Forthcoming in Volume 30, Issue 2 of the* Journal of Technology Law & Policy*, University of Florida Levin College of Law. This excerpt is subject to revision and editorial changes prior to final publication.

WHO HAS "POSSESSION, CUSTODY, OR CONTROL" OF THE EMPLOYEE'S PERSONAL MOBILE DEVICE? TIME FOR AMENDMENTS TO THE FEDERAL RULES

Judge Xavier Rodriguez[*]

Abstract

As mobile devices have become indispensable tools for professional communication, the distinction between personal and business data has blurred—creating critical challenges for litigators and organizations navigating discovery obligations. This Article explores the evolving jurisprudence surrounding whether and when a corporate defendant has "possession, custody, or control" over data stored on an employee's personal mobile device. Drawing from a recorded podcast conversation[1] between the authors and expanding on the legal foundations, we scrutinize the two primary frameworks courts use to analyze control—the "legal right" test and the "practical ability" test—and question their fitness in the context of modern mobile usage patterns.

This Article evaluates competing conceptions of "control" against three core criteria: (1) doctrinal coherence with the text and structure of the Federal Rules, (2) ex ante predictability for litigants and courts, and (3) the ability to reduce socially costly errors—particularly spoliation risk and unnecessary invasions of employee privacy. A test is "adequate," in this sense, if it supplies administrable guidance ex ante, produces reasonably consistent outcomes across jurisdictions, and does not systematically externalize preservation burdens onto individual employees or shield parties who exploit technical arrangements to avoid discovery. Given this measurement, both the legal right and practical ability tests are inadequate: the former is underinclusive and encourages evasion, while the latter is overinclusive, unevenly applied, and insensitive to privacy and power imbalances.

This Article also considers the growing disconnect between technological reality and static discovery rules, emphasizing the need for

---

* Judge Rodriguez extends his thanks to Christian Krueger, a third-year law student at the University of Texas School of Law for his invaluable research, proofing and cite checking assistance. My thanks also to Kelly Twigger for prompting the idea of writing on this topic and providing me access to Minerva for research purposes.

1. To hear a discussion with the author on this topic, see SPOTIFY: *Meet and Confer with Kelly Twigger*, *Mobile Minutes: Judge Xavier Rodriguez on Possession, Custody, or Control* (July 24, 2025).

clarity in preservation and production expectations. Finally, we address the implications of emerging state statutory and case law developments regarding privacy, the General Data Protection Act,[2] and the Hague Evidence Convention[3]—where an employer's limited control over personal devices may be further complicated by these privacy laws and jurisdictional boundaries. In response, we propose a more functional approach to assessing control and offer practical recommendations for litigators, courts, and policymakers to modernize discovery frameworks in a Bring Your Own Device (BYOD) world.

This Article proposes an agency-anchored conception of "control" as one promising candidate for a more uniform national standard. Under this approach, a rebuttable presumption of control would attach to electronically stored information (ESI) on the personal devices of officers, directors, and individuals with meaningful managerial authority acting within the scope of their agency, while other employees' devices would ordinarily be treated as outside the responding party's control and only reachable, if at all, through Rule 45.

2. Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1.

3. Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 847 U.N.T.S. 231.

I. INTRODUCTION

A. *Mobile Devices Meet 1938 Rules*

Few developments in modern civil litigation have unsettled the discovery obligations imposed by the Federal Rules of Civil Procedure more than the explosion of personal mobile devices. Where smartphones are ubiquitous, always on, and deeply entwined with both personal and professional life, courts increasingly face the question: when must a corporate defendant collect and produce information stored on employees' personally owned devices? The issue implicates a central phrase in the Federal Rules of Civil Procedure—"possession, custody, or control"—that has guided document production obligations since the Rules' inception in 1938.

This question is far from academic. In contemporary workplaces, employees routinely use personal phones to send emails, exchange text messages, access corporate databases, and communicate via messaging platforms. Many corporations encourage or even mandate this integration through BYOD policies. Others tolerate the practice informally. In either event, the blending of personal and professional data on personal mobile devices complicates discovery obligations, and raises profound questions about privacy, proportionality, employee morale, and the extent of corporate responsibility for evidence spoliation.

Federal Rule of Civil Procedure 34(a)(1) provides that a party may request certain items in the responding party's possession, custody, or control.[4] The phrase seems straightforward. But applied to personal

4. FED. R. CIV. P. 34(a) states:

(a) In General. A party may serve on any other party a request within the scope

devices, it quickly becomes elusive. Does "control" mean a corporation must collect text messages from employees' personal phones? Or does it mean the employer has no obligation unless it can legally compel access? Or does it occupy some middle ground, such as when the employer has the "practical ability" to obtain the information?

B. *Stakes for Litigants*

The question of whether an employer has control over ESI on an employee's personal mobile device has become common, especially in the wake of the BYOD movement,[5] thus deserving careful attention.

When the duty to preserve in a case is triggered, litigants must take measures to preserve relevant material or potentially face later sanctions. Does a company take measures to preserve mobile devices owned by an employee? What form should those preservation measures take? How are they enforceable? Should employers discipline employees who refuse to cooperate? How do requesting parties know whether the corporation will assist in the discovery process or later argue that they do not possess or control any data that may be resident in an employee mobile device? If these conversations will not take place until the meet and confer sessions, will relevant and unique data be lost? If the parties agree to certain ESI protocols that contemplate corporation control over employee devices, can a corporation be later sanctioned when employees refuse to cooperate? At what point in these discussions should a requesting party issue Rule 45 subpoenas to individuals? At what point do courts become involved in this issue—before the issuance of any requests for production (RFP)? Does court involvement take place after a response to the RFPs and objections have been filed asserting no control over employee devices? If Rule 45 subpoenas are issued to individual employees, does

---

> of Rule 26(b):
>
> (1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:
>
> (A) any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form . . . .

5. *See generally* Garry G. Mathiason & Michael J. McGuire, *The 'Bring Your Own Device' to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*, THE LITTLER REP. (2012), https://www.littler.com/sites/default/files/press/pdf/WP_12EE_BringYourOwnDevice_7-23-13.pdf [https://perma.cc/NZE3-G8WU] (discussing BYOD issues).

the corporation retain counsel for these employees to navigate the process of responding or objecting?

Courts are split, and litigants face uncertainty. In some jurisdictions, requesting parties (usually plaintiffs) can compel corporations to collect and produce employee text messages, especially when corporate policies suggest some measure of control.[6] In other jurisdictions, courts shield employers, leaving plaintiffs to pursue non-party subpoenas under Rule 45.[7] The difference is consequential. Rule 34 production requests impose obligations directly on the corporate defendant, whereas Rule 45 subpoenas[8] place the burden on employees themselves to respond, object, or resist production.[9] In addition, while the issue of possession, custody, or control is disputed, the passage of time may cause relevant data on mobile devices to be lost through failures to disable automatic deletion settings in text settings, the overwriting of data, physical damage to the device, or replacement of the device.

For requesting parties (usually plaintiffs), access to data in an employee's mobile device may be critical to proving claims. In

---

6. O'Bryan v. U.S. Bank Nat'l Ass'n, No. 3:20-CV-00153, 2022 WL 22736591, at *4 (M.D. Tenn. Mar. 10, 2022) (finding that the Bank's Employee Mobility Program purports to give U.S. Bank ownership of specific information on its employees' personal devices under certain circumstances, but that it was unclear whether those circumstances existed).

7. Control "for purposes of Rule 34 means demonstrating that the party served with the document request 'has the legal right to obtain the documents on demand' from someone else. This is understood to include 'the legal right to command release from the party with actual possession.'" Halabu Holdings, LLC v. Old Nat'l Bancorp, No. 20-10427, 2020 WL 12676263, at *3 (E.D. Mich. June 9, 2020) (internal citations omitted).

8. FED. R. CIV. P. 45(a)(1)(C) provides:

> A command to produce documents, electronically stored information, or tangible things or to permit the inspection of premises may be included in a subpoena commanding attendance at a deposition, hearing, or trial, or may be set out in a separate subpoena. A subpoena may specify the form or forms in which electronically stored information is to be produced.

9. FED. R. CIV. P. 45(d)(2)(B) states:

> A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served . . .

employment discrimination suits,[10] wage-and-hour cases,[11] antitrust conspiracies,[12] and trade secret disputes,[13] text messages or encrypted chats may contain decisive evidence. From the perspective of plaintiffs and other requesting parties, personal devices may be the only realistic source of evidence of harassment, off-the-clock work, or informal communications that never pass through corporate systems. A standard that presumptively insulates most personal devices from Rule 34 may therefore raise serious access-to-justice concerns in employment, wage-and-hour, and civil rights litigation. For corporate defendants, insisting on identifying, reviewing, and potentially producing data from individual employees' mobile devices raises burdens and risks: alienating employees, potentially invading personal privacy, and creating opportunities for spoliation if employees refuse cooperation.

It is unclear what constitutes possession, custody, or control. Though the phrase "possession, custody, or control" is used in Rules 26, 34, and 45, the Federal Rules do not define the phrase.[14] Consequently, courts have had to reason with the words' meaning. For the most part, physical possession and actual custody are straightforwardly determined.[15] Much of the real debate focuses on "control," specifically, with different courts adopting different standards.[16] Courts have broadly coalesced around three tests, respectively: legal right, practical ability, and legal right plus notification.[17] On top of there being multiple tests, there is also variation

10. Shim-Larkin v. City of N.Y, No. 1:16-CV-6099-AJN-KNF, 2019 WL 5198792, at *1 (S.D.N.Y. Sep. 16, 2019) (sanctioning defendant for loss of text messages stored on the personal cellular telephone of the defendant's assistant lifeguard coordinator).

11. Small v. Univ. Med. Ctr., No. 2:13-CV-0298-APG-PAL, 2018 WL 3795238, at *71 (D. Nev. Aug. 9, 2018) (sanctions assessed against employer).

12. *In re* Pork Antitrust Litig., No. 18-CV-1776 (JRT/HB), 2022 WL 972401, at *15 (D. Minn. Mar. 31, 2022).

13. Allergan, Inc. v. Revance Therapeutics, Inc., No. 3:23-CV-00431, 2025 WL 2182324, at *1 (M.D. Tenn. June 20, 2025).

14. *See* FED. R. CIV. P. 26(a)(1)(A)(ii) ("a copy—or a description by category and location—of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses"); FED. R. CIV. P. 34(a)(1) ("to produce and permit the requesting party or its representative to inspect, copy, test, or sample . . . items in the responding party's possession, custody, or control"); FED. R. CIV. P. 45(a)(1)(A)(iii) ("produce designated documents, electronically stored information, or tangible things in that person's possession, custody, or control").

15. The Sedona Conference, *Commentary on Rule 34 and Rule 45 'Possession, Custody, or Control'*, 25 SEDONA CONF. J. 1, 14 (2024) [hereinafter *Rules 34 and 45 Commentary*].

16. *See id.* at 17–34 (outlining the different tests and which courts use each of them).

17. *See id.* at 18 (explaining the legal right test as "the legal right to obtain the Documents and ESI," the practical ability test as "the 'practical ability'" to "obtain the Documents and ESI" without a legal right to do so, and the legal right plus notification test as "the legal right to obtain the Documents and ESI" plus the duty to "notify . . . [the] adversary" if "the party does not have the legal right to obtain the Documents and ESI").

in application of each test, resulting in a still messier amalgamation.[18] The consequent inconsistency causes uncertainty among litigants on an important matter. Pursuant to the Federal Rules, a party is obligated to preserve relevant ESI under penalty of sanction.[19] In addition to raising spoliation concerns, irregularity in the standard for "control" over devices may cause lengthy discovery disputes that delay expeditious lawsuit resolution. Finally, inter-jurisdictional discrepancies contravene the Federal Rules' interest in uniformity.[20]

There is a need for greater predictability regarding employers' control of employees' personal mobile devices, but none of the established tests are without fault. While The Sedona Conference has advocated for the universal adoption of the legal right test,[21] this approach is underinclusive, potentially leading to spoliation, evasion, and omission. The practical ability test has its own shortcomings, most notably in implementation (what if an employee simply says, "No"?). A test based on principles of agency law would be superior. Under it, a requesting party would be able to gather data from the responding party's officers, directors, supervisors and managers. In other words, ESI on the personal mobile devices of high-level agents would be presumed to be under the company's control, whether by right or ability. Agents authorized to act on behalf of the company should have to produce relevant information. To avoid overbreadth, all other employees would have to be individually subpoenaed by the requesting party under Rule 45. Such an approach to a uniform national standard merits further consideration.

18. *See id.* at 28, 34 ("To further complicate matters, even within these general categories there are differences in the ways in which federal courts within the circuits define and apply the standards," leaving "parties and courts with conflicting guidance to consider when making defensible discovery decisions.").

19. FED. R. CIV. P. 37(e).

20. Rhys Dipshan, *Diverging 'Possession, Custody, or Control' Tests Impact E-Discovery Outcomes. But is a Uniform Standard Feasible?*, LEGALTECH NEWS (May 5, 2023), https://monitor.lawnext.com/article/diverging--possession--custody-or-control--tests-impact-e-discovery-outcomes.-but-is-a-uniform-standard-feasible- [https://perma.cc/96SJ-9F5W].

21. *Rules 34 and 45 Commentary*, *supra* note 15, at 63–64.