**“Can They Really Get Access to Our Hard Drives?”  
The Fine Line between the Discovery of Electronic   
Information & the Reasonable Expectation of Privacy**

*Jake Rutherford & T. Ray Guy[[1]](#footnote-1)*

Given the proliferation of electronic communications and cloud-based data storage and the general increase in reliance on technology to conduct business, litigators by now know they must possess a modicum of computer savvy (or at least hire associates who do) to effectively and competently engage in the discovery process. Countless CLE courses and practice aids are devoted to this very topic. Indeed, a significant part of a typical litigation associate’s first few years in a law firm will be devoted to immersing him- or herself in the increasingly complex and ever-changing e‑discovery landscape.

Both federal and state courts have done their best to update their respective rules of civil procedure to keep up with the resulting practice changes—largely consistent with the general principles that have informed the discovery rules for decades, with additions as necessary to reflect today’s realities. Much has been written on the subject, but litigators must keep constantly keep abreast of new trends given the recursive nature of our discovery rules and their interpretation by courts.

The Texas Supreme Court recently revisited one important aspect of e-discovery in *In re Shipman*: when, and under what circumstances, is a party entitled to direct access to and forensic examination of an opposing party’s hard drives? 540 S.W.3d at 562 (Tex. 2018). As such, we thought the time was right to review this question in the context of the federal and state rules and decisions to identify common themes and key differences.

***The General Framework***

The framework for analyzing these disputes is more or less uniform between the federal rules and those of the states that we have reviewed. As an initial matter, gaining direct access to an opposing parties hard drives, computers, and other storage media is viewed as “highly intrusive,” and is the exception, not the rule. The Advisory Committee Notes to the 2006 amendment to Federal Rule 34(a) state:

The addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party’s electronic information system . . . . Courts should guard against undue intrusiveness resulting from inspecting and testing such systems.

Still, there are circumstances when such intrusion becomes appropriate, whether it be through a producing party’s lack of technological wherewithal or its obstinacy in complying with discovery obligations in the first instance.

In *In re Weekley Homes, L.P.*, 295 S.W.3d 309 (Tex. 2009), the Texas Supreme Court effectively summarized the federal framework:

1. “As a threshold matter, the requesting party must show that the responding party must that the responding party has somehow ***defaulted in its obligation*** to search its records and produce the requested data.” *Id.* at 318.
2. If the threshold is met, ***only a qualified expert***, not the party itself, should be afforded access to the opponents’ device—and only when there is some indication that the data sought will be present on the device. *Id.*
3. ***Reasonable limitations*** should be imposed on any search to address concerns over privilege, privacy, and confidentiality concerns.

Courts—whether state or federal—work through this general framework under Rule 26’s cost-benefit analysis (or a state-law equivalent). *Id.* at 317. As such, and as a foreseeable consequence of this analysis, the scales are more likely to tip in favor of the requesting party’s direct access to the opponent’s electronic media when there is a close relationship between the claims at issue and the equipment to which the party is seeking access.

***Establishing the Default***

For any dispute in which direct access to the opponent’s media might be an eventuality, there are certain steps to be taken to lay the groundwork. Somewhat counter-intuitively, litigators who anticipate requesting such discovery should take every reasonable step to obtain the information without the necessity of direct access. Courts view direct access as a last resort, and will generally only allow the same when the record shows that the requesting party has acted in good faith and given the opposing party every reasonable opportunity to comply with the discovery requests. *See, e.g.*, *Vaughan Co. v. Global Bio‑Fuels Tech., LLC*, Civ. No. 1:12-CV-1292(DNH/DJS), 2016 WL 6605070 at \*2 (N.D.N.Y. May 20, 2016). For example, the *Vaughan* court, in granting the plaintiff direct access to the defendant’s personal computer, took solace in the fact that (1) the defendant’s work computer had been lost (making the information otherwise unavailable), and (2) the plaintiff’s counsel made good faith attempts to acquire the information by less intrusive means. *Id.*

Second, in seeking direct access, the requesting party needs an evidentiary record that rises above “mere skepticism or bare allegations that the responding party has failed to comply with its discovery duties.” *In re Shipman*, 540 S.W.3d at 568. The *Shipman* court dealt with the question of the responding party’s lack of technical savvy as a justification for direct access. It found that the requesting party had not established that the responding party was unable to conduct a search of the back-up files in question—rather, there was only “mere skepticism” that that was the case. To that end, *Shipman* provides a valuable lesson to those seeking to resist direct access discovery. If you encounter additional responsive information at any point, *produce it* (as any responsible litigator would). The court specifically cited the prompt production of additional documents, as they were located, as evidence of the producing party’s ability to operate his computer and locate and retrieve responsive information.

Alternatively, if the claim is that the producing party is *unwilling* to provide the requested discovery, the requesting party should provide evidence that the responding party has destroyed evidence or has otherwise failed to meet his or her discovery obligations. *See, e.g.*, *Diepenhorst v. City of Battle Creek*, No. 1:05-CV-734, 2006 WL 1851243 at \*4 (W.D. Mich. June 30, 2006).

***Tailoring the Requests***

The requesting party must show that the proposed method of direct access will yield responsive material. In denying the plaintiff’s request for direct access, the *Weekley* court pointed out that the requesting party did not establish that a search of the employee’s hard drives would be likely to reveal deleted emails or that any such e-mails would be recoverable. *In re Weekley*, 295 S.W. at 319–20. Put simply, the requesting party’s expert should be able to specify why he or she thinks there is responsive information and why such information will be accessible if located.

Given the volume and breadth of data available in a direct-access inspection of an opposing party’s electronic devices, court require specific protections for sensitive personal or otherwise proprietary information. In *Vaughan*, the court ordered that the requesting party establish search terms and criteria by agreement between the parties, or otherwise by approval of the court, that were designed to prevent the disclosure of “confidential, or personal and irrelevant, material.” *Vaughan*, 2016 WL 66505070 at \* 3. Likewise, in *TBG Insurance Services Corp. v. Superior Court*, the court found that “[a]ppropriate protective orders can define the scope of [the plaintiff’s] inspection and copying of information . . . to that which is directly relevant.” 96 Cal. App. 4th 445, 454 (2nd Dist., Div. 1 Feb 22, 2002). To be safe, rather than wait for the court’s direction, the requesting party’s expert should provide evidence that such protections are feasible and, in appropriate cases, provide suggestions for the contours of those protocols. *See Diepenhorst*, 2006 WL 1851243 at \*4 (explaining that defendant had not “identified any category of relevant discovery material that may be uncovered”). After all, even in this new era, courts will not allow fishing expeditions. *In re Shipman*, 540 S.W.3d at 566.

***Close Relationship***

As discussed, courts are more likely to allow direct access to storage devices or electronics when the device itself is closely related to the dispute. This is because, “[i]n most cases, the computer itself is not evidence . . . [i]t is merely the instrument for creating evidence.” *Diepenhorst*, 2006 WL 1851243 at \*2. Seeking to recover additional responsive information through deleted e-mails and the like is simply not as compelling as circumstances in which the device itself is likely to provide direct, highly-relevant evidence.

From our review, this principle seems to manifest itself most often in employment disputes. For example, in *Vaughan*, the court allowed direct access to the defendant’s personal laptop when the company laptop had been lost and the allegations were that defendant “utilized Vaughan’s confidential files on his computer in order to underbid Vaughan on various projects,” because the laptop was likely to contain information that was “relevant to the dispute.” *Vaughan*, 2016 WL 6605070 at \*2. Likewise, in *TBG Insurance Services Corp.*, the plaintiff claimed to have fired defendant for cause due to his penchant for perusing pornographic websites on the company’s computers. Although the plaintiff had through discovery obtained evidence from the defendant’s office computer, it was entitled to access to the defendant’s work-provided home computer, in part to rebut the defendant’s defense that he was simply the victim of “pop ups” which contained pornography. The *TBG* court viewed the defendant’s at-home behavior as “a significant piece of evidence,” which could only be recovered through direct access to that device. *TBG*, 96 Cal. App. 4th at 447.

To be clear, even for these direct-relationship cases, the requesting party still needs to demonstrate a default in the discovery obligations; that the requested information will be present on the device; and reasonable limitations on the search. To that end, the existence of the direct relationship principally affects the cost-benefit analysis, rather than obviating any of the other requirements.

***Other Considerations***

Because of the requisite cost-benefit analysis, the requesting party should be prepared with evidence of the expected costs to support a finding in its favor. The typical considerations—amount in controversy, increased expense, etc.—all still apply. But given that the requesting party will presumably have access to information far in excess of what is responsive, that party should provide additional evidence that its proposed search is the most cost-effective means of locating the responsive information.

To be clear, simply imaging a hard drive is much cheaper and easier than the accepted practice of negotiating search terms. And, if allowed to do so, the requesting party could develop its own search protocol to test against the data at no incremental cost to the producing party. But, as discussed, because of the privacy and confidentiality concerns inherent in the high volume of data to which the requesting party would otherwise have access, the court and the producing party will have a vested interest in ensuring that the protocol is narrowly tailored and that mechanisms are in place to protect sensitive personal information and trade secrets. As such, the requesting party should consider, and provide evidence, of multiple alternatives and why the chosen alternative is the most effective.

Further, employers should pay particularly attention to the *TBG* case which, at bottom, concerned a free-speech challenge to direct access. That court found that “employers can diminish an individual employee’s expectation of privacy by clearly stating the policy that electronic communications are to be used solely for company business, and that the company reserves the right to *monitor or access all employee Internet or e-mail usage*.” *TBG Ins. Servs. Corp.*, 96 Cal. App. 4th at 451. The court relied heavily on the plaintiff’s policy—which the defendant signed—in support of its ruling that plaintiff could access the employee’s home computer that was provided by the company. Any company that provides mixed-use electronic devices such as take-computers or cell phones should consider including such a provision in its employment agreement.

1. Jake Rutherford is an associate and T. Ray Guy is a partner, in the Litigation group in the Dallas office of Weil, Gotshal & Manges LLP. [↑](#footnote-ref-1)