Professional Perspective

Risks of Custodian Self-Collections in eDiscovery

Elan Hersh, Akerman LLP, and Ivan Feris, Continental PLLC

Bloomberg Law

Risks of Custodian Self-Collections in eDiscovery

Editor's Note: The views expressed in this article are those of the authors and do not purport to reflect the views or position of their respective law firms.

Contributed by Elan Hersh, Akerman LLP, and Ivan Feris, Continental PLLC

In the electronic age, attorneys and litigants are faced with the task of identifying, preserving, and collecting electronically stored information (ESI) during discovery. Attorneys generally ensure that ESI is preserved by issuing a "litigation hold," which instructs litigants to preserve ESI that is potentially relevant to an anticipated litigation. "Self-collection" by a records custodian is when a litigant with relevant ESI personally engages in the identification, preservation, and collection of their own data.

Litigants gravitate toward self-collection to save time and money, especially if the client believes it is best positioned to find its own responsive documents. Yet, attorneys have a duty to adequately supervise litigants during self-collection or risk sanctionable discovery failures.

This article discusses the risks of custodian self-collection, and how courts balance countervailing interests in ordering forensic collection of ESI to overcome those concerns.

Pitfalls of Self-Collection

With minimal attorney instruction, self-collection has significant downsides that can ultimately lead to judicial intervention. Prevalent issues with self-collection include failure to: identify sources of responsive information, preserve evidence, locate all relevant documents, and fully disclose documents. What's more, in certain cases where self-collection has been deemed to be insufficient, courts may go as far as to order a forensic analysis of a party's ESI.

Sources of Responsive Information

An attorney has a heightened duty to instruct her clients on relevant information for self-collection or else risk a client's failure to identify all responsive ESI. In *Board of Regents of University of Nebraska v. BASF Corporation*, corporate defendants moved to compel discovery of ESI from a university-board plaintiff for its failure to disclose all relevant ESI. The attorney for the university allowed the client to self-collect without direction or supervision, resulting in voluminous and delayed disclosures. The court reasoned that the university's attorney failed to properly instruct and supervise his client, and failed to issue a litigation hold, warranting sanctions. See *Bd. of Regents of University of Nebraska v. BASF Corp.*, No. 4:04CV3356., 2007 BL 150167, (D. Neb. Nov. 05, 2007).

Preserving Evidence

Another downside of self-collection is the failure to preserve ESI. Counsel and litigants have a duty to preserve ESI when litigation is reasonably anticipated and failure to do so may result in sanctions. A court may find that forensic analysis of a parties' ESI is appropriate when counsel fails to issue a litigation hold. In *Procaps v. Patheon Inc.*, attorneys never met with their client to understand the client's ESI storage system. The attorney allowed the client to self-collect, leading to discovery deficiencies that the court reasoned justified forensic analysis of the client's ESI to ensure that relevant information was located and preserved. See *Procaps S.A. v. Patheon Inc.*, 2014 BL 55511,12-24356-CIV-GOODMAN (S.D. Fla. Feb. 28, 2014).

A party's failure to adequately preserve ESI is also sanctionable behavior. In *Nacco Materials Handling Group, Incorporated v. Lilly Corporation*, the court ordered forensic analysis of a defendant corporation's computer system, where ESI was inadequately preserved. Upon suit, the corporation's attorney issued a litigation hold to the corporation's president, who waited two weeks to issue it to only seven corporation employees without further instruction. The court determined that the corporation's duty to preserve arose, at earliest, when the lawsuit was filed. The court held that the corporation failed to ensure that ESI was properly preserved, and took no steps to collect relevant ESI, leaving the employees to self-collect information without guidance. See *NACCO Materials Handling Group, Inc. v. The Lilly Co.*, 278 F.R.D. 395 (W.D. Tenn. 2011).

Producing Responsive Documents

Even if a litigant identifies the universe of relevant information for a case, the party may fail to find or produce all responsive documents. In *Radiologix, Incorporated v. Radiology & Nuclear Medicine, LLC*, the court discussed a discovery failure resulting from a search error. The parties agreed on specified search terms, and one party gathered its ESI into a database and ran the agreed search terms. Counsel produced the populated documents, but not all responsive documents were identified because of a mistaken setting on the search field parameters. Although the court did not impose sanctions because the error was a technical oversight, rather than a failure by counsel to direct the party, the mistake led to incomplete discovery in this case. See *Radiologix, Inc. v. Radiology & Nuclear Med., LLC*, No. 15-4927-DDC-KGS, 2019 BL 28486, (D. Kan. Jan. 29, 2019).

Conversely, courts have required forensic analysis where incomplete discovery results from an attorney improperly directing clients on how to search for ESI. In *Procaps,* an attorney never instructed his client on how to conduct a search or what to search for. The client's agents self-searched and self-collected ESI in an email database, using only one search term and limiting the parameters of the search to correspondence between the parties to the litigation, in exclusion of internal emails that may have contained relevant information. The court held that the client's searches were inadequate; therefore, forensic analysis of the databases was appropriate.

The process of crafting appropriate search terms for ESI should be a cooperative undertaking that includes both parties' ESI experts. However, incomplete discovery may also arise with self-collection where a party deliberately withholds certain ESI from opposing parties. In *Wachtel v. Health Net*, Incorporated, an insurer failed to produce thousands of documents until the court intervened or until it was useful for the insurer's case. The insurer engaged in self-collection where a company paralegal instructed specific employees to search for specific documents.

Counsel did not inquire about the completeness of the searches, resulting in the custodians willfully omitting thousands of inculpatory emails and other ESI from discovery. The insurer did not issue a litigation hold until two years into discovery, even though its ESI retention system deleted emails every ninety days. The insurer also failed to search back up data for responsive correspondence. The court ordered sanctions against the insurer. See *Wachtel v. Health Net, Inc.*, 239 F.R.D. 81 (D.N.J. 2006).

Documenting Your Discovery Efforts

Failure to keep detailed documentation about how searches are conducted is another concern. In self-collection, the client may fail to document the sources of information searched or the search methods used, which makes self-collection less defensible. In *DR Distribs., LLC v. 21 Century Smoking, Inc.*, the custodian for the defendant distributor self-collected ESI, asserting that four computers contained all the responsive information. An expert in ESI was outsourced solely to search through and to conduct mirror imaging of those computers' hard drives.

However, defense counsel did not properly investigate the fact that the defendant used web-based sources to store data in the cloud, rather than in the four hard drives. This misrepresentation by the custodian led to a myriad of discovery issues such as spoliation of web-based emails and chats. Despite several meetings between the custodian and defense counsel regarding a protocol, no documentation of any kind was created about these meetings. The court noted, "[t]he lack of documentation permeates this entire case."

The court stressed the importance of the documentation where a client is left to self-collect ESI in order to defend challenges to actions taken during discovery. The court imposed sanctions against the defendant and his lawyers for, among other things, the failure to document the steps taken to self-collect ESI. See *DR Distribs., LLC v. 21 Century Smoking, Inc.*, No. 12 CV 50324, 2022 BL 358733, (N.D. Ill. Oct. 06, 2022).

Forensic Analysis

Forensic analysis typically involves a computer forensic technician undertaking a process of imaging and searching ESI storage systems. Forensic analysis may involve mirror imaging—"a forensic duplicate, which replicates bit for bit, sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive." Courts generally agree that ordering forensic analysis of ESI "is highly intrusive" and are hesitant to allow litigants unbridled access. Courts weigh this right to information against a responding party's right to confidentiality and privacy.

If an electronic device or computer is the focus of a claim, courts are more likely to allow forensic analysis of an opposing party's ESI. In *Weatherford U.S., LP v. Innis*, an oil refinery plaintiff brought suit against a former employee who allegedly downloaded files from the refinery's computer onto a thumb drive and misappropriated the information. The thumb drive was subjected to forensic analysis, uncovering files downloaded without authorization. The refinery sought further imaging of the former employee's computers, but he objected that the imaging would be unduly intrusive. The court held that there was a sufficient nexus between the computers sought to be analyzed and the litigation, and ordered forensic analysis. See *Weatherford U.S., LP v. Innis*, Case No. 4:09-cv-061., 2011 BL 145680, (D.N.D. June 02, 2011).

Courts are inclined to compel forensic analysis of ESI where there are discovery failures. For example, in *In Re Abilify*, the defendant manufacturer sought to compel the electronic records of the plaintiffs' online gambling habits, which were relevant to causation and damages issues. The plaintiffs disclosed bank records and other information, but they were insufficient to ascertain all the gambling activity. The manufacturer requested the court to compel forensic analysis, despite the plaintiff's objection that it would be unduly intrusive. The court balanced the intrusiveness of the forensic analysis compared to its utility and held that forensic analysis was appropriate because the plaintiffs had self-collected ESI without instruction on how to properly search for relevant information. See *In re Abilify (Aripiprazole) Prods. Liab. Litig.*, No. 3:16-md-2734, 2017 BL 546913, (N.D. Fla. Dec. 07, 2017).

Self-Collection Successes

Self-collection is more likely to succeed when it is executed with proper precautions, including: issuing a written litigation hold that addresses auto-delete features, instructing the custodian to conduct a thorough search, inquiring into the custodian's collection methods, and documenting the measures taken. In *Mirmina v. Genpact LLC*, the court compelled a defendant company to search for additional ESI. The defense counsel recounted the steps taken, which were issuing a litigation hold, instructing the custodians about specific search parameters, and remaining involved throughout the collection. After the self-collection was complete, the in-house defense counsel forwarded the findings to outside defense counsel for further review. The court held that, despite self-collection, these steps were sufficient to ensure integrity in the discovery process. See *Mirmina v. Genpact LLC*, No. 3:16CV00614 (AWT), 2017 BL 260425, (D. Conn. July 27, 2017).

Similarly, in *Nissan North America, Inc. v. Johnson Electric North America, Inc.*, a plaintiff corporation moved for a protective order, where the defendant requested that the corporation produce information regarding how data was stored, who accessed it, and how it was retained. The corporation had been ordered to supplement discovery earlier in the litigation, and, as a result, had already produced almost two million pages of ESI. The defendant alleged that the ESI produced was incomplete. The corporation argued that its self-collection was sufficient to uncover all responsive ESI and that backup files were not readily accessible. The court was satisfied with the diligent self-collection process of the corporation.

Concluding Tips

Considering the dangers of custodian self-collection, attorneys can mitigate the risks to themselves and their clients through engaging an ESI expert. Lawyers who do not specialize in the constantly evolving world of eDiscovery, would be well advised to engage ESI experts early in a litigation to avoid costly mistakes or overly-intrusive discovery being ordered by a court later on.

Short of this, keep in mind the below practical tips to guard against the risks of spoliation, deficient document productions, and other eDiscovery problems.

Circulate a Litigation Hold Notice

Make sure to circulate a litigation hold notice to all relevant data custodians as soon as litigation is reasonably foreseeable. Track who has received the litigation hold notice and send periodic reminders to ensure that the preservation directive remains top of mind for the data custodians. Preserve broadly so that if a custodian neglects to include relevant documents as part of their collection, the data will still be available for collection at a later date. Make sure the hold notice goes to the organization's IT department, which should suspend auto-deletion programs covering relevant files.

Be Aware of Search Limitations

Be aware that documents with no searchable text, like imaged versions of PDFs, will ordinarily not be picked up when searching email in Microsoft Outlook or when searching electronic documents in Windows. Therefore, a PDF attachment to an email which contains a search term but does not have extracted text will not be returned in a keyword search in Outlook. For this reason, it is recommended to export a custodian's full mailbox for the relevant time period so that it can be processed using eDiscovery software. Among other things, processing data involves making non-searchable text searchable, indexing the files, and extracting documents from compressed container files–e.g., ZIP and RAR files. Once the data is processed, search results are more accurate.

Be Careful With Metadata

One of the biggest problems with custodian self-collection is that the metadata of loose native files can be easily altered when a custodian moves a document. While collecting documents forensically is the gold standard for data collection, one method for collecting standalone files or folders without altering the underlying metadata is to "containerize" the files by zipping them up into a compressed container file, like a ZIP file, or exporting MS Outlook email into a PST container file. Once the data is "containerized," the container file can be moved or copied without changing the metadata of the contents within the container.

Memorialize Your Process

Keep detailed notes of the steps you have taken to preserve and collect ESI. Your opponent may attempt to undermine your case by calling into question the defensibility of your discovery efforts. To avoid having the merits of your case derailed by time-consuming and costly discovery disputes, make sure to document the steps you and your client have taken to preserve, collect, review, and produce relevant documents.

Stipulate to an ESI Protocol if Possible

Attorneys can reduce the likelihood of costly discovery disputes by entering into an agreed-upon ESI protocol with opposing counsel before undertaking document discovery. These agreements, known as "ESI Protocols," ordinarily set forth the parties' agreement on various items, including but not limited to:

- The relevant time period from which ESI should be preserved, collected, and searched
- Data sources considered inaccessible (and therefore not subject to being searched)
- The list of custodians who may have relevant documents
- Keyword search terms to identify relevant documents
- The format of production for ESI
- The protocol for deduplicating documents and applying analytics technology
- The list of metadata fields to produce

A stipulated ESI protocol can be a valuable tool for counsel wishing to get through the eDiscovery process with less disagreement and conflict.

With assistance from Asha Wedemier-Allan.