THOMSON REUTERS
PRACTICAL LAW™

Possession, Custody, and Control of ESI in Federal Civil Litigation

by William J. O'Brien III and Patricia A. McNulty, Skadden, Arps, Slate, Meagher & Flom LLP, with Practical Law Litigation

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-002-9023**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

Neither the FRCP nor existing case law provide bright-line rules on who has control over discoverable ESI that resides in multiple places. This Practice Note examines the applicable federal rules on the possession, custody, and control of ESI, the traditional tests that courts use to determine control over documents and ESI that nonparties possess, and emerging jurisdictional issues relating to cloud-based ESI.

The Federal Rules of Civil Procedure (FRCP) require parties (and some nonparties) to preserve and produce electronically stored information (ESI) in their "possession, custody, or control." Organizations and individuals store discoverable ESI in many locations, including on network servers, computer hard drives, cell phones, and social media websites, such as Facebook, Twitter, and LinkedIn. ESI is also increasingly generated and stored in the "cloud," as more organizations and individuals use internet-based computing for business and personal purposes. Cloud computing users can access a variety of proprietary and commercial software applications through the internet and use these applications to create and store emails, instant messages, chat messages, ephemeral messages, enterprise systems, voice files, and video files This ESI typically is hosted on servers maintained by cloud service providers, rather than by the individual or organization generating the content.

The proliferation of ESI and growing use of cloud computing, as well as the increasingly complex structures of large, multinational organizations, have led to significant and costly discovery-related issues in litigation. Although the duty to preserve and produce ESI has a straightforward application for documents (including ESI) in a party's physical possession or actual custody, neither the FRCP nor their accompanying advisory committee notes provide a definition of "control." This ambiguity is particularly problematic with ESI that resides on servers in multiple jurisdictions and is accessible to countless entities and individuals.

This Note discusses:

- The FRCP that address the possession, custody, and control of ESI (see Applicable Rules).
- The traditional tests that courts use to determine control over documents that a nonparty possesses (see Tests for Control).
- How courts analyze an entity's control in common factual scenarios (see Analyzing Control in Common Circumstances).
- Emerging jurisdictional issues relating to cloud-based ESI (see Stored Communications Act Warrants and Foreign-Stored ESI).

Applicable Rules

References to the possession, custody, and control standard appear throughout the FRCP and most commonly refer to:

- **Initial disclosures.** FRCP 26 requires a party to produce documents and ESI in its possession, custody, or control that it may use to support its claims or defenses (FRCP 26(a)(1)(A)(ii)).
- **Discovery requests and responses.** FRCP 34 permits a party to request (and requires a responding party to produce) nonprivileged documents and ESI that are:
  - in the responding party's possession, custody, or control; and
  - within the scope of discovery under FRCP 26(b).

  (FRCP 34(a)(1).)While FRCP 33 is silent on the issue, some courts have found that a party's interrogatory responses should similarly reflect information under the party's control, even if the information is possessed by a nonparty (see, for example, *Costa v. Kerzner Int'l Resorts, Inc.*, 277 F.R.D. 468, 471 (S.D. Fla. 2011)).

- **Nonparty subpoenas.** FRCP 45 requires a subpoena recipient to produce requested, nonprivileged documents and ESI that are within its possession, custody, or control (FRCP 45(a)(1)(A)(iii)).
- **30(b)(6) depositions.** Courts have applied the FRCP 34 control standard to require corporate representatives to be reasonably knowledgeable about information under the corporate party's control during the FRCP 30(b)(6) deposition, even if the information is in a nonparty's possession (see, for example, *In re Benicar (Olmesartan) Prod. Liab. Litig.*, 2016 WL 5817262, at *5 (D.N.J. Oct. 4, 2016)).
- **Sanctions for preservation failures.** Although the phrase does not appear in FRCP 37(e), some courts borrow the FRCP 34 control standard to impose sanctions on parties who failed to preserve relevant ESI. These courts have found that:
  - a party's duty to preserve extends to all documents and ESI under its control, even when the ESI resides with a nonparty; and
  - courts may sanction a party for failing to ensure that the nonparty preserves relevant ESI.

  (See, generally *La Belle v. Barclays Cap. Inc.*, 340 F.R.D. 74, 81 (S.D.N.Y. 2022) (explaining that an element to demonstrate a spoliation claim is "that the party having control over the evidence had an obligation to preserve it at the time it was destroyed"); see also, for example, *U.S. Equal Emp. Opportunity Comm'n v. MVM, Inc.*, 2020 WL 6482193, at *1 (D. Md. Nov. 2, 2020) (affirming order for sanctions where party had control over documents that were in a non-party's possession); *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179, 195-96 (S.D.N.Y. 2007) (finding that because the defendant had control under FRCP 34(a), it had a duty to preserve ESI possessed by a nonparty affiliate).)

In connection with the 2015 amendments to the FRCP, the FRCP advisory committee acknowledged that the increasingly vast stores of ESI created by billions of internet applications pose unique and persistent discovery and evidentiary problems. The advisory committee also highlighted the specific challenge posed by ESI moving to the cloud and placing ESI in a nonparty's possession and custody. To address these concerns, the committee recommended that a court generally should not sanction a party for ESI spoliation if the ESI was lost due to events beyond the party's control (such as natural disasters, cyber attacks, or unforeseeable insolvency by a cloud service provider), unless it was reasonable for the party to know of and protect against these risks (FRCP 37(e) advisory committee's note to 2015 amendment). However, neither the advisory committee nor the courts have comprehensively addressed a party's liability for ESI loss when the party both:

- Meets the legal criteria for control (see Tests for Control).
- Lacks effective control over how a nonparty stores or maintains its ESI (such as a party that entered into a form contract with a cloud service provides that limits the party's ability to influence the way the provider preserves its ESI).

See Practice Note, Requesting Parties: Initial Considerations (Federal) for more on identifying parties and nonparties with possession, custody, or control of relevant documents (including ESI).

Tests for Control

A court's test to determine whether a party controls relevant documents (including ESI) can impose significant hardship and obligations on parties who meet the criteria but lack effective control over how documents are stored or maintained. This is because the relationships between litigants and nonparties who possess potentially relevant documents are becoming more complex as technology evolves.

To determine whether a party controls documents or ESI that are outside of its possession and custody, federal courts apply either:

- The legal right standard (see Legal Right).
- The practical ability standard (see Practical Ability).

Some courts will apply both tests. The requesting party bears the burden of establishing control under either standard (see *Silver Sands Motel Inc. v. Long Island Cap. Mgmt.*, 2022 WL 767698, at *2 (E.D.N.Y. Mar. 14, 2022); *In re Pork Antitrust Litig.*, 2022 WL 972401, at *4 (D. Minn. Mar. 31, 2022)). Notably, where a party controls documents that are in a nonparty's physical possession, a court may direct the requesting party to subpoena the nonparty if doing so would be a more convenient or less burdensome way of obtaining the documents (compare, for example, *Lynn v. Monarch Recovery Mgmt., Inc.*, 285 F.R.D. 350, 361 (D. Md. 2012) (ordering a party to subpoena a nonparty under FRCP 26(b)(2)(C) where the adverse party did not have physical possession of the requested documents) with *Matthew Enter., Inc. v. Chrysler Grp. LLC*, 2015 WL 8482256, at *4 (N.D. Cal. Dec. 10, 2015) (denying a request to force the adverse party to serve a nonparty subpoena on a database vendor where the party could produce the same records more easily)).

Legal Right

Some courts follow the legal right standard. Under this standard, a party controls documents in a nonparty's possession if the party has the legal right to obtain them on demand (see *Jones v. United States*, 2022 WL 473032, at *4 (Fed. Cir. Feb. 16, 2022); *Sergeeva v. Tripleton Int'l Ltd.*, 834 F.3d 1194, 1201 (11th Cir. 2016); *In re Citric Acid Litig.*, 191 F.3d 1090, 1107 (9th Cir. 1999); *Chaveriat v. Williams Pipe Line Co.*, 11 F.3d 1420, 1426 (7th Cir. 1993)).

A party's legal right to access documents in a nonparty's possession may stem from:

- **Contractual relationships.** Courts have found that a legal right exists where contractual language states that a party either owns the requested information or may access that information when needed (see, for example, *Williams v. Angie's List, Inc.*, 2017 WL 1318419, at *3 (S.D. Ind. Apr. 10, 2017); *Lofton v. Verizon Wireless (Vaw) LLC*, 2014 WL 10965261, at *2 (N.D. Cal. Nov. 25, 2014); *Columbia Pictures Indus. v. Bunnell*, 2007 WL 2080419, at *6 (C.D. Cal. May 29, 2007) (requiring the party to preserve and produce server log data that was stored on servers maintained by a nonparty with which the party had a contractual relationship)).
- **Principal-agent relationships.** Courts have found that if a party has a principal-agent relationship with the nonparty that possesses the documents, that relationship is sufficient to establish that the party has control over the documents. However, a requesting party is not required to prove that a principal-agent relationship exists if it can make a showing that the responding party controls the nonparty parent, subsidiary, or affiliate. (See, for example, *Milke v. City of Phoenix*, 497 F. Supp. 3d 442, 465 (D. Ariz. 2020), aff'd, WL 259937 (9th Cir. Jan. 27, 2022); *McKesson Corp. v. Islamic Republic of Iran*, 185 F.R.D. 70, 77-78 (D.D.C. 1999).)

Notably, an employer may not have a legal right to emails in an employee's personal account, even if the emails were used for business purposes, except where an express contractual provision states otherwise (see, for example, *Matthew Enter.*, 2015 WL 8482256, at *3-4 (finding that an employee handbook instructing employees to keep corporate information in the "sole possession" of the employer was not sufficient to show control over personal emails)).

Practical Ability

Other courts follow the practical ability standard. Courts applying this standard focus on whether a party has a practical ability to obtain the requested documents, regardless of the party's legal entitlement or physical possession of them (see, for example, *Shcherbakovskiy v. Da Capo Al Fine, Ltd.*, 490 F.3d 130, 138 (2d Cir. 2007); *United States Sec. & Exch. Comm'n v. Collector's Coffee Inc.*, 2021 WL 391298, at *6 (S.D.N.Y. Feb. 4, 2021)). Under this broad standard, a party's access to documents typically is sufficient to establish control over those documents (see, for example, *SEC v. Strauss*, 2009 WL 3459204, at *8 (S.D.N.Y. Oct. 28, 2009)). Conversely, where a party does not have the ability to access the requested material, control will not be established (see, for example, *Laub v. Horbaczewski*, 2020 WL 7978227, at *4 (C.D. Cal. Nov. 17, 2020) (finding that defendant did not have possession, custody, or control over messages sent and received through Slack.com because they were inaccessible ESI and that obligating defendant to produce the messages would not be proportional to the needs of the case); but see *FTC v. Amer. Future Sys., Inc.*, 2023 WL 3559899, at *4 (E.D. Pa. Mar. 28, 2023) (rejecting *Laub* as unpersuasive and critiquing the ownership analysis for Slack data both generally and under Third Circuit precedent)).

These courts have found that control exists in:

- **Contractual relationships.** Courts have found that when a contract with a nonparty expressly provides a party with the right to obtain the requested documents and ESI, that party has control over it (see, for example, *Henderson v. United Student Aid Fund, Inc.*, 2015 WL 4742346, at *5-6 (S.D. Cal. July 28, 2015) (finding that a creditor controlled documents held by a collection agency when the collections contract recognized the creditor's ownership of certain documents that the collection agency possessed and used)).
- **Employer-employee relationships.** Courts have found that employers generally have sufficient access to information in a nonparty employee's possession to constitute control over the information (see, for example, *First Am. Bankcard, Inc. v. Smart Bus. Tech.*, Inc., 2017 WL 2267149, at *3 (E.D. La. May 24, 2017) (holding that a defunct corporate party had sufficient practical control over information in former owners' and officers' possession); *Selectica, Inc. v. Novatus, Inc.*, 2015 WL 1125051, at *5 (M.D. Fla. Mar. 12, 2015)).
- **Service provider relationships.** Courts have found that account holders have practical access and, therefore, control over documents in service providers' possession, such as telephone carriers and financial institutions (see, for example, *Lynn*, 285 F.R.D. at 361; *Fisher v. Fisher*, 2012 WL 2050785, at *6 (D. Md. June 5, 2012)).

- **Principal-agent relationships.** Courts have found that a party controls documents in the possession of nonparty affiliates and subsidiaries under the (sometimes mistaken) assumption that a party can informally request these documents from the affiliate (see, for example, *VeroBlue Farms USA, Inc. v. Wulf*, 2022 WL 2817612, at *10 (D. Kan. July 19, 2022) (directing principal to produce documents of its agent)).
- **Client and customer relationships.** Courts have found that a service provider's ability to access a client's server through the service provider's employees is sufficient to establish the service provider's control for preservation and production purposes (see, for example, *Hageman v. Accenture, LLP*, 2011 WL 8993423, at *4 (D. Minn. Oct. 19, 2011) (finding that an IT consulting company had control over its employees' emails stored on a nonparty customer's server, even when the company did not have access to the servers and the customer owned the information on the servers, because it had the practical ability to obtain the emails through its employees)).
- **Litigation or investigation relationships.** In one case, a court found that a party had the practical ability to access a database hosting a nonparty auditor's work papers because it issued an investigative subpoena. Given that access, the court found that the investigating party controlled the information. However, because the contract between the investigating agency, the SEC, and the nonparty auditor expressly forbade the SEC from granting access to other third parties, the court denied the motion to compel access to the database. (*Strauss*, 2009 WL 3459204, at *8; but see *In re Vitamin C Antitrust Litig.*, 2012 WL 5879140, at *3 (E.D.NY. Nov. 21, 2012) (finding that a corporate defendant did not have control over work papers of its outside auditor where it lacked the practical ability to obtain the materials).)

Analyzing Control in Common Circumstances

Courts frequently confront the issue of whether a party (or subpoenaed nonparty) has control over:

- **An affiliated organization's documents.** Generally, parent corporations have sufficient control over a wholly-owned subsidiary that it must produce the subsidiary's responsive, discoverable information (*Dietrich v. Bauer*, 2000 WL 1171132, at *3 (S.D.N.Y. Aug. 16, 2000)). However, a subsidiary's control over a parent company's documents is less clear. For example, courts have found that a subsidiary has control over documents in its parent's possession where the subsidiary:
  - was an alter ego of the parent;
  - was an agent of the parent in the relevant transaction resulting in litigation;
  - had a relationship such that they could secure documents to meet its business needs and documents helpful in business;
  - had access to documents when the need arose in the ordinary course of business; and
  - served as a marketer and servicer of the parent's product in the US.

  (*U.S. Int'l. Trade Comm. v. ASAT, Inc.*, 411 F.3d 245, 254 (D.C. Cir. 2005).)
- **Their current counsel's documents.** Several courts have held that clients control their lawyers' documents and must produce or log them in a privilege log (see, for example, *Estate of Manship v. United States*, 232 F.R.D. 552, 561 (M.D. La. 2005) (explaining that the federal rules require parties to log relevant and responsive documents contained in an attorney's legal files)). However, very few litigants comply with this obligation in practice.

Stored Communications Act Warrants and Foreign-Stored ESI

Cloud-based ESI typically exists in more than one physical location, which can subject an organization to multiple preservation schemes and production obligations and challenges. Email providers and social media companies rely on the cloud to serve their global user base, as many users may not be sufficiently close to a server.

Courts in both the Second and Ninth Circuits addressed whether email service providers (such as Microsoft and Google) and social media companies (such as Facebook and Twitter) have control over account holders' email and other messages stored on their servers, even if those servers:

- Reside in jurisdictions that are not subject to US law.
- Are bound by significant limitations on data transfers.

These cases involved Stored Communications Act (SCA) warrants for ESI that nonparties possessed and stored overseas. The courts reached inconsistent conclusions, with:

- The Second Circuit:
  - distinguishing between subpoenas (which contemplate the production of materials located abroad) and warrants (which traditionally involve domestic limits and Fourth Amendment privacy implications); and

  - holding that the SCA does not authorize courts to issue and enforce warrants to seize email content stored exclusively on foreign servers.

  (*In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197, at 215-16 (2nd Cir. 2016); see Legal Update, SCA Warrant Cannot Compel Microsoft to Produce Customer Emails Stored Outside the US: Second Circuit).

- The US District Court for the District of Arizona:
  - holding that social media companies controlled user messages on their websites, regardless of the location; and
  - denying defendants' effort to suppress messages that the prosecution obtained by serving an SCA warrant on Facebook and Twitter and which defendants claimed were located overseas.

  (*United States v. Martin*, 2015 WL 4463934, at *4 (D. Ariz. July 21, 2015).)

- The US District Court for the Eastern District of Pennsylvania:
  - accepting the Second Circuit's two-part *Microsoft* test and deferring to some of its findings;
  - finding that Google's production of foreign-stored ESI would not violate the Fourth Amendment, because the related search (or privacy infringement) would occur in the US when Google produced the document to the government, rather than when Google transferred the ESI overseas to the US; and
  - holding that Google was required to produce ESI that it stored overseas in response to an SCA warrant.

  (*In re Search Warrant No. 16–960–M–01 to Google*, 232 F.Supp.3d 708 (E.D. Pa. 2017).)

In October 2017, the US Supreme Court of Appeals granted certiorari for the Second Circuit's *Microsoft* decision and was poised to resolve whether SCA warrants could compel the production of foreign-stored ESI. However, before the Supreme Court ruled on the case, Congress passed the Clarifying Lawful Overseas Use of Data ("CLOUD") Act and rendered the case moot. The CLOUD Act, which took effect in March 2018, amended the SCA to clarify that warrants issued under the SCA apply equally to domestic- and foreign-stored ESI. (*U.S. v. Microsoft Corp.*, 138 S.Ct. 1186 (2018); 18 U.S.C. § 2713.)

However, the SCA does not allow defendants in a criminal case to subpoena email service providers and social media. Only the government, not private parties, may request disclosure pursuant to the SCA. (*United States v. Maxwell*, 2022 WL 576306, at *10 (S.D.N.Y. Feb. 25, 2022); *Facebook, Inc. v. Wint*, 199 A.3d 625, 629 (D.C. 2019) (collecting cases).)