The Privacy-Protection Hook in the Federal Rules

BY LEE H. ROSENTHAL
& STEVEN S. GENSLER

Imagine you are a lawyer seeking to prevent the production of electronically stored information (ESI) that is, or includes, some highly sensitive personal information. What rule do you invoke to get the protection you seek? If you are the judge, what rule do you use to grant that protection?

It's easy to imagine being this lawyer or judge. Requests to compel or prevent the production of private information in discovery arise often. Even as we reveal our innermost preferences to Amazon and our innermost feelings to social media, we are increasingly alarmed by the amount of personal information that is harvested, analyzed, sold, and sometimes stolen. And as all of this personal information proliferates, so too do the opportunities for it to come up in discovery.

By its nature, civil discovery is at odds with privacy.[1] Discovery is what makes litigation adversaries turn over the bits and bobs — or bales — that they want to keep private. The tension between pri- ▸

vacy and discovery is complicated by the fact that privacy interests cover a lot of ground, from protecting profits (as with trade secret or business proprietary information) to avoiding embarrassment, humiliation, or perhaps a job loss (as with medical information or information about past transgressions or errors in judgment). The pressures to balance our commitment to broad discovery with escalating privacy risks are already intense and continue to build.

What hooks do the Federal Rules of Civil Procedure provide to help judges know when to protect these privacy interests and when not to protect them, or at least not much? Robert Keeling and Ray Mangum argue that the 2015 proportionality amendments began a new era in protecting privacy from discovery. Their thesis is that the 2015 amendments made privacy part of the threshold proportionality analysis under Rule 26(b)(1). Accordingly, they argue, parties seeking to avoid discovery of relevant-but-private information may no longer need to seek a protective order under Rule 26(c) because the privacy concerns — as a proportionality factor — may place the information outside of what is discoverable in the first place.[2] In other words, in their view, parties can now hang their privacy arguments and objections on the Rule 26(b) scope hook rather than (or at least in addition to) the Rule 26(c) protection hook.

We agree with Keeling and Mangum that privacy is a significant challenge in discovery. But we think their proposed approach misses its mark in some key respects. We think there are important reasons to let Rule 26(c) do the heavy lifting of protecting privacy in discovery. And we don't think the 2015 amendments provide a sufficient, much less explicit, basis for making privacy part of the Rule 26(b) scope determination. In short, we think the 2015 amendments left the privacy-protection hook right where it was and — at least for now — right where it should be.

Rule 26(c): The privacy hook we've been using and why it works. As Keeling and Mangum acknowledge, the established mechanism for protecting privacy in discovery is to seek a protective order under Rule 26(c).[3] Protective orders have been used to shield private information in part because they are wonderfully flexible. They can prevent discovery into information — even if it is otherwise discoverable — because it is private. They can allow the discovery but reduce the intrusion by restricting how the information is accessed, used, or disseminated. Protective orders can be sought by or issued to parties and nonparties. The flexibility lets both ask the court to balance the level of privacy intrusion against the value of the information when the players cannot agree.

Do judges or lawyers view Rule 26(c) protective orders as inadequate for the task? We see no compelling evidence that Rule 26(c), which is both broad and flexible, has fallen short.[4] We recognize that an empirical case for or against is necessarily hard to present. But that raises the question we want to ask: What precisely is the Rule 26(c) protective order privacy beef that makes it desirable to move privacy protection into Rule 26(b)(1)?

Keeling and Mangum argue that making privacy part of the threshold scope analysis will benefit the system because protecting privacy then becomes a shared obligation.[5] But parties already have duties under Rule 26(g) that likely cover the most troublesome types of privacy-threatening behavior, such as seeking irrelevant private information or seeking relevant private information in order to disclose it. And Rule 1 makes clear that the obligations are shared by the parties and the court. Rule 26(b)(1) isn't needed to put all parties under the shared obligation to avoid inflicting embarrassment or unnecessary burden in discovery by exploiting privacy concerns. Rule 26(c) has proven up to that task.

The main consequence — and, as they see it, the main benefit — of their proposal is that responding parties could forego certain discovery activities if they determined that privacy protection needs kept the information sought outside the scope of the discoverable.[6] Privacy risks, they argue, are inherent in every step of the discovery process, from search to preservation, collection, review, and finally to production. They view discovery as a progressive set of hole-ridden, expensive, and burdensome dikes, with constant risks of leaks. The best way to avoid those risks, they suggest, is to avoid any of the discovery steps. Thus, upon concluding that there were overriding privacy interests, parties could unilaterally: (1) exclude information sources from being searched and the information preserved; (2) exclude information from what is collected; (3) exclude information from what is reviewed; (4) exclude information from what is produced at all; or (5) make "privacy redactions" from what is produced.

Consider a scenario Keeling and Mangum offer as illustration. Documents are requested from a company with a BYOD ("bring your own device" to work) policy. Relevant information is likely to be on the mobile devices of its employees; the company won't know until it looks. Personal information (most likely irrelevant) is certain to be on those devices as well. Under the scheme Keeling and Mangum describe, if the company concluded that privacy interests placed the information outside the Rule 26(b)(1) scope, the

RULE 26(B)(1) ISN'T NEEDED TO PUT ALL PARTIES UNDER THE SHARED OBLIGATION TO AVOID INFLICTING EMBARRASSMENT OR UNNECESSARY BURDEN IN DISCOVERY BY EXPLOITING PRIVACY CONCERNS. RULE 26(C) HAS PROVEN UP TO THAT TASK.

company could decide not to search or preserve, much less produce, information from those devices, even if some of those employees are involved in the dispute and even if some of their private information might be important.[7]

And that makes clear what we're really talking about. The Keeling and Mangum proposal is designed to "allow *counsel* to make an informed choice about whether privacy interests should limit the scope of what is collected and, if so, in what manner."[8] As they see it, the "burden" of intruding into the private information, the "expense" of disclosing the private information, and the risks that privacy will simply be lost in the leaky discovery steps outweigh the benefits of engaging in any part of the discovery process. No searching. No preserving. No way to question where the privacy line is drawn.

What's missing from this model? First, an exchange between parties on whether they can agree on a way to deal with the risks without foregoing discovery. The rules encourage cooperation in devising discovery in each case. Keeling and Mangum's approach, however, seems to encourage, or at least allow, unilateral choices. That is contrary to where the sidewalk moved in 2015, and the way we want to keep walking.

The second missing link is the judge. When opposing parties disagree on when stuff is too private to see the light of discovery, judges have resolved the issues by protective orders under Rule 26(c). Judges who engage in active and earlier case management often work with parties to protect privacy while allowing discovery. And in doing that work, judges have been guided by important norms like not barring inquiry or production altogether when some lesser form of protection would be adequate.

What would justify transferring that exercise of judgment from the judge to a party? Keeling and Mangum point to the risk that a judge might not provide the right level of protection, or the risk that the information might get leaked despite the judge ordering protection. We don't doubt that mistakes have been made. But we don't find much benefit in changing a risk of occasional under-protection to a likelihood of consistent over-protection. We recognize that some may deliberately disregard a judge's orders. But that is not a problem unique to privacy, and judges have tools to respond if that occurs. We don't currently allow parties to unilaterally restrict inquiry into promising sources of relevant information by silently concluding that their proprietary business information is too important to put at risk. We provide ways for this conclusion to be expressed, challenged, and tested.

We prefer the model of requiring the party seeking to avoid discovery into private information to have the burden of showing a need for protection. Parties often seek discovery of information that is intermingled with private information, including private information of or about nonparties to a lawsuit. Common examples are pornography on the devices or servers used by employees who are not parties in an employment discrimination case, amorous emails sent or received by these employees, or electronic evidence of employees shopping or movie watching on company time. This kind of information is often swept up in the relevant information, and it can be burdensome and expensive to begin to segregate it.

To show that relevant information need not be searched or preserved because it is intermingled with private information, the party seeking protection based on privacy concerns must show good cause for a protective order against discovery, which weighs the negative consequences of disclosure against the positives of getting the relevant information in discovery. Generally, good cause for an order preventing discovery of private information is a showing that simply ordering the receiving party not to use or disseminate the private stuff isn't enough to avoid the harm, because the nonmovant can't be trusted. A Rule 26(c) protective order does not find that the information is outside the scope of discovery. A Rule 26(c) protective order requires identifying, at least in general terms, what the information is and seeking guidance on disputes as to obligations to search or preserve it. A Rule 26(c) order doesn't let the responding party unilaterally run the privacy show. It's a structurally different hook than Rule 26(b)(1). That difference matters, not just to academics, but to lawyers and clients, and to judges. Hooks have consequences.

Rule 26(b): Did the 2015 amendments add a new privacy hook? We now return to Keeling and Mangum's main thesis — that the 2015 amendments changed the privacy-protection landscape by opening the door for privacy concerns to be factored into the scope analysis. As they put it, "[t]he renewed prominence of the Rule 26(b) ▸

IT IS HARD TO FATHOM WHAT THE RESPONSE MIGHT HAVE BEEN IF THE ADVISORY COMMITTEE HAD PROPOSED TO MAKE PRIVACY YET ANOTHER LIMIT TO THE SCOPE INQUIRY. COURTS HAVE BEEN SCOLDED FOR "AMENDING" THE RULES OUTSIDE THE CAREFUL, DELIBERATIVE RULEMAKING PROCESS.

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."[9] They conclude that "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)."[10]

Respectfully, but frankly, we don't see it that way. The cases they discuss involve requests to be given direct access to, or a forensic image of, another party's electronic device. Such broad requests for forensic walks through the parks of a party's cell phones, iPads, and laptops have long been subject to special requirements and limits. It's a distinctive setting. American civil discovery has operated on a longstanding norm that parties get to search their own records for requested information. Our discovery system is built on an assumption of trust — trust that parties will follow the rules and trust that attorneys will honor their duties to oversee the process. Thus, courts permit direct access only when the circumstances suggest that it would not be sufficient to rely on the efforts (past or future) of the responding party. When Rule 34 was amended in 2006 as part of the e-discovery amendments, the Advisory Committee made a point of emphasizing that the addition of the words "testing and sampling" to Rule 34(a) was "not meant to create a routine right of direct access to a party's electronic information system."[11]

The presumption against direct access protects privacy in two important ways. First, direct access indiscriminately exposes to the other side all of the contents within a source, whether or not the information is relevant or even relates to a requested topic. One key consequence of the presumption against direct access is that it permits parties to keep irrelevant information private. Second, the presumption against direct access recognizes that it is inherently intrusive for someone to rummage around in your own records, even when they are relevant.

But neither of these privacy concerns turns on whether the information in the source is personal or sensitive. The presumption against direct access applies without a need to show that the contents in the source are personal or sensitive. And the fact that a court denies direct access does not mean that the contents are outside the scope of discovery. Indeed, courts often deny direct access but then allow traditional discovery of the contents even when they are sensitive or personal. When courts talk about proportionality in the context of direct access, it is in the sense that the requesting party has not demonstrated a need for allowing a *method* of discovery that is antithetical to our "search your own" norm, that is inherently intrusive, and that is likely to expose large amounts of irrelevant information.

We think that the cases Keeling and Mangum discuss in their paper are best read as upholding the traditional privacy-based norm that a requesting party must have a very good reason to justify the intrusion associated with direct access. In *Henson* and *3M*, the responding party had already searched the devices in question and produced responsive information; the "privacy" concerns related solely to the intrusiveness of the request for direct access. In *Anthem*, the court denied the request for direct access — finding that "the burden of providing access to each plaintiff's computer system greatly outweighs its likely benefit" — but then held that the requesting party "might seek other, less intrusive and more targeted means" to seek the information it wanted, showing that its burden-benefit (i.e., "proportionality") conclusion concerned the request for direct access and not the underlying information. *Premera* and *Logan* similarly turn on the court's conclusion that the requesting party's explanation for why it wanted direct access didn't support that kind of intrusion. In most of these cases, the information sought through these forensic examinations was not relevant, much less important. In none of those cases did the court hold that the information being sought was outside the scope of discovery because it was private.

There's a second and more fundamental reason why we don't view the 2015 amendments as having interjected privacy into proportionality and scope instead of protective orders. The change Keeling and Mangum suggest would be a major departure from longstanding practice with significant (and as yet unexplored) practical implications. In a deliberative process that is known for its meticulous attention to every proposed addition, deletion, or change, one would expect a change of that nature to be made clearly and unmistakably, after extended Advisory Committee, Standing Committee, and public discussion. It would have been very easy

for the Advisory Committee to add the word "privacy" when it tinkered with and reordered the list of proportionality factors, but it didn't. Nor did the Advisory Committee mention privacy concerns in the accompanying committee note.[12] It is true that the term "burden" is open-ended and captures noneconomic concerns. But we struggle to accept the idea that the Advisory Committee interjected privacy into the proportionality calculus (and therefore into the scope of discovery) without using the word privacy in the rule text or the committee notes — and all while repeatedly telling people that the addition of the term "proportionality" was intended to reinforce existing discovery norms rather than change them.[13] The rulemakers do not hide elephants in mouseholes.

To be clear, the concept that Keeling and Mangum support is far from irrational. Under the current scheme, parties are often asked to round up and sift through vast stores of private information in response to far-ranging discovery requests. Traditional proportionality analysis may narrow and focus the process, but given the broad definition of relevance, much of that information can still make the cut. And much of it won't make any difference in the case outcome. We share their discomfort with a system that may expose so much for so little. It may well be time to rethink some of the rule choices we made in the past.

But those conversations did not occur as part of the 2015 amendments. They surely would have been noticed, and the question would have added to the controversy. Simply elevating the existing proportionality norm from the "basement" of Rule 26(b)(2) to the street-window level of Rule 26(b)(1) produced an enormous outcry from various interests concerned that making proportionality a part of scope would give producing parties a blunt weapon to deny access to information in discovery. It is hard to fathom what the response might have been if the Advisory Committee had proposed to make privacy yet another limit to the scope inquiry. Courts have been scolded for "amending" the rules outside the careful, deliberative rulemaking process. Yet that is precisely what Keeling and Mangum endorse here.

So, does privacy matter? Yes, and increasingly so. Should the law of discovery evolve to be more protective of private personal information? Probably, but we haven't had the conversations about how and when to do that. We think the correct path is not to try to retrofit privacy into proportionality, but to take the subject head on and see what happens. So, let's talk — in public, about what is private, what is discoverable, and what lies in between. We need all the tools we can get, as carefully and intentionally wrought as we know how to do.

LEE H. ROSENTHAL is chief judge of the U.S. District Court for the Southern District of Texas, vice president of the American Law Institute, and a member of the Bolch Judicial Institute Advisory Board.

STEVEN S. GENSLER is the Gene and Elaine Edwards Family Chair in Law and the President's Associates Presidential Professor at the University of Oklahoma College of Law.

1 *See Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 30 (1984) ("The Rules do not differentiate between information that is private or intimate and that to which no privacy interests attach. . . . Thus, the Rules often allow extensive intrusion into the affairs of both litigants and their third parties.").

2 *See* Keeling & Mangum, *supra* pp. 67, 70.

3 *See Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 34-35 (1984) ("Because of the liberality of pretrial discovery permitted by Rule 26(b)(1), it is necessary for the trial court to have the authority to issue protective orders conferred by Rule 26(c). It is clear from experience that pretrial discovery . . . has a significant potential for abuse. This abuse is not limited to matters of delay and expense; discovery also may seriously implicate privacy interests of litigants and third parties."); Fed. R. Civ. P. 34(a) advisory committee note (1970) ("Protection may be afforded to claims of privacy or secrecy or of undue burden or expense under what is now Rule 26(c).") (emphasis added).

4 As discussed later, we think the cases Keeling and Mangum discuss are off point because they involve requests for direct access or forensic imaging, a question of method of discovery rather than whether the content is or is not discoverable. But even in those cases, we can't think of any reason why those courts couldn't have, and wouldn't have, come to the same conclusions had the matter been presented by way of a request for a protective order under Rule 26(c).

5 *See* Keeling & Mangum, *supra* p. 71.

6 *Id.* at 71–74.

7 Ordinary proportionality principles might lead to a decision not to collect data from the device of an individual who was only tangentially involved in the dispute. But that's nothing new. In the paper world, companies didn't have to look in every folder in every file cabinet in every office.

8 *See* Keeling & Mangum, *supra* p. 72 (emphasis added).

9 *Id.* p. 67.

10 *Id*.

11 Fed. R. Civ. P. 34(a) advisory committee's note (2006). Keeling and Mangum cite to the 2006 Rule 34 committee notes as evidence that the door has been opened to treat privacy as a scope factor. *See* Keeling & Mangum, *supra* p. 69. The passages they cite all appear in the part of the note explaining the presumption against direct access and do not address underlying discoverability.

12 We also don't see in the extensive discussions leading up to the 2015 amendments to Rule 26(b)(1) much, if any, specific discussion about protecting privacy. We don't see evidence that the rulemakers, or the lawyers and litigants who advised the rulemakers during the public comment period, saw an important part of the Rule 26(b)(1) reform as protecting private information from discovery as disproportionate.

13 *See* Fed. R. Civ. P. 26 advisory committee's note (2015) ("Restoring the proportionality calculus to Rule 26(b)(1) does not change the existing responsibilities of the court and the parties to consider proportionality.").