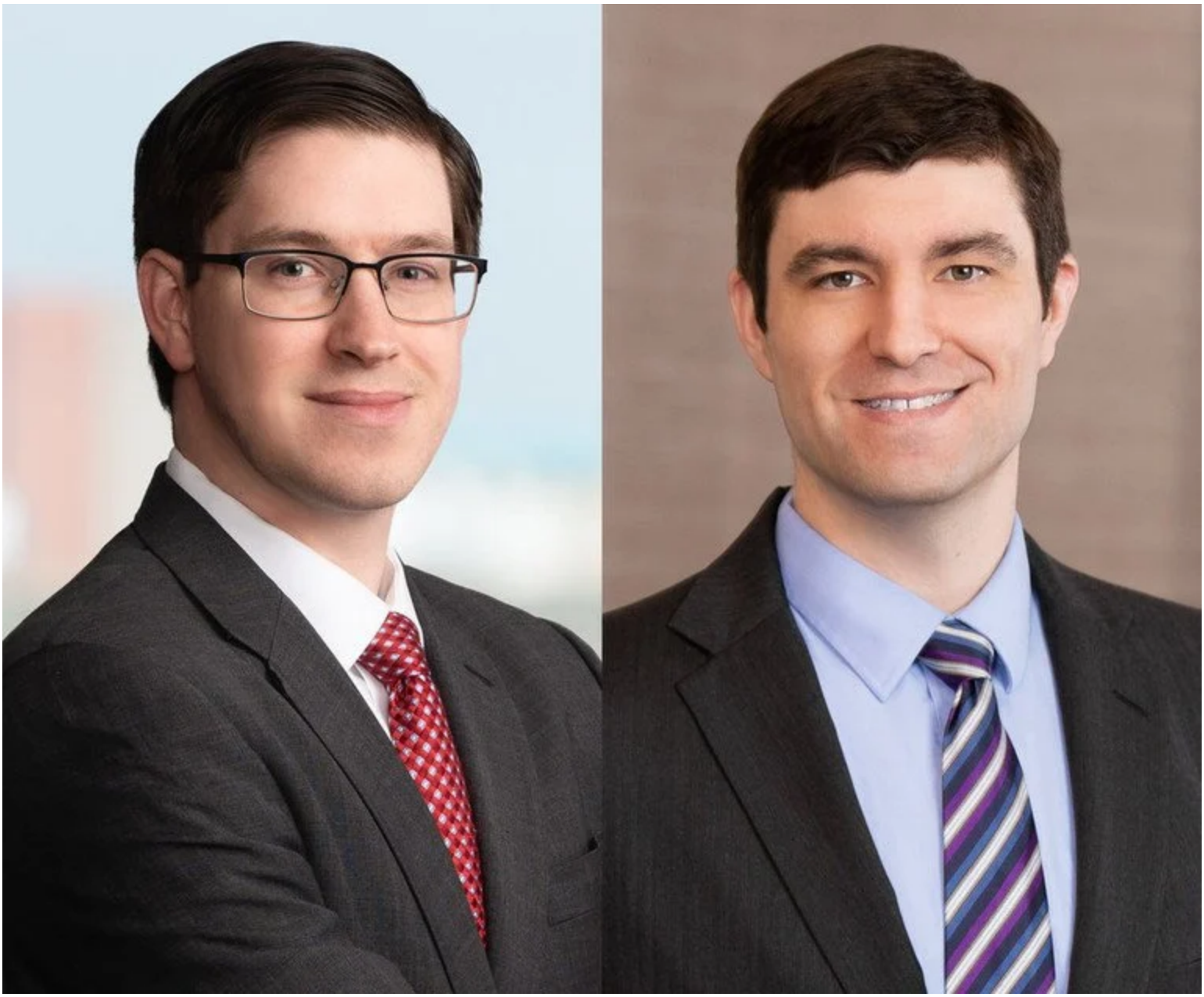
Knowing When to Take a Deeper Dive: Requests for Forensic Examinations in E-Discovery

Increasingly, these disputes end up in a fight over relief that was once rarely sought (and even more rarely granted) but has become more and more common: requests for a court-ordered forensic examination of the producing party's systems or devices to find any "missing" data.

By **Nick B. Snavely and Benjamin M. Redgrave** | February 02, 2022



Benjamin M. Redgrave(L) and Nick B. Snavely(R) of Redgrave. Courtesy photos

We have all seen it before. You are trying to get information to prove or defend your case, but what the opposing party produces does not seem sufficiently complete. Or perhaps it is the other way around; your client has already produced thousands (or millions) of documents, but still, the other side believes you are hiding something and that more data "must" exist. Increasingly, these disputes end up in a fight over relief that was once rarely sought (and even more rarely granted) but has become more and more common: requests for a court-ordered forensic examination of the producing party's systems or devices to find any "missing" data.

As recent cases in this space have demonstrated, courts have generally refused to order such examinations based solely on the requesting party's speculation or skepticism, but it is a different story where there is clear evidence data existed at one point that now cannot be found. And even where examinations are ordered, courts have put a variety of safeguards in place to protect the privacy and confidentiality interests that such examinations threaten. Before initiating a request for forensic examination, here are some considerations and background to keep in mind.

Forensic Examination Availability

Courts agree on the starting point: because it involves direct intrusion into a company's internal data environment, a forensic examination is "an extraordinary remedy" *Belcastro v. United Airlines*, No. 17 C 1682, (N.D. Ill. Dec. 23, 2019) and a "drastic discovery measure …" See *Stewart v. First Transit*, No. CV 18-3768, (E.D. Pa. Sept. 3, 2019). Courts tread lightly before granting such relief, and with good reason—improvidently ordered forensic examinations or imaging are one of the rare circumstances in which federal appellate courts have granted mandamus relief in the discovery context. See *John B. v. Goetz*, 531 F.3d 448, 460 (6th Cir. 2008) (granting mandamus relief and overturning a district court order that had compelled forensic imaging of computer hard drives, because "compelled forensic imaging is not appropriate in all cases, and courts must consider the significant interests implicated by forensic imaging before ordering such procedures.").

For courts to even consider ordering an examination, there needs to be something more than "[m]ere suspicion" or "speculation that an opposing party may be withholding discoverable information …" See *Hespe v. City of Chicago*, No. 13 C 7998, (N.D. Ill. Dec. 15, 2016). And even where some legitimate basis exists to think a forensic exam would turn up missing data, "the court must weigh the utility of the proposed examination against inherent privacy concerns." See *Valdes v. Greater Naples Fire Rescue District,* No. 2:17-CV-417-FTM-29CM, (M.D. Fla. Sept. 7, 2018). In particular, "a court must be mindful of the potential intrusiveness of ordering forensic imaging," and before compelling a forensic examination "must weigh inherent privacy concerns against its utility." See *Wynmoor Community Council v. QBE Insurance*, 280 F.R.D. 681, 687 (S.D. Fla. 2012). Moreover, courts will generally deny a motion to compel forensic imaging of personal electronic devices "if the party seeking the image fails to show that it will likely produce the material it seeks, if an alternative, less invasive means of obtaining the evidence exists, or if the motion is not accompanied by a proposal for a protocol appropriately tailored to protect the privacy concerns of the opposing party." See *Hardy v. UPS Ground Freight*, No. 3:17-CV-30162-MGM, (D. Mass. July 22, 2019).

Two recent cases seeking to examine individuals' mobile phones illustrate the difference. In one, the defendants sought a forensic examination of a litigant's phone to test generally whether the production from it was complete. The court denied the request because the defendants could point to no clear discrepancy in the production, and "mere skepticism, suspicion, or speculation concerning the completeness of a party's discovery production" was no basis to order a forensic exam. See *In re 3M Combat Arms Earplug Products Liability Litigation*, No. 3:19-MD-2885, (N.D. Fla. Oct. 15, 2020). In the second case, by contrast, there was something beyond mere suspicion to suggest an examination would turn up relevant data: the plaintiffs had produced an eight-second video taken with a mobile phone, but screenshots suggested the video was originally 13-seconds long. The court ordered a forensic examination of the phone over the plaintiffs' objection, emphasizing that the plaintiffs admitted the full video "existed at some point" and that the video was relevant to a central factual issue. See *Frazier v. Southeast Georgia Health System*, No. 2:21-CV-21, (S.D. Ga. Sept. 22, 2021).

Forensic Examination Safeguards and Standards

The commentary to the 2006 Amendments to Federal Rule 34 made clear that "direct access to a party's electronic information system … might be justified in some circumstances," but that "courts should guard against undue intrusiveness" in considering such relief. See Fed. R. Civ. P. 34, Advisory Committee Notes—2006 Amendment. Accordingly, if a court finds a forensic examination to be appropriate, it cannot simply order the producing party to fully open up its systems or devices to the other side—it needs to think creatively about how to protect privacy and confidentiality.

One consensus best practice that has emerged to mitigate the privacy and confidentiality (and sometimes, privilege) risks of a court-ordered forensic exam is for a neutral third party to conduct the exam, rather than the requesting party's experts. The Sedona Conference suggests that courts ordering forensic examinations "usually should provide that either a special master or a neutral forensic examiner undertake the inspection." See The Sedona Principles, Third Edition, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 19 SEDONA CONF. J. 1, 152-53 (2018). Courts around the country have followed suit, almost universally rejecting parties' requests that their own experts be permitted to examine opposing parties' systems rather than leaving the exam in the hands of a neutral third party. See, e.g., *United Artists v. United Artist Studios*, No. 219CV00828MWFMAAX, (C.D. Cal. Oct. 7, 2019) (ordering the parties to work cooperatively to select an independent expert to perform the tasks enumerated in the Search Protocol); Wynmoor Community Council, at *687 (noting that the court was "mindful of the potential intrusiveness of a compelling a forensic examination" and so would appoint "an independent computer expert" to conduct the examination).

To be sure, exceptions exist. But even then, courts take steps to protect the producing party's confidentiality interests. In *Peterson v. City of Minot*, No. 1:16-CV-271, (D.N.D. Oct. 17, 2018), the court permitted a limited forensic review of the plaintiff's laptop by defendants' expert after defendants offered "enough to demonstrate a reasonable possibility amounting to more than mere conjecture that material that is now discoverable may have been on the computer and deleted prior to the computer coming into the possession of plaintiff's counsel." To address the privacy concerns at stake, the court ordered that the examination "be limited in terms of content" to searching for specific types of information identified by the court. The court also set forth a protocol for the search and production of responsive information that required, among other things, that defendants' expert file a declaration with the court in which they agreed not to communicate the contents of any information reviewed or retained to any person(s), including defendants' counsel, without a prior order of the court, and that the defendants bear the costs of the examination.

An independent expert remains the gold standard, however, with protocols typically requiring the expert to agree to and sign a confidentiality order and provide the opposing party an opportunity to review any documents that are located before production to the requesting party. See, e.g., *Profit Point Tax Technologies v. DPAD Group*, No. 2:19-CV-698, (W.D. Pa. Mar. 3, 2021), report and recommendation adopted, No. 2:19-CV-698, (W.D. Pa. Apr. 22, 2021), No. 2:19-CV-698, (W.D. Pa. May 17, 2021).

Conclusion

The path to arriving at a court-ordered forensic examination is steep, though an opposing party's discovery conduct may warrant such an examination. Mere suspicion of misconduct or incompleteness is not enough, however, and courts are unlikely to order an examination absent compelling circumstances because of the substantial privacy concerns involved. Even if an examination is granted, the most likely outcome is the appointment of an independent expert, whose fees may have to be borne in whole or in part by the requesting party—not direct access for the requesting party and its experts. Thus, before investing time and money in pursuing a motion for forensic examination, the practitioner should ask himself whether the opposing party's unexamined production process is indeed worth exploring.

Nick Snavely *is a partner with the law firm of Redgrave LLP in its Chicago office. An experienced litigator, Snavely focuses his practice on complex e-discovery issues, including negotiations with opposing counsel and third parties. He can be reached at nsnavely@redgravellp.com.*

Benjamin Redgrave *is an attorney with the firm n its Chicago office. Redgrave works on e-discovery issues arising from complex litigation or corporate transactions. He can be reached at bredgrave@redgravellp.com.*