The Sedona Conference Journal

Volume 20 2019

The Burden of Privacy in Discovery

Robert D. Keeling & Ray Mangum

Recommended Citation:

Robert D. Keeling & Ray Mangum, *The Burden of Privacy in Discovery*, 20 SEDONA CONF. J. 415 (2019).

THE BURDEN OF PRIVACY IN DISCOVERY*

*Robert D. Keeling & Ray Mangum***

Traditionally, the scope of discovery under Rule 26 of the Federal Rules of Civil Procedure and its state law analogues was defined exclusively in terms of relevance, with privilege providing but a narrow exception. Private matters by default were discoverable, even where the privacy interests were significant and the relevance only marginal. To obtain relief, a producing party was required to seek a protective order under Rule 26(c) and establish good cause. Beginning with the 1983 amendments, however, the scope of discovery under Rule 26(b) has been limited by a growing list of proportionality factors, which weigh both monetary and nonpecuniary burdens imposed upon the

---

* This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The views and opinions expressed in this article are those of the authors only and do not reflect in any way the views and opinions of any law firm, company, agency, or other entity to which the authors are affiliated.

** Robert Keeling is a partner at Sidley Austin LLP, an experienced litigator whose practice includes a special focus on electronic discovery matters, and co-chair of the firm's eDiscovery Task Force. He represents both plaintiffs and defendants in civil litigation throughout the nation and conducts internal investigations in the United States and throughout the world. Ray Mangum is an associate at Sidley Austin LLP who represents clients in a variety of government investigations and commercial disputes, with a particular focus on matters involving complex data analytics and eDiscovery issues. Special thanks to Michael Buschbacher for his careful research and thoughtful edits. Thanks also to Christopher Joyce and Kristen Bartolotta for their valuable assistance.

producing party against the likely value of the otherwise discoverable material. Although these proportionality factors began as an integral part of the definition of the scope of discovery, for more than two decades these limitations resided in a separate subsection of the Rule, resulting in considerable confusion and less-than-rigorous enforcement. The 2015 amendments to Rule 26(b)(1), however, were meant to resolve any doubt, returning the proportionality factors to their original place as part of the very definition of what is discoverable. To be within the scope of discovery, an inquiry now must be both relevant as well as proportional.

This emphasis on proportionality in discovery arrives at a time when the protection of privacy is of increasing concern in the United States and abroad. Recent advances in technology—smart phones and social media in particular—have allowed businesses to collect, store, and find ways to monetize far more personal data than ever before. With the rise of Big Data, however, there has been a growing and well-founded concern that personal information might be used unethically or exposed improperly. Protection of personal privacy has consequently become an important goal both in technological development—e.g., the increasing prevalence of "privacy by design" in communications programs such as "ephemeral" messaging systems—and in governmental regulation. To pick just two recent examples of the latter, the European Union's General Data Protection Regulation[1] (GDPR) and the California Consumer

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119/1) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents.

Privacy Act[2] (CCPA) both impose sweeping requirements on businesses with the aim of increasing consumers' privacy and control over how their personal data is used.

The renewed prominence of the Rule 26(b) proportionality factors as part of the definition of the scope of discovery has provided a solid textual basis for giving weight to such privacy "burdens" in defining the scope of discovery. As a result, an emerging consensus of courts and commentators has concluded that privacy may—indeed, should—be considered as part of the proportionality analysis required under Rule 26(b)(1). As we aim to explain in this article, that conclusion is well founded not only in the text of Rule 26, but also in its historic underpinnings, which provide important context for more recent developments and continue to inform how judges and advocates should consider privacy concerns in discovery.

HISTORY OF PROPORTIONALITY AND THE SCOPE OF CIVIL DISCOVERY

The principle of proportionality in civil discovery is hardly new.[3] The Federal Rules of Civil Procedure have begun—since their inception—with a guiding command for courts to seek "to secure the just, speedy, and inexpensive determination of every action and proceeding."[4] In keeping with that aim, the scope of

2. CAL. CIV. CODE § 1798.100.

3. *See, e.g.,* Welty v. Clute, 1 F.R.D. 446, 446–47 (W.D.N.Y. 1940) (finding that it was unnecessary to grant a second deposition of plaintiff in addition to granting discovery); Waldron v. Cities Serv. Co., 361 F. 2d 671, 673 (2d Cir. 1966) (stating that a plaintiff "may not seek indefinitely . . . to use the [discovery] process to find evidence"); *see also* Daniel J. Solove & Woodrow Harzog, *The Ultimate Unifying Approach to Complying with all Laws and Regulations*, 19 GREEN BAG 2D 223 (2016) ("Be reasonable.").

4. ADVISORY COMMITTEE ON RULES FOR CIVIL PROCEDURE, REPORT OF THE ADVISORY COMMITTEE ON RULES FOR CIVIL PROCEDURE CONTAINING

discovery has always been cabined. The original Rule 26, which applied to depositions only, limited the "Scope of Examination" to matters "not privileged" and "relevant to the subject matter involved in the pending action."[5] Even prior to the adoption of the Federal Rules in 1938, courts applied principles of proportionality to the cases in their dockets.[6]

Yet an express proportionality limitation on the scope of discovery did not appear in the Federal Rules until 1983, when Rule 26(b)(1) was further amended.[7] The revised Rule required courts to consider a variety of proportionality factors, including whether "the discovery sought [was] unreasonably cumulative or duplicative" and whether "the discovery [was] unduly burdensome or expensive" in light not only of "the amount in controversy" but also of less-tangible and even nonpecuniary considerations such as "the needs of the case," the "limitations on the parties' resources," and "the importance of the issues at stake in the litigation."[8]

The revised Rule "recogni[zed] that the right of pretrial disclosure is subject to some limitation beyond relevance."[9] Yet it

---

PROPOSED RULES OF CIVIL PROCEDURE FOR THE DISTRICT COURTS OF THE UNITED STATES (1937).

5. *Id.* at 66 (Rule 26(b)).

6. *See* Hon. Elizabeth D. Laporte & Jonathan M. Redgrave, *A Practical Guide to Achieving Proportionality Under New Federal Rule of Civil Procedure 26*, 9 FED. CTS. L. REV. (ISSUE 2) 19, 24–25 (2015) ("Indeed, the concept of proportionality existed in practice long before being officially embodied in the Federal Rules.").

7. FED. R. CIV. P. 26(b)(1) (1983).

8. *Id.*

9. Edward D. Cavanagh, *The August 1, 1983 Amendments to the Federal Rules of Civil Procedure: A Critical Evaluation and a Proposal for More Effective Discovery through Local Rules*, 30 VILLANOVA L. REV. 767, 786 (1985); see also Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 HARV. L. REV. 427, 459 (1991) ("A basic shift in discovery

was aimed most squarely at curbing the types of duplicative, excessive, "scorched earth" discovery practices prevalent at the time—i.e., at the problem of so-called "overdiscovery."[10] As the advisory committee's note to the 1983 amendment explained, the amended Rule sought to "prevent use of discovery to wage a war of attrition or as a device to coerce a party, whether financially weak or affluent."[11] In other words, the 1983 amendment was seen as limiting the depth rather than the breadth of discovery.[12]

Ten years later, in 1993, the scope of discovery was further refined when Rule 26(b) was again amended, this time in recognition that "[t]he information explosion of recent decades ha[d] greatly increased both the potential cost of wide-ranging discovery and the potential for discovery to be used as an instrument for delay or oppression."[13] Two additional proportionality factors were added: the first asked whether "the burden or expense of the proposed discovery outweighs its likely benefit," and the second considered "the importance of the proposed

---

philosophy was evidenced by the [1983] elimination of the sentence in Rule 26(a) stating that 'the frequency of use of [the discovery] methods is not limited.'").

10. *See, e.g.*, Am. Bar Ass'n Section of Litig., Comments on Revised Proposed Amendments to the Federal Rules of Civil Procedure 6–11 (1979) (unpublished) (discussing the reasoning for the proposed amendments to Rule 26, and noting that ample evidence existed to support the idea that "overuse" of discovery was a real problem).

11. FED. R. CIV. P. 26(b) advisory committee note to 1983 amendment.

12. *See* Cavanagh, *supra* note 9, at 786–87 n.93 (citing FED. R. CIV. P. 26(b)(1); AM. BAR ASS'N SECTION OF LITIG., REPORT OF THE SPECIAL COMMITTEE FOR THE STUDY OF DISCOVERY ABUSE *in* 92 F.R.D. 149 (1977); Maurice Rosenberg & Warren R. King, *Curbing Discovery Abuse in Civil Litigation: Enough is Enough,* 1981 B.Y.U. L. REV. 579 (1981); Hon. Mary M. Schroeder & John P. Frank, *The Proposed Changes in the Discovery Rules,* 1978 ARIZ. ST. L.J. 475 (1978).

13. FED. R. CIV. P. 26(b) advisory committee note to 1993 amendment.

discovery in resolving the issues."[14] These changes were intended to "enable courts to keep a tighter rein on the extent of discovery."[15] Unfortunately—out of a desire to avoid a larger renumbering of Rule 26(b) that would have resulted from other revisions—Rule 26(b)(1) was split into two subparagraphs, severing the proportionality limitations from the core definition of the scope of discovery.[16] As the 2015 advisory committee note observed, while not intended, this structural change to Rule 26 "could [have been] read to separate the proportionality provisions as 'limitations,' no longer an integral part of the (b)(1) scope provisions."[17] Indeed, in the years following the 1993 amendments, "[t]he Committee [was] told repeatedly that courts ha[d] not implemented these [proportionality] limitations with the vigor that was contemplated." In a minor effort to combat that trend, Rule 26(b)(1) was amended yet again in 2000 to add an "otherwise redundant cross-reference" to the proportionality factors then residing in Rule 26(b)(2).[18]

Most recently, in 2015, the scope of discovery under Rule 26(b) was amended to "restore[] the proportionality factors to their original place in defining the scope of discovery."[19] No longer are the proportionality considerations described as separate "limitations" on an inquiry governed solely by relevance.[20] Under the revised Rule 26(b)(1), proportionality once again stands on equal footing alongside relevance in defining the

14. FED. R. CIV. P. 26(b) advisory committee note to 2015 amendment.
15. FED. R. CIV. P. 26(b) advisory committee note to 1993 amendment.
16. *See* FED. R. CIV. P. 26(b) advisory committee note to 2015 amendment.
17. *Id.*
18. FED. R. CIV. P. 26(b) advisory committee note to 2000 amendment.
19. FED. R. CIV. P. 26(b) advisory committee note to 2015 amendment.
20. *Id.*

scope of discovery.[21] If it is not both relevant as well as proportional, it is not discoverable. At the same time, an additional proportionality factor was added— "the parties' relative access to relevant information"—and the growing list of proportionality factors was re-ordered to begin with the more-specific factors and to conclude with a general proportionality limitation whenever "the burden or expense of the proposed discovery outweighs its likely benefit."[22] While these changes did not add much new in substance, the increase in clarity and the emphasis on proportionality augured a significant practical effect on how discovery is actually conducted. As Chief Justice John Roberts put in his *2015 Year-End Report on the Federal Judiciary*, these changes "crystalize[d] the concept of reasonable limits on discovery through increased reliance on the common-sense concept of proportionality."[23]

PRIVACY IS A "BURDEN" UNDER RULE 26(b)(1)

"The Federal Rules of Civil Procedure were designed to effect a revolution in litigation by broadening the availability of discovery."[24] While this broadening arguably served the interests of justice in many cases,[25] it also created a system that could

21. FED. R. CIV. P. 26(b)(1).

22. *Id.*

23. CHIEF JUSTICE JOHN G. ROBERTS, JR., 2015 YEAR-END REPORT ON THE FEDERAL JUDICIARY, U.S. SUP. CT. (Dec. 31, 2015), https://www.supremecourt.gov/publicinfo/year-end/2015year-endreport.pdf.

24. Richard L. Marcus, *Myth and Reality in Protective Order Litigation*, 69 CORNELL L. REV. 1, 6 (1983).

25. *See, e.g.*, Hickman v. Taylor, 329 U.S. 495, 507 (1947) ("No longer can the time-honored cry of 'fishing expedition' serve to preclude a party from inquiring into the facts underlying his opponent's case.").

be burdensome and susceptible to abuse.[26] As Justice Lewis Powell observed when writing on behalf of a unanimous Court in *Seattle Times Co. v. Rhinehart*, abuse of discovery "is not limited to matters of delay and expense; discovery also may seriously implicate privacy interests of litigants and third parties."[27] Yet, prior to the 1983 amendments, Rule 26(b)(1) provided no avenue for relief from the production of private information, even if only of marginal relevance.[28] Thus, when Justice Powell looked to the text of the discovery rules at issue in *Seattle Times*,[29] he found that:

> [t]he Rules do not differentiate between information that is private or intimate and that to which no privacy interests attach. Under the Rules, the only express limitations are that the information sought is not privileged, and is relevant to the subject matter of the pending action. Thus, the Rules often allow extensive intrusion into the affairs of both litigants and third parties.[30]

---

26. *See, e.g.*, Marcus, *supra* note 24, at 6; Herbert v. Lando, 441 U.S. 153, 177 (1979) (Powell, J., concurring) (Experience has shown that the Rules have "not infrequently [been] exploited to the disadvantage of justice.").

27. 467 U.S. 20, 34–35 (1984).

28. FED. R. CIV. P. 26(b) advisory committee note to 1983 amendment (stating that the changes to Rule 26(b)(1) were "designed to . . . limit the use of the various discovery devices").

29. *Seattle Times* involved a First Amendment challenge to a protective order issued by a state court pursuant to Washington Superior Court Civil Rule 26(c). 467 U.S. at 34. As noted in the opinion, however, the Washington rules were modeled after the Federal Rules, *id.* at 29–30, and Washington Superior Court Civil Rule 26(b)(1) in particular was identical to Federal Rule of Civil Procedure 26(b)(1) in effect at the time, *id.* at 30 n.15.

30. *Id.* at 30.

A protective order under Rule 26(c) provided the only tool for courts— upon motion and good cause shown—to "protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense," including by ordering "that certain matters not be inquired into."[31] Showing good cause was (and is) often difficult in contested matters.[32] And even with the rise of stipulated protective orders, invasive discovery remained the norm, and protection of personal privacy the exception.[33] Thus, as prominent trial lawyer (and former federal judge) Simon Rifkind remarked in 1976, "a foreigner watching the discovery proceedings in a civil suit would never suspect that this country has a highly-prized tradition of privacy enshrined in the fourth amendment."[34]

It is therefore somewhat surprising to look back at the pre-2015 history of the amendments to the scope of civil discovery under Rule 26(b) and find little mention of privacy interests in the discussion.[35] Rather, early discussion of the proportionality factors focused primarily on economic factors.[36] A notable (though partial) exception to this lack of discussion arose from cases where a party sought direct access to an opposing party's

---

31. FED. R. CIV. P. 26(c) (1970).

32. *See, e.g.*, Marcus, *supra* note 24, at 23–26.

33. FED. R. CIV. P. 26 advisory committee note to 1983 amendment (noting existing practice of issuing protective orders, but concluding that "[o]n the whole, however, district judges have been reluctant to limit the use of the discovery devices").

34. Hon. Simon H. Rifkind, Are We Asking Too Much of Our Courts?, Address at the National Conference on the Causes of Popular Dissatisfaction with the Administration of Justice (1976) *in* 70 F.R.D. 96, 107.

35. *See* Babette Boliek, *Prioritizing Privacy in the Courts and Beyond*, 103 CORNELL L. REV. 1101, 1128–29 (2018).

36. *See* FED. R. CIV. P. 26(b) advisory committee note to 1983 amendment; *see also* Boliek, *supra* note 35, at 1129 ("[t]he word 'privacy' was curiously absent from this new list of factors").

computer systems under Rule 34(a)(1), which allows parties "to inspect, copy, test or sample . . . any designated tangible things."[37] Computers are tangible things, after all, and many litigants over the years have sought to test, sample, or obtain copies of an opposing party's computer or entire computer system. Such requests are disfavored, however, not only because of the cost and inconvenience, but also because of the threat to privacy.[38] As the advisory committee notes explain, "issues of burden and intrusiveness" raised by Rule 34(a)(1) include "confidentiality [and] privacy."[39] Notably, the advisory committee concluded that such issues "can be addressed under [either the proportionality factors formerly codified in] Rule 26(b)(2) [or] [under the protective order procedures set forth in Rule] 26(c)."[40] An important assumption in this directive was the advisory committee's intent that the burden of privacy should be considered in setting the scope of discovery.

---

37. FED. R. CIV. P. 34(a)(1).

38. *See, e.g.*, S.E.C. v. Strauss, No. 09 Civ. 4150, 2009 WL 3459204, at *12 n.8 (S.D.N.Y. Oct. 28, 2009) ("There is a general reluctance to allow a party to access its adversary's *own* database directly."); NOLA Spice Designs, LLC v. Haydel Enterprises, Inc., No. CIV.A. 12-2515, 2013 WL 3974535, at *2 (E.D. La. Aug. 2, 2013).

39. FED. R. CIV. P. 34(a)(1) advisory committee note to 2006 amendment; see also The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Production*, 19 SEDONA CONF. J. 1, 128–29 (2018) [hereinafter The Sedona Principles, Third Edition] ("Direct access to an opposing party's computer systems under a Rule 34 inspection also presents possible concerns such as: . . . revealing . . . highly confidential or private information, such as personnel evaluations and payroll information, properly private to individual employees; . . . revealing confidential attorney-client or work-product communications; . . . [and] placing a responding party's computing systems at risk of a data security breach.").

40. FED. R. CIV. P. 34(a)(1) advisory committee note to 2006 amendment.

However, while many cases discussing direct access requests have cited privacy concerns, few have done so within the framework of a Rule 26(b) proportionality analysis.[41] It is not that these cases have rejected this proportionality framework, but rather that they have simply ignored it. For example, in *John B. v. Goetz*, the Sixth Circuit granted mandamus relief to two state defendants who had been ordered by the district court to provide forensic imaging of their computers, noting that "[t]he district court's compelled forensic imaging orders here fail[ed] to account properly for the significant privacy and confidentiality concerns present in this case."[42] Despite putting great weight on the privacy implications in its decision to grant relief, that opinion did not cite Rule 26(b).

In this context and others, it remained common to think of privacy as a separate consideration—distinct from proportionality—even among thoughtful and forward-looking commentators. For example, when *The Sedona Principles, Second Edition* were published in June 2007, Principle 10 stated that "[a] responding party should follow reasonable procedures to protect privileges and objections in connection with the production of electronically stored information"[43] and Comment 10.e addressed "[p]rivacy, trade secret, and other confidentiality concerns."[44] The Comment recognized that "[e]lectronic

41. The only pre-2015 case we have found that analyzed a direct-access request using the proportionality framework of Rule 26(b) is *NOLA Spice Designs*, 2013 WL 3974535, at *2.

42. 531 F.3d 448, 460 (6th Cir. 2008); *see also* White v. Graceland Coll. Ctr. for Prof'l Dev. & Lifelong Learning, Inc., No. CIV.A. 07-2319-CM, 2009 WL 722056, at *7 (D. Kan. Mar. 18, 2009).

43. The Sedona Conference, *The Sedona Principles, Second Edition: Best Practices, Recommendations, & Principles for Addressing Electronic Production*, p. 51 (June 2007), *available at* https://thesedonaconference.org/publication/The_Sedona_Principles.

44. *Id.* at 56, cmt. 10.e.

information systems contain significant amounts of information that may be subject to trade secret, confidentiality, or privacy considerations," including a wide variety of proprietary business information as well as "customer and employee personal data (e.g., social security and credit card numbers, employee and patient health data, and customer financial records)."[45] Moreover, the Comment appropriately warned that "[p]rivacy rights related to personal data may extend to customers, employees, and non-parties." Yet it did not mention any of the proportionality factors as potentially imposing a limit on the discovery of private information. Rather, it concluded that "the identification and protection of privacy rights are not directly addressed in the [then-recent] 2006 amendments" and reassured parties that "ample protection for such information during discovery is available through a Rule 26(c) protective order or by party agreement."

Even today, it remains common, among both the bench and the bar, to think of proportionality in discovery as relating primarily to financial burdens.[46] With the re-emphasis on

45. *Id.*

46. Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235, 253 (2015) ("Even with the renewed emphasis on proportionality in the 2015 amendments, the proportionality test itself largely focuses on economic concerns. Indeed, the ''burden or expense'' that the court weighs against the needs of the case are largely financial burdens."); *see also* Samsung Elec. Am. Inc. v. Chung, 325 F.R.D. 578, 592 (N.D. Tex. 2017) (listing the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit as part of the proportionality analysis, many of which relate to the financial burden of discovery). *But see* Henson v. Turn, Inc., No. 15-cv-01497-JSW (LB), 2018 WL 5281629, at *5 (N.D. Cal. Oct. 22,2018) ("While questions of proportionality often arise in the context of

proportionality brought about by the 2015 amendments and the growing public debate over the importance of privacy, however, there has been a clear trend by courts and commentators toward recognition of privacy interests as an integral part of the proportionality analysis required by Rule 26(b)(1).

With the publication of *The Sedona Principles, Third Edition* in 2018, Principle 10 was "modified to refer specifically to privacy obligations because of the increasing importance of privacy in the United States and abroad."[47] Principle 10 now states that "[p]arties should take reasonable steps to safeguard electronically stored information, the disclosure or dissemination of which is subject to privileges, work product protections, privacy obligations, or other legally enforceable restrictions." And new Comment 10.j, which expands on the prior Comment 10.e, instructs that "[p]arties should be aware of and identify personal privacy, trade secret, and confidential ESI [Electronically Stored Information], and properly protect such information from unlawful or inappropriate disclosure."[48] While the Comment still instructs parties that the possibility of a protective order or party agreement provides "[a]mple protections," the Third Edition now also urges parties to discuss appropriate protections for confidential information at the Rule 26(f) conference and even suggests, by way of example, that the "parties may agree to exclude from production categories of private, personal information that are only marginally relevant to the claims and defenses or are cumulative of other produced information."[49] Taken together with Comment 2.c's instruction that "[p]roportionality of discovery of ESI should be addressed by the parties

disputes about the expense of discovery, proportionality is not limited to such financial considerations.").

47. *The Sedona Principles, Third Edition*, *supra* note 39, at 44.

48. *Id.* at 162, cmt. 10.j.

49. *Id.* at 163.

and counsel at the Rule 26(f) meet and confer," Comment 10.j appears to embrace privacy as an aspect of proportionality.[50]

Support has also come from the academic sphere. Shortly after the 2015 amendments, Professor Agnieszka A. McPeak argued in *Social Media, Smartphones, and Proportional Privacy in Civil Discovery* that the proportionality analysis under Rule 26(b)(1) ought to consider not only financial burdens but also the burden of privacy.[51] Looking to the historical development of civil discovery under the Federal Rules and analyzing the intersection between civil discovery and general principles of privacy law, Professor McPeak concluded that courts should consider privacy interests as part of proportionality, particularly as applied to digital data compilations such as social media accounts and mobile devices.[52] More recently, Professor Babette Boliek has advocated for similar limitations in her 2018 article *Prioritizing Privacy in the Courts and Beyond*.[53]

Most importantly, a growing number of courts have followed suit. In October 2018, Magistrate Judge Laurel Beeler expressly held in *Henson v. Turn, Inc.* that privacy interests were an appropriate part of the proportionality analysis required by Rule 26(b)(1).[54] The case involved a data-privacy class action wherein plaintiffs alleged that the defendant had placed so-called "zombie cookies" on users' mobile devices that not only allowed the defendant to track users across the web but also "respawned" whenever users attempted to delete them. During discovery, the defendant issued a number of requests to plaintiffs, including requests for the production of the plaintiffs'

50. *Id.* at 67, 162.

51. McPeak, *supra* note 46, at 236.

52. *Id.*

53. Boliek, *supra* note 35, at 1129–31.

54. 2018 WL 5281629, at *5 (N.D. Cal. Oct. 22, 2018).

mobile devices for inspection (or complete forensic images of such devices), production of plaintiffs' full web browsing history from their mobile devices, and production of all cookies stored on or deleted from plaintiffs' mobile devices.[55] Plaintiffs objected that Turn's requests were "overbroad, irrelevant, and invasive of their privacy interests" and "fl[ew] in the face of Rule 26(b)'s relevancy and proportionality requirements."[56] In ruling on the requests, Judge Beeler unambiguously held that privacy was a valid proportionality consideration:

> While questions of proportionality often arise in the context of disputes about the expense of discovery, proportionality is not limited to such financial considerations. Courts and commentators have recognized that privacy interests can be a consideration in evaluating proportionality, particularly in the context of a request to inspect personal electronic devices.[57]

Judge Beeler collected numerous cases to support this proposition, mostly regarding requests either for inspection or for forensic images of computers or mobile devices, wherein the courts had found that such requests were disproportionate to the needs of the case.[58]

One such case involved an order from Magistrate Judge Nathanael M. Cousins of the Northern District of California in *In re: Anthem, Inc. Data Breach Litigation*, another data-privacy class

---

55. *Id.*

56. *Id.* at *4.

57. *Id.* at *5 (citing Tingle v. Hebert, No. 15-626-JWD-EWD, 2018 WL 1726667, at *7–8 (M.D. La. Apr. 10, 2018); Areizaga v. ADW Corp., No. 3:14-cv-2899-B, 2016 WL 9526396, at *3 (N.D. Tex. Aug. 1, 2016); Johnson v. Nyack Hosp., 169 F.R.D. 550, 562 (S.D.N.Y. 1996)).

58. *Henson*, 2018 WL 5281629, at *5.

action wherein the defendant had requested either access to or forensic images of plaintiff's devices—namely "computer systems that connect to the internet."[59] The defendant argued that its request was necessary in order to analyze whether the devices contained malware or other electronic markers establishing that the plaintiffs' personal information had been compromised prior to the cyberattack in question.[60] Plaintiffs, on the other hand, objected that the discovery was "highly invasive, intrusive, and burdensome." In denying defendant's request, Magistrate Judge Cousins applied the last Rule 26(b)(1) proportionality factor, finding that "the burden of providing access to each plaintiff's computer system greatly outweighs its likely benefit" and noting the "Orwellian irony" that would have resulted from a contrary ruling requiring "that in order to get relief for a theft of one's personal information, a person has to disclose even more personal information."[61] As Judge Cousins reminded the parties, "under the revised discovery rules, not all relevant information must be discovered."[62]

---

59. Order Denying Anthem's Request to Compel Discover of Plaintiff's Computer Systems, *In re* Anthem, Inc. Data Breach Litig., No. 15-md-02617 LHK (NC), 2016 WL 11505231, at *1 (N.D. Cal. Apr. 8, 2016).

60. *Henson*, 2018 WL 5281629, at *5.

61. *In re Anthem*, 2016 WL 1150523, at *1; *cf.* Miller, *supra* note 9, at 465 ("A legal system that does not recognize the right to keep private matters private raises images of an Orwellian society in which Big Brother knows all.").

62. *In re Anthem*, 2016 WL 1150523; *see also* Prado v. Equifax Info. Servs. LLC, No. 18-cv-02405-PJH (LB), 2019 WL 1305790, at *3 (N.D. Cal. Mar. 22, 2019); T.C *ex. rel.* of S.C. v. Metro. Gov't of Nashville & Davidson Cty., Tenn., No. 3:17-CV-01098, 2018 WL 3348728, at *14 (M.D. Tenn. July 9, 2018) ("[T]he party seeking to discover those thoughts and feelings via social media must still make a showing of relevance and proportionality to the claims of the litigation."); Hespe v. City of Chicago, No. 13 C 7998, 2016 WL 7240754, at *3 (N.D. Ill. Dec. 15, 2016) ("[I]nspection of plaintiff's electronic devices is not proportional to the needs of this case because any benefit the inspection might provide is outweighed by plaintiff's privacy and confidentiality

In addition to these decisions, several other recent cases have denied motions to compel because of privacy concerns but without explicitly framing the question within the proportionality framework provided by Rule 26(b). For example, in *Locke v. Swift Transportation Co. of Arizona, LLC*, a district court denied a motion to compel production of the entirety of the plaintiffs' social media accounts: "that some of a party's social media information is discoverable does not make the entirety of a party's social media information available for inspection [as this would] ''sanction an[] inquiry into scores of quasi-personal information that would be irrelevant and non-discoverable."[63]

Finally—and quite recently—the recently published *Sedona Conference Primer on Social Media, Second Edition* likewise takes the view that "[t]he proportionality limitation on the scope of

interests.") (internal quotation marks omitted); *Areizaga*, 2016 WL 9526396, at *3 (N.D. Tex. Aug. 1, 2016) ("[T]he Court finds that, on this record, ADW's request to obtain a forensic image of Plaintiff's personal electronic devices is too attenuated and is not proportional to the needs of the case at this time, when weighing ADW's explanation and showing as to the information that it believes might be obtainable and might be relevant against the significant privacy and confidentiality concerns implicated by ADW's request—even with ADW's offer to pay all expenses and to use a third-party vendor who will restrict ADW's access to the substantive information of any user-created files and particularly data that appears to be of a personal nature that may be included in the proposed forensic image."); Rodriguez Ayala v. Cty. of Riverside, No. EDCV 16-686-DOC (KKx), 2017 WL 2974919, at *4 (C.D. Cal. July 12, 2017) ("Here, in light of the limited relevance of the information balanced against the burden of production on the privacy rights of non-parties, the Court finds the discovery sought does not meet the proportionality requirement of Rule 26."); Crabtree v. Angie's List, Inc., No. 1:16-cv-00877-SEB-MJD, 2017 WL 413242, at*3 (S.D. Ind. Jan. 31, 2017) ("[T]he Court finds that the forensic examination of Plaintiffs' electronic devices is not proportional to the needs of the case because any benefit the data might provide is outweighed by Plaintiffs' significant privacy and confidentiality interests.").

63. No. 5:18-CV-00119-TBR-LLK, 2019 WL 430930, at *3 (W.D. Ky. Feb. 4, 2019).

discovery includes two factors that implicate privacy concerns, i.e., ''the importance of the discovery in resolving the issues, and whether the burden . . . of the proposed discovery outweighs its likely benefit."[64] Although the Primer cautions that privacy is not a per se bar to discovery as in the case of legal privileges, it nevertheless states that parties "consider managing the discovery to minimize potential embarrassment to third parties and protect against unnecessary disclosure of their sensitive personal information."[65]

THE IMPLICATIONS OF PRIVACY BEING AN ASPECT OF PROPORTIONALITY

Including privacy as part of the proportionality analysis has important implications for courts and litigants alike. As the Rules make clear, achieving proportionality is the responsibility of all parties: "the parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes."[66] Nor is the proportionality inquiry relevant *only* at the time when documents are finally handed over to the opposing party. As the advisory committee note to the 2015 amendment of Rule 37(e) explains, proportionality considerations are relevant as early as the preservation stage and will be considered a "factor in evaluating the reasonableness of preservation efforts."[67] Indeed, Comment 2.b of *The Sedona Principles, Third Edition* states that "[p]roportionality should be considered and applied by the court and parties to all aspects of the discovery and production of ESI including: preservation; searches for likely relevant ESI; reviews for

64. The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 27–28 (2019).

65. *Id.*

66. FED. R. CIV. P. 26 advisory committee's note to 2015 amendment.

67. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

relevancy, privilege, and confidentiality; preparation of privilege logs; the staging, form(s), and scheduling of production; and data delivery specifications."[68] Privacy considerations, therefore, are relevant from the outset—even when initially identify-ing the custodians, data sources, and time period likely to contain relevant information.[69]

A. Preservation

Our experience has shown that in a document review of any scale—especially if emails or other communications are involved—private personal information inevitably will be preserved and later swept up during the collection process. This includes not only personally identifiable information such as social security numbers and credit card information, but also more intimate and potentially embarrassing details, including everything from vacation photos to medical records. The more custodians, the broader the time period, and the more personal the data sources—especially chat systems, social media, and mobile devices—the more personal information will be potentially implicated downstream as a consequence. Moreover, such communications will very often involve numerous third parties, potentially implicating their privacy interests as well under both the Federal Rules and newer regulatory regimes such as GDPR and the CCPA.

Thus, while many preservation steps can seem like passive exercises, the impact on privacy can nevertheless be significant. Suspending the periodic deletion of emails under a corporate party's records retention policy, instructing employees in a legal hold not to delete text messages, and retaining the laptop of a

68. *The Sedona Principles, Third Edition*, *supra* note 39, at 67.

69. *See* Boliek, *supra* note 35, at 1134 ("A means to assure protection [of privacy] is to consider and weigh the affected parties' privacy interest at every step of the discovery process.").

departing employee (rather than repurposing it) all typically result in an increase in the volume of private personal information and, therefore, the potential exposure of private information in the event of an inadvertent release or data breach. Reducing such exposure is one of the primary reasons that companies implement such programs as part of their information governance programs. To achieve proportionality, therefore, a producing party may appropriately consider not only what is likely to be relevant but also what is likely to implicate privacy interests. Privacy interests therefore may serve as appropriate factors to reasonably limit the scope of preservation in many cases. For example, a party employee's personal email account—even if used on rare occasion for business purposes—might therefore lie outside of the appropriate scope of discovery.

B. Collection

At the collection and processing phases, privacy concerns are truly amplified. Data is copied from its source location and transferred to other systems for processing. Processed copies of the data are then loaded into still other systems, such as Early Case Assessment tools, for further analysis prior to review. Along the way, it is common for the data to pass through many hands. A typical collection workflow may involve the party's own Information Technology (IT) personnel, a dedicated eDiscovery collection vendor, and a separate eDiscovery review vendor, all overseen by inside and outside counsel. At the end of collections, there may be multiple copies of the data in both "raw" and processed forms stored in multiple locations, including intermediate locations such as removable media, file shares, and "staging" locations. As the Sixth Circuit has noted, "[d]uplication, by its very nature, increases the risk of improper

exposure, whether purposeful or inadvertent."[70] And "ESI productions in civil litigations can be ripe targets for corporate espionage and data breach as they may contain trade secrets and other proprietary business information; highly sensitive and private medical, health, financial, religious, sexual preference, and other personal information; or information about third parties subject to contractual confidentiality agreements."[71]

Those charged with identifying and collecting relevant data may therefore appropriately determine what data sources are likely to contain sensitive information *prior* to collection. Among other things, well-designed custodian interviews and close cooperation with internal IT personnel can help determine the likely relevance of a data source as well as the kind of sensitive information that might be contained in it. This information will allow counsel to make an informed choice about whether privacy interests should limit the scope of what is collected and, if so, in what matter.

Minimizing the privacy burdens when collecting from mobile devices is especially challenging.[72] For example, if a corporate party allows its employees to use their personal phones for business purposes, as is now common with bring-your-own-device (BYOD) programs, it can be difficult to disentangle business from personal data given the current state of mobile device collection technology, which often requires "imaging" the entire contents of the device. This is especially true where an employee has used text messaging or other personal communications apps for substantive business purposes. In such situations, if an employee's use for business purposes has been limited—as is

70. John B. v. Goetz, 531 F.3d 448, 457 (6th Cir. 2008).

71. *The Sedona Principles, Third Edition*, *supra* note 39, at 179 n.147.

72. *See generally* Robert D. Keeling, *The Challenge of Collecting Data from Mobile Devices in eDiscovery*, 18 SEDONA CONF. J. 177 (2017).

often the case—it may be more proportional to not collect the device at all. Or, at most, to assist the employee with running a limited number of searches and "screenshotting" any relevant messages, rather than capturing a forensic image of the entire device. Although this approach would not capture potentially relevant metadata, the relative importance of that metadata must be weighed against the potential privacy harm resulting from a forensic collection.

Personal messaging apps also present particular challenges when used for business purposes. Increasingly often, these tools include a number of privacy-oriented features such as encrypted and self-destructing messages. While these important features help to protect user privacy, they can result in communications being beyond an organization's reach if its employees use these apps for their work. Organizations may therefore wish to consider adopting a policy requiring employees to use a dedicated enterprise application with a limited retention period for business messaging. Although these "ephemeral" messaging applications have been scrutinized by some in the wake of the *Waymo, LLC v. Uber Technologies, Inc*. matter, not every use of such technology should arouse suspicion.[73] As stated in the recent public comment version of *The Sedona Conference Commentary on Legal Holds, Second Edition: The Trigger & The Process*: "Transient or ephemeral data not kept in the ordinary course of business (and that the organization may have no means of preserving) may not need to be preserved."[74] Moreover, certain enterprise editions of these tools allow parties to set a definite retention period (e.g., none, 3 days, 6 days, 15 days, 20 days), facilitate search and collection, and encourage separation of

73. No. C 17-00939, 2018 WL 646701 (N.D. Cal. Jan. 30, 2018).

74. The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341, 395 (2019).

business and personal communications. Their use should not be discouraged.

C. Review

At the review stage, the privacy implications are second perhaps only to those of production. In large reviews, dozens or even hundreds of lawyers, including contract lawyers retained solely for the purpose of review, will read and classify the collected materials. This disclosure is itself burdensome. Sharing sensitive information—especially regarding intimate personal, medical, religious, or financial matters—to a large group of people is a substantial burden, even if that information goes not further.

The use of Technology Assisted Review (TAR) can greatly mitigate the potential privacy burdens at the review stage, however. In the majority of matters, the most personal and embarrassing documents are often among the least likely to be relevant. Culling the document population based on likely relevance (as determined by a well-trained TAR model) will significantly reduce the need for any human to lay eyes on irrelevant documents containing private information. In addition, a number of search, analytics, and machine-learning approaches can help identify documents that are likely to implicate privacy concerns.

D. Production

In any large review, however, some not insignificant number of private information will nevertheless be subject to eyes-on review. For those documents that are irrelevant, the reviewers' task is typically to make sure that they are not inadvertently

produced.[75] A determination that a document is relevant, however, is not the end of the inquiry, as the Rules provide parties and courts with great flexibility to ensure that privacy concerns are respected.

One way this can be accomplished is through the use of Rule 26(c) protective orders. Often, parties agree to enter blanket protective orders that govern how confidential documents may be used by the receiving party.[76] However, even a carefully drafted protective order is sometimes insufficient. For one thing, there is no guarantee that it will be granted. Legal process in the U.S. tilts strongly toward public disclosure, and courts have on occasion rejected agreed-upon disclosure limitations because they gave "each party carte blanche to decide what portions of the record shall be kept secret."[77]

This aside, once a document is provided to another party, the producing party's control over that information is dramatically limited and the risk of disclosure heightened.[78] "[P]rotective

75. This can be easier said than done, especially in large reviews, which further bolsters the case for culling at the preservation, collection, and processing stages.

76. In recent years, privacy-conscious parties have negotiated consensual protective orders that not only limit how confidential information may be used, but also how produced information may be stored and transmitted. *See, e.g.*, *In re* Takata Airbag Prods. Liab. Litig., 1:15-cv-02599 (S.D. Fla. Aug. 28, 2015); *In re* Wells Fargo Collateral Protection Ins. Litig., 8:17-ml-02797 (C.D. Cal. Jan. 9, 2018). Often parties also negotiate procedures for the eventual deletion of many produced documents once the matter has been resolved.

77. Citizens First Nat. Bank of Princeton v. Cincinnati Ins. Co., 178 F.3d 943, 945 (7th Cir. 1999) (Posner, J.); *cf.* Miller, *supra* note 9, at 431–32 (opposing this trend).

78. *Cf.* John B. v. Goetz, 531 F.3d 448, 458 (6th Cir. 2008) ("[T]he imaging of these computers and devices will result in the duplication of confidential and private information unrelated to the [underlying] litigation. This

orders are effective only when the signatories comply with their parameters, and even then information can be misplaced or disclosed inadvertently."[79] This danger is particularly acute when the information produced has value outside of the litigation. Data breaches and leaks can irrevocably expose sensitive information to the public. This danger was realized in dramatic fashion in the *Zyprexa* litigation, in which a plaintiffs' expert, a lawyer not directly involved in the litigation, and a New York Times reporter subpoenaed millions of documents that were sealed under a protective order under false pretenses and then disclosed many of those documents to the public.[80] Further, even if information is not disclosed improperly, disclosing private information to a litigation opponent can itself pose a substantial burden on privacy interests.

Such concerns in our view should encourage parties to properly consider privacy concerns in evaluating individual documents. Consider, for example, a large spreadsheet file containing several dozen worksheets, each with thousands of lines, many of which contain extensive personal customer information that is of no relevance to the case. If one of the entries is technically relevant to a party's request, but it is not of significant "importance . . . in resolving the issues" in the case, must the entire file therefore be produced? We believe that a party acting in good faith can reasonably conclude that it need not, as it is not "proportional to the needs of the case" and is therefore not

duplication implicates significant privacy and confidentiality interests—regardless of whether the imaged media are initially held under seal—and these interests cannot be fully protected *ex post*.").

79. Boliek, *supra* note 35, at 1132.

80. *See id.*; William G. Childs, *When the Bell Can't Be Unrung: Document Leaks and Protective Orders in Mass Tort Litigation*, 27 REV. LITIG. 565, 578–97 (2008) (recounting the saga of the Zyprexa leak).

within the scope of discovery.[81] That it has already been collected and reviewed—and that the majority of the monetary costs of discovery associated with this document have therefore already been incurred—does not change this. The burden of privacy is distinct and independent from the expense of litigation,[82] and the risks to privacy are felt primarily after, rather than before, production.

If so, the question then arises: must the party seek judicial relief before doing so or disclose the judgment to the opposing party? We are inclined to think not. While the temptation to use privacy as a stalking horse to gain an unfair litigation advantage is real, it is not unique. For better or worse, the same danger is present whenever a party makes relevance determinations, which are not logged or otherwise disclosed. And unlike documents withheld on the basis of the attorney-client privilege—which are often highly relevant—the good-faith determination discussed here is that the burden of privacy outweighs the value in the production of a marginally relevant document.[83] This kind of calculus is codified in Rule 26(b) and reflects the kind of common sense decision-making that parties have routinely made, both before and after the 2015 amendments.[84] When a

81. FED. R. CIV. P. 26(b)(1).

82. *See* McPeak, *supra* note 46, at 291 ("Nonpecuniary burdens are a necessary consideration as a limit to civil discovery and an important aspect of the proportionality analysis.").

83. So-called "privacy logs," are unnecessary and would amount to a *de facto* amendment to Rule 26(b)(1). They may, however, be useful in instances where there are other legal protections of privacy in play. *See In re* Xarelto (Rivaroxaban) Prods. Liab. Litig., MDL NO. 2592, 2016 WL 2855221, at *5 (E.D. La. May 16, 2016); Kristen A. Knapp, *Enforcement of U.S. Electronic Discovery Law Against Foreign Companies: Should U.S. Courts Give Effect to the EU Data Protection Directive?*, 10 RICH. J. GLOBAL L. & BUS. 111, 127 (2010).

84. *Cf. In re* Convergent Techs. Sec. Litig., 108 F.R.D. 328, 331 (N.D. Cal. 1985) (Under the 1983 amendments, "counsel . . . *must* make a common sense

document (or set of documents) is both of significant relevance and poses a significant burden on privacy, however, a party should identify the right balance to strike—whether through redactions, a protective order, or some other mechanism. As with most other discovery matters, a little common sense and reflection usually allow a party acting in good faith to reach a reasonable and defensible conclusion.

Finally, the burden of protecting appropriate privacy interests during litigation counsels in favor of cost shifting in many cases. If a requesting party has served document requests that will require significant work to protect legitimate privacy interests in the course of responding to those requests, the producing party often will be justified in seeking the producing party to share some or all of that burden. The burdensome and expensive costs of privacy redactions, for example, often constitutes a prime opportunity for cost shifting. This will further have the effect of encouraging cooperation between the parties on limiting the scope of production of minimally relevant documents that entail expensive privacy review in order to produce.

CONCLUSION

There is an emerging consensus that privacy burdens may properly be considered as part of the proportionality analysis required by revised Rule 26(b)(1) to determine the scope of discovery. Those burdens grow heavier as discovery progresses

---

determination, taking into account all the circumstances, that the information sought is of sufficient potential significance to justify the burden the discovery probe would impose, that the discovery tool selected is the most efficacious of the means that might be used to acquire the desired information (taking into account cost effectiveness and the nature of the information being sought), and that the timing of the probe is sensible, i.e., that there is no other juncture in the pretrial period when there would be a clearly happier balance between the benefit derived from and the burdens imposed by the particular discovery effort.").

from identification through review and onto production, yet early decisions at the identification and preservation stage regarding the scope of discovery may have significant and widespread downstream privacy consequences. From the earliest stages of discovery, therefore, a producing party and its counsel may appropriately consider not only what is likely to be relevant but also what is likely to be private and unlikely to be relevant—i.e., to give careful attention to potential situations where "the burden or expense of the proposed discovery outweighs its likely benefit" and may therefore be beyond the scope of discovery. To the extent private information nevertheless is included in the collection, producing parties and their counsel may take reasonable steps at each phase of discovery, including making use of available technology, to reduce potential privacy burdens.