# Proportionality & Privacy

With the proliferation of social media platforms and other new technologies has come a renewed legal focus on privacy. Most of that focus has centered on data collection, storage, sharing, and, in particular, third-party transactions in which customer information is harnessed for advertising purposes. But what about other contexts? Could a party, for instance, decline to produce, review, or even collect certain types of data due to privacy concerns? Should privacy be considered a "burden" under the proportionality analysis required by Federal Rule of Civil Procedure Rule 26(b)?

Yes, say ROBERT D. KEELING and RAY MANGUM, a partner and associate, respectively, at Sidley Austin LLP. No, say Chief Judge LEE H. ROSENTHAL of the Southern District of Texas and Professor STEVEN S. GENSLER of the University of Oklahoma College of Law. For this edition of Point/Counterpoint, we asked each author team to contribute an essay to share their perspectives, making us privy to their privacy thoughts. — *Editors*

# The Burden of Privacy In Discovery

BY ROBERT D. KEELING
& RAY MANGUM

Historically, 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 were discoverable by default, 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 expense and nonpecuniary burdens imposed upon the 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 and proportional.

This emphasis on proportionality in discovery is particularly relevant at a time when the protection of privacy is of increasing concern in the United States and abroad. Relatively recent advances in technology — smartphones 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 EU's General Data Protection Regulation[1] (GDPR) and the California Consumer 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 proper scope of discovery.[3] As a result, an emerging consensus of courts and commentators has concluded that privacy interests may — and indeed, should — be considered as part of the proportionality analysis required under Rule 26(b)(1). As we 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.[4] 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."[5] In keeping with that aim, the scope of 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."[6] Even prior to the adoption of the Federal Rules in 1938, courts applied principles of proportionality to the cases on their dockets.[7]

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.[8] 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 ▸

## UNDER THE REVISED RULE 26(B)(1), PROPORTIONALITY ONCE AGAIN STANDS ON EQUAL FOOTING ALONGSIDE RELEVANCE IN DEFINING (AND LIMITING) THE SCOPE OF DISCOVERY. IF IT IS NOT BOTH RELEVANT AND PROPORTIONAL, IT IS NOT DISCOVERABLE.

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."[9]

The revised Rule "recogni[zed] that the right of pretrial disclosure is subject to some limitation beyond relevance."[10] At that time, it was aimed most squarely at curbing the types of duplicative, excessive, "scorched earth" discovery practices that were prevalent — i.e., at the problem of so-called "overdiscovery."[11] 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."[12] In other words, the 1983 amendment was seen as limiting the depth rather than the breadth of discovery.[13]

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."[14] 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 discovery in resolving the issues."[15] These changes were intended to "enable the court[s] to keep a tighter rein on the extent 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 (and limiting) the scope of discovery.[21] If it is not both relevant and 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 noted 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)

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.[24] 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."[25] Showing good cause was (and is) often difficult in contested matters.[26] Even with the rise of stipulated protective orders, invasive discovery remained the norm, and protection of personal privacy the exception.[27]

The pre-2015 history of the amendments to Rule 26(b)(1) shows that early discussions of the proportionality factors focused primarily on economic concerns rather than nonpecuniary burdens.[28] Moreover, when courts did apply the proportionality factors, they similarly emphasized the economic burdens of discovery as the primary consideration to limit the scope of discovery.[29] This focus on the monetary costs of e-discovery was particularly acute with the rapid technological advancements that brought about the "information explosion" of the early 1990s, and that has now ushered in the

current era of Big Data.[30] It seems less than surprising, that with the increasingly voluminous amount of data now within the realm of discoverable information, the parties and courts would be concerned with the excessive costs of disproportionate discovery requests.[31]

This is all to say that the significant monetary expense of over-discovery was but one factor — and, admittedly, an important one — in the decision to emphasize proportionality in discovery. But the fact that specific, nonpecuniary burdens, such as privacy, were not explicitly discussed at length in the pre-2015 history of the amendments does not foreclose it as a proper factor in conducting a proportionality analysis.[32] To the contrary, the Rule's text is plain, and it clearly evinces the drafters' intent that both monetary costs and additional nonpecuniary "burdens" must be weighed. The 2015 Advisory Committee Note to Rule 26(b)(1) expressly makes this point: "It also is important to repeat the caution that the monetary stakes are only one factor, to be balanced against other factors."[33] Further, the Advisory Committee recognized that, even in 1993, the concerns justifying proportionality in discovery were not limited to monetary costs: The 1993 Committee Note further observed that "[t]he information explosion of recent decades has 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."[34] Rather than foreclose privacy as an appropriate factor in the analysis, the text and history expressly contemplate that proportionality should take into account nonpecuniary burdens of precisely this sort.

The history of a similar provision within the Rules further supports the position that privacy is a kind of "burden" that a court should consider. In discussing Rule 34, the Advisory Committee Note to the 2006 Amendments expressly states that "issues of burden" raised by Rule 34(a)(1) include "confidentiality [and] privacy" concerns. Thus, construing the word "burdens" in the Rule 26(b)(1) proportionality analysis to include privacy concerns is consistent with the use of that term in a related provision of the same Rules. This construction is further bolstered by the fact that the Advisory Committee stated that Rule 34(a)(1) privacy 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)."[35] Implicit in this directive is the Advisory Committee's intent that the burden of privacy may be considered in setting the scope of discovery.

Cases that address direct-access requests under Rule 34(a)(1) are instructive on how privacy should factor into proportionality analysis. Courts have frequently emphasized privacy concerns in these cases, where a party sought direct access to an opposing party's computer systems under Rule 34(a)(1), which allows parties "to inspect, copy, test or sample . . . any designated tangible things."[36] 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, not only because of the cost and inconvenience, but also because of the threat to privacy.[37]

While many of the early cases discussing direct-access requests under Rule 34(a)(1) cited privacy concerns, few did so within the framework of a Rule 26(b) proportionality analysis.[38] It is not that these cases rejected the proportionality framework, but rather that they simply did not reference 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."[39] Despite putting great weight on the privacy implications in its decision to grant relief, that opinion did not cite Rule 26(b).[40]

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 second edition of the *Sedona Principles* was 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,"[41] and Comment 10.e addressed "[p]rivacy, trade secret, and other confidentiality concerns."[42] The comment recognized that "[e]lectronic 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)."[43] 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."

## A Growing Consensus: Privacy Concerns are Part of the Proportionality Analysis

Even today, it remains common, among both the bench and the bar, to think of proportionality in discovery as relating primarily to financial burdens.[44] With the re-emphasis on 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). Indeed, a significant number of recent cases support the position that privacy concerns may properly limit the scope of discovery under Rule 26(b)(1)'s proportionality analysis.[45]

One of the earlier cases to expressly make the point, in October 2018, *Henson v. Turn, Inc.* held that privacy interests were an appropriate part of the proportionality analysis required by Rule 26(b)(1).[46] 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 that also "respawned" whenever users attempted to delete them. During discovery, the defendant requested production of the plaintiffs' mobile devices for inspection (or complete forensic images of such devices), plaintiffs' full web browsing history from their mobile devices, and cookies stored on or deleted from plaintiffs' mobile devices.[47] 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."[48] In its ruling, the court 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.[49]

The court 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.[50]

One such case cited by the *Henson* court involved an order from the Northern District of California in *In re: Anthem, Inc. Data Breach Litigation*, another data-privacy class action wherein the defendant had requested either access to or forensic images of plaintiffs' devices — namely "computer systems that connect to the internet."[51] 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.[52] Plaintiffs objected that the discovery was "highly invasive, intrusive, and burdensome."[53] In denying defendant's request, the court agreed that the requested information may be relevant to causation, but applied the last Rule 26(b)(1) proportionality factor to find that "the burden of providing access to each plaintiff's computer system greatly outweighs its likely benefit."[54] The court noted 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."[55] As the court reminded the parties, "under the revised discovery rules, not all relevant information must be discovered."[56]

Relying on these and other decisions,[57] the body of caselaw finding privacy as a proper basis for limiting discovery under Rule 26(b)(1) has continued to emerge and grow. In 2019, for example, the District of Oregon denied a motion to compel forensic imaging of plaintiffs' personal digital devices in a healthcare data security breach class action, *In re Premera Blue Cross Customer Data Security Breach Litigation*.[58] The court determined that the request was not proportional to the needs of the case in light of the competing privacy concerns: "[Defendants' request] may meet the low threshold for relevance of some information that potentially may be found on Plaintiffs' Devices, but it does not show a sufficiently close relationship between Plaintiffs' claims and the Devices to support the Court ordering the burdensome and intrusive imaging of Plaintiffs' Devices."[59]

Similarly, in 2020, the court in *In re 3M Combat Arms Earplugs Products Liability Litigation* rejected defendant's motion to compel forensic imaging of

THE COURT NOTED 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."

plaintiff's mobile device.[60] Defendant sought this data to show that plaintiff had spoliated evidence; specifically, that he deleted relevant text and Facebook messages with three individuals, the existence of which came to light during plaintiff's deposition.[61] Citing Rule 26(b)(1), the court explained that, "[e]ven assuming" the relevance of the deleted messages, "the parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes."[62] The court found that defendant "failed to demonstrate a compelling reason sufficient to justify compelled intrusion on [Plaintiff's] privacy."[63] Because recovery of the text of the deleted messages was not probable, the court held the requested forensic examination was "disproportionate to the slight importance of this potential discovery to the case."[64]

Most recently, in 2021, a court denied a motion to compel forensic examination of defendant's cell phone in *Estate of Logan v. City of South Bend*, a case raising constitutional claims based on the alleged use of excessive and deadly force by a police officer.[65] Turning to the scope of discovery under Rule 26(b)(1), the court found that plaintiff failed to identify how the requested cell phone information went "to the heart of — or [was] even relevant to — the . . . case," leaving the court unable to determine whether the request was proportional enough to justify invading defendant's privacy interests.[66] The court concluded that even though the expense of the inspection "would be negligible, the likely benefit is outweighed by the Defendant's privacy and confidentiality interests."[67]

In addition to this growing body of caselaw that recognizes privacy as part of the proportionality calculus,[68] the *Sedona Conference Primer on Social Media, Second Edition* likewise takes the view that "[t]he proportionality limitation on the scope of 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.'"[69] 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 "should consider managing the discovery to minimize potential embarrassment to third parties and protect against unnecessary disclosure of their sensitive personal information."[70]

## The Implications of Privacy As 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: "[T]he parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes."[71] 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 to 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."[72] Indeed, Comment 2.b of the third edition of the *Sedona Principles* 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 relevancy, privilege, and confidentiality; preparation of privilege logs; the staging, form(s), and scheduling of production; and data delivery specifications."[73] Privacy considerations, therefore, are relevant from the outset — even when initially identifying the custodians, data sources, and time period likely to contain relevant information.[74]

### 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 third parties, potentially implicating their privacy interests as well, both under 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 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 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 policies as part of their information governance programs. To achieve proportionality, a producing party may appropriately consider not only what is likely to be relevant, but also what is likely to implicate privacy interests. In other words, privacy interests may serve to reasonably limit the scope of preservation in certain cases. For example, a party employee's personal email account — even if used on rare occasion for business purposes — might lie outside of the appropriate scope of discovery and, accordingly, outside the scope of the duty to preserve.

## 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 IT personnel, a dedicated e-discovery collection vendor, and a separate e-discovery 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."[75] 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."[76]

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 within it. This information will allow counsel to make an informed choice about whether privacy interests may 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.[77] 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 because current mobile-device-collection technology generally 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 often the case — it may be more proportional not to collect the device at all; or, at most, it may be more proportional to assist the employee with running a limited number of searches and "screenshotting" 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 full forensic collection.[78]

Personal messaging apps also present particular challenges when used for business purposes. Increasingly, 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 employees use these apps for 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.[79] As stated in *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

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 NO FURTHER.

(and that the organization may have no means of preserving) may not need to be preserved."[80] 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 business and personal communications.

## REVIEW

At the review stage, the privacy implications are second perhaps only to those of the production stage. In large reviews, dozens or even hundreds of lawyers, including contract lawyers retained solely for the purpose of review, will read the collected materials and classify them for relevance and privilege. 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 no further.

The use of Technology Assisted Review (TAR) can greatly mitigate the potential privacy burdens at the review stage. 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.

## PRODUCTION

In any large review, however, some not-insignificant number of private information will nevertheless be subject to eyes-on review and potentially production. For those documents that are irrelevant, the reviewers' task is typically to make sure that they are not inadvertently produced.[81] A determination that a document is relevant, however, does not mean the document necessarily must be produced. The Rules provide parties and courts with great flexibility to ensure that privacy concerns are respected.

One way privacy can be protected is through the use of Rule 26(c) protective orders.[82] Often, parties agree to enter blanket protective orders that govern how confidential documents may be used by the receiving party. 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."[83]

This issue 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. "[P]rotective orders are effective only when the signatories comply with their parameters, and even then information can be misplaced or disclosed inadvertently."[84] 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 three individuals — 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.[85] 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 the discoverability of individual documents. Consider, for example, a large spreadsheet 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 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 within the scope of discovery.[86] [87] That the spreadsheet has already been collected and reviewed — and that the majority of the monetary costs of discovery associated with this document have already been incurred — does not change this calculus. The burden of privacy is distinct and independent from the expense of litigation,[88] and ▸

AS WITH MOST OTHER DISCOVERY MATTERS, A LITTLE COMMON SENSE AND REFLECTION USUALLY ALLOWS A PARTY ACTING IN GOOD FAITH TO REACH A REASONABLE AND DEFENSIBLE CONCLUSION.

the risks to privacy are felt primarily after, rather than before, production.

At every step in the discovery process, a party and its lawyers are charged with acting in good faith under the Rules to make reasonable determinations about whether certain information is discoverable. For example, a party makes countless relevance determinations prior to production that require the exercise of its subjective judgment about where to draw the line on relevance. None of these determinations are logged or otherwise disclosed. We believe a party is similarly capable of making an independent determination of whether a document is discoverable in light of privacy concerns. Unlike documents withheld on the basis of the attorney-client privilege — which are often highly relevant — the good-faith determination endorsed here is that the significant burden of privacy outweighs the value in the production of a *marginally* relevant document.[89] 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.[90]

We are not suggesting that a party may use privacy as a stalking horse to gain an unfair litigation advantage. Rather, we simply maintain that the burden on privacy is a proper factor in considering whether data is discoverable. When a document (or set of documents) is both highly relevant and poses a significant burden on privacy, a party must act in good faith to comply with its discovery obligations and identify the right balance to strike — whether through redactions,[91] seeking a protective order, or some other mechanism. As with most other discovery matters, a little common sense and reflection usually allows 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 responding to those requests, the producing party often will be justified in seeking the requesting party to share some or all of that burden. The burdensome and expensive cost of privacy redactions, for example, often constitutes a prime opportunity for cost-shifting. Cost-shifting will further encourage cooperation between the parties to limit requests for minimally relevant documents that entail expensive privacy review before production.

## 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 from identification through review and onto production, and early decisions at the identification and preservation stages 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.

**ROBERT D. KEELING** is the founder and head of the e-discovery and data analytics group at Sidley Austin LLP. He is the inaugural chair of the Electronic Discovery Reference Model (EDRM) Global Advisory Council.

**RAY MANGUM** is a litigation associate at Sidley Austin with a focus on complex e-discovery and data analytics. In 2021, he was named by *Chambers USA* as an "Associate to Watch" in the area of e-discovery and information governance.

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), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-:32016R0679#PP3Contents.

2 Cal. Civ. Code § 1798.100.

3 In their thoughtful response to our article, Judge Lee Rosenthal and Professor Steven Gensler suggest that we would assign to Rule 26(b)(1) the work of protecting privacy considerations in discovery, which they believe is solely within the province of Rule 26(c). Respectfully, it is the text of Rule 26(b)(1) itself, as numerous courts have recognized, that gives weight to "whether the *burden or expense* of the proposed discovery outweighs its likely benefit." Whereas "expense" covers monetary considerations, it is undisputed that "burden" is a separate and distinct category of factors that covers non-monetary considerations, and that properly includes privacy burdens.

4 *See, e.g.*, *Welty v. Clute*, 1 F.R.D. 446, 446–447 (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 Hartzog, *The Ultimate Unifying Approach to Complying with All Laws and Regulations*, 19 Green Bag 2d 223, 223 (2016) ("Be reasonable.").

5 Advisory Comm. on Rules for Civil Procedure, *Report of the Advisory Committee on Rules for Civil Procedure Containing Proposed Rules of Civil Procedure for the District Courts of the United States* (April 1937).

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

7 *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.").

8 Fed. R. Civ. P. 26(b)(1) (1983).

9 *Id.*

10 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 Vill. 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 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.'").

11 *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).

12 Fed. R. Civ. P. 26 advisory committee's notes (1983).

13 *See* Cavanagh, *supra* note 10, at 786–87 n.93 (citing Fed. R. Civ. P. 26(b)(1)); Am. Bar Ass'n Section of Litig., *Second Report of the Special Committee for the Study of Discovery Abuse*, 92 F.R.D. 149 (1977); Maurice Rosenberg & Warren R. King, *Curbing Discovery Abuse in Civil Litigation: Enough is Enough*, 1981 BYU L. Rev. 579; Mary M. Schroeder & John P. Frank, *The Proposed Changes in the Discovery Rules*, 1978 Ariz. St. L.J. 475.

14 Fed. R. Civ. P. 26 advisory committee's notes (1993).

15 Fed. R. Civ. P. 26 advisory committee's notes (2015).

16 Fed. R. Civ. P. 26 advisory committee's notes (1993).

17 *Id.*

18 Fed. R. Civ. P. 26 advisory committee's notes (2000).

19 Fed. R. Civ. P. 26 advisory committee's notes (2015).

20 *Id.*

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 Fed. R. Civ. P. 26 advisory committee's notes (1983) (stating that the changes to Rule 26(b)(1) were "designed to . . . limit the use of the various discovery devices").

25 Fed. R. Civ. P. 26(c) (1970).

26 *See, e.g.*, Richard L. Marcus, *Myth and Reality in Protective Order Litigation*, 69 Cornell L. Rev. 1, 23–26 (1983).

27 Fed. R. Civ. P. 26 advisory committee's notes (1983) (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").

28 *See* Fed. R. Civ. P. 26(b) advisory committee's notes (1983) (justifying the amendment because the overuse of discovery led to "excessively costly and time-consuming activities that are disproportionate to the nature of the case, the amount involved, or the issues or values at stake"); *see also* Babette Boliek, *Prioritizing Privacy in the Courts and Beyond*, 103 Cornell L. Rev. 1101, 1129 (2018) ("[t]he word 'privacy' was curiously absent from this new list of factors").

29 *Id.*

30 *See* Fed. R. Civ. P. 26(b) advisory committee's note to 1993 amendment ("The information explosion of recent decades has 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."). *See also id.* at advisory committee's note to 2000 amendment.

31 *See* Nicholas M. Pace & Laura Zakaras, RAND Inst. for Civ. Just., *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery* (2012), https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1208.pdf (detailing excessive costs of eDiscovery).

32 J. Rosenthal and Gensler give weight to the apparent absence of discussions regarding privacy concerns leading up to the 2015 amendments. While we agree that statements rooted in a provision's history may support an argument about the drafters' intent where the text is ambiguous, the same cannot be said for the absence of specific historical statements. Unlike affirmative statements, the omission of a particular statement tells us little about what the drafters actually intended.

33 Fed. R. Civ. P. 26(b) advisory committee's note to 2015 amendment.

34 *Id*. (emphasis added).

35 Fed. R. Civ. P. 34(a)(1) advisory committee's notes (2006).

36 Fed. R. Civ. P. 34(a)(1).

37 *See*, *e.g.*, *SEC 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 Enters., Inc.*, No. CIV.A. 12-2515, 2013 WL 3974535, at *2 (E.D. La. Aug. 2, 2013).

38 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, LLC*, 2013 WL 3974535, at *2.

39 531 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, 2009 WL 722056, at *7 (D. Kan. Mar. 18, 2009);

40 Even more recently, some courts have continued to deny Rule 34(a) requests because of privacy concerns but without explicitly framing the question within the proportionality framework provided by Rule 26(b). *See Locke v. Swift Transp. Co. of Ariz., LLC*, No. 5:18-CV-00119, 2019 WL 430930, at *3 (W.D. Ky. Feb. 4, 2019) (denying motion to compel production of entirety of plaintiffs' social media accounts because it would "sanction an[] inquiry into scores of quasi-personal information that would be irrelevant and non-discoverable").

41 *The Sedona Principles, Second Edition: Best Practices Recommendations & Principles for Addressing Electronic Document Production* 51 (The Sedona Conference Working Group Series, 2007).

42 *Id.* at 56 (Cmt. 10.e).

43 *Id.*

44 Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. Kan. L. Rev. 235, 253 (2015).

45 *See infra* note 53 and accompanying text for a discussion of supporting caselaw. J. Rosenthal and Gensler dismiss the cases we cite as exclusively direct access cases where judges seem to be protecting personal information because it is not relevant, not because it is private. Respectfully, many of the cases we cite find privacy concerns limit discovery under Rule 26(b)(1), even where the requested information is or may be relevant. For example, in the *Anthem* case discussed below, the court *agreed* with plaintiff that the requested information "might be probative of causation," but squarely held that the requested discovery was "disproportional to the needs of the case" and denied the motion to compel on that ground alone.

46 2018 WL 5281629, at *5.

47 *Id.*

48 *Id.* at *4.

49 *Id.* at *5 (citing *Tingle v. Hebert*, No. 15-626, 2018 ▶

WL 1726667, at *7–8 (M.D. La. Apr. 10, 2018); *Areizaga v. ADW Corp.*, No. 3:14-cv-2899, 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)) (emphasis added).

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

51 *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617, 2016 WL 11505231, at *1 (N.D. Cal. Apr. 8, 2016).

52 *Id*.

53 *Id*.

54 *Id*.

55 *Id*.; cf. Miller, *supra* note 10, 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.").

56 *Id*.

57 *See, e.g.*, *Prado v. Equifax Info. Servs. LLC*, No. 18-CV-02405, 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.*, No. 3:17-CV-01098, 2018 WL 3348728, at *14 (M.D. Tenn. July 9, 2018); *Hespe v. City of Chicago*, No. 13 C 7998, 2016 WL 7240754, at *3 (N.D. Ill. Dec. 15, 2016); *Areizaga v. ADW Corp.*, No. 3:14-cv-2899, 2016 WL 9526396, at *3 (N.D. Tex. Aug. 1, 2016); *Rodriguez Ayala v. County of Riverside*, No. EDCV16-686-DOC, 2017 WL 2974919, at *4 (C.D. Cal. July 12, 2017); *Crabtree v. Angie's List, Inc.*, No. 1:16-CV-00877, 2017 WL 413242, at *3 (S.D. Ind. Jan. 31, 2017).

58 *In re Premera Blue Cross Customer Data Security Breach Litig.*, 329 F.R.D. 656 (D. Or. 2019).

59 *Id*.

60 *In re 3M Combat Arms Earplugs Prods. Liab. Litig.*, No. 3:19-md-2885, 2020 WL 6140469 (N.D. Fla. Oct. 15, 2020).

61 *Id*. at *2.

62 *Id*. at *6.

63 *Id*.

64 *Id*.

65 *Estate of Logan v. City of South Bend*, No. 3:19-CV-495, 2021 WL 389412 (N.D. Ind. Feb. 3, 2021).

66 *Id*.

67 *Id*.

68 In addition to the many cases examined above in the text, numerous additional courts have weighed privacy concerns under Rule 26(b)(1)'s proportionality analysis to deny motions to compel the production of private information. *See*, *e.g.*, *Ruby Slipper Café, LLC v. Belou*, No. 18-cv-1548, 2020 WL 1674157, at *3–5 (E.D. La. Apr. 6, 2020) (citing Rule 26(b)(1) and denying motion to compel forensic imaging of two computers where the request was not proportional to the needs of the case); *Wengui v. Clark Hill, PLC*, No. 19-cv-3195, 2021 WL 106417, at *7 (D.D.C. Jan. 12, 2021) (applying Rule 26(b)(1) proportionality analysis and allowing for privacy redactions where the "germaneness" of the private information "is likely weak enough to be outweighed by the clients' privacy interests"); *Motorola Solutions, Inc. v. Hytera Commc'ns. Corp.*, 365 F. Supp. 3d 916, 924–26 (N.D. Ill. 2019) (noting request would impinge party's privacy interests and holding, under Rule 26(b)(1), that the "requested discovery is significantly out of proportion to the needs of the case"); *Hardy v. UPS Ground Freight, Inc.*, No. 3:17-cv-30162, 2019 WL 3290346, at *2 (D. Mass. July 22, 2019) (on motion to compel forensic imaging of cell phone, courts have considered "whether such an examination is proportional to the needs of the case given the cell phone owner's compelling privacy interest in the contents of his or her cell phone").

69 *The Sedona Conference, Primer on Social Media, Second Edition*, 20 Sedona Conf. J. 1, 27–28.

70 *Id.*

71 Fed. R. Civ. P. 26 advisory committee's note (2015).

72 Fed. R. Civ. P. 37(e) advisory committee's note (2015).

73 *The Sedona Principles, Third Edition* 67.

74 *See* Boliek, *supra* note 28, 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.").

75 *Goetz*, 531 F.3d at 457.

76 *The Sedona Principles, Third Edition* 179 n.147.

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

78 J. Rosenthal and Gensler express concern that counsel might unilaterally weigh privacy concerns against likely relevance to arrive at an appropriate approach to collecting a BYOD device, including potentially not collecting it. The better approach, they suggest, would be to discuss the need for preservation with the opposing party and, if agreement cannot be reached, to seek relief through a protective order. We are not suggesting that cooperation in discovery has no role in this process, and we agree that where the information at issue is likely to be central to the matter — or even likely to be of some importance — such an approach may be warranted. We believe that the scenario we describe above, however, is different. It involves a common, day-to-day, discovery decision that counsel might make at the end of a custodial interview with a collection vendor at her side — one of thousands of such decisions that might be made over the course of a matter. For those types of decisions, a pragmatic framework that allows counsel to operate in good faith to balance the appropriate considerations is far more workable, and is what Rule 26(b)(1)'s proportionality framework provides.

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

80 *The Sedona Conference, Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 Sedona Conf. J. 241 (forthcoming 2019), https://thesedonaconference.org/publication/Commentary_on_Legal_Holds.

81 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.

82 J. Rosenthal and Gensler claim that it is unnecessary to invoke Rule 26(b)(1) to protect privacy concerns because a Rule 26(c) protective order has "proven up to that task." But this argument does not consider the plain text of Rule 26(b)(1), the Advisory Committee Notes to the Rules, and the growing body of caselaw, all of which contemplate that privacy may be addressed under either Rule. Moreover, Rule 26(b)(1)'s proportionality analysis allows a party to address privacy at the outset of the discovery process, and in our view provides a more secure and flexible solution to the privacy burden.

83 *Citizens First Nat'l Bank of Princeton v. Cincinnati Ins. Co.*, 178 F.3d 943, 945 (7th Cir. 1999) (Posner, J.); *cf.* Miller, *supra* note 10, at 431–32 (opposing this trend).

84 Boliek, *supra* note 28, at 1132.

85 *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).

86 Fed. R. Civ. P. 26(b)(1).

87 Nor would it likely be proportional to attempt to redact the entire contents of the spreadsheet except for the single, technically relevant entry. Redactions, especially for spreadsheets, are tedious, time-consuming, and costly.

88 *See* McPeak, *supra* note 44, at 291 ("Nonpecuniary burdens are a necessary consideration as a limit to civil discovery and an important aspect of the proportionality analysis.").

89 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.*, No. MDL 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).

90 *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 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.").

91 *See*, *e.g.*, *Wengui*, 2021 WL 106417, at *7 (ordering redactions of private information in otherwise relevant documents).