They may have the best knowledge of how the final version came to be and the revision history.

Version custodianship – In systems that support full version storage by policy or legal hold application, it may be possible to retrieve every version by the contributor and date/time. While this approach is complicated and can balloon eDiscovery volume/costs, there are scenarios such as contract clause negotiations, evidence tampering or untangling executive decision context that justify the impact.

Next Generation of Collaborative ESI

Modern attachments have been around for several years, though they are now built into most messaging platforms. Microsoft Loop and Google Smart Canvas introduce next generation collaborative components that may challenge our traditional custodianship models. Users can embed dynamic elements such as tables, polls, task lists and more in chats, emails, whiteboards and other 'locations'. While the early versions of components

seemed like more convenient 'modern attachments', they act as 'live' documents and frequently lack compliance and eDiscovery functionality such as versioning, edit history and ability to merge metadata/context of all collaborators. Their architecture and often hidden storage locations make them behave more like disappearing messages.

Beyond collaborative components are the latest wave of collaborative cloud applications such as the Loop Workspaces, Notion, Smart Canvas and more where the ESI only exists behind the web interface. Loop Workspaces move storage to Microsoft Syntex repository services environment that is inaccessible by customers except through the appropriate APIs. While the compliance and eDiscovery functionality will eventually catch up to the traditional apps, the innovative interfaces break down old fashioned 'document' architypes.

Summary

Civil discovery rules, caselaw and practices have lagged behind rapidly evolving business and collaboration technologies. Many eDiscovery platforms are still struggling with multiparty short message ESI and modern attachments. Practitioners should consider the unique content, players, issues and parties involved in matters before determining the best custodianship approach when negotiating eDiscovery protocols and declarations. Early data assessment and identification of key ESI is critical to ensuring that potential evidence can be authenticated and presented in context.