BY KATHERINE V.A. SMITH AND MICHAEL HOLECEK

Guidelines for Managing a Forensic Inspection of ESI

FORENSIC INSPECTION HAS BECOME a powerful new tool in civil litigation as discovery focuses more on electronically stored information (ESI). Although forensic inspections can vary in scope and purpose, most involve the copying (or mirror imaging) of a computer hard drive and the use of software to comb through data in an attempt to identify and recover files.[1] Increasingly, forensic inspections also involve the examination of web-based e-mail and cloud storage accounts.

In the digital age, a forensic inspection is a potential game-changer in almost any litigation involving electronically stored evidence. It can uncover a "smoking-gun" document, or even evidence of spoliation, the latter of which may lead the court to issue severe—even terminating—sanctions.[2] For this reason, courts are quickly becoming more versed in (and receptive to) forensic inspections. Certain considerations and guidelines may assist in securing and managing a forensic inspection of ESI.

A forensic inspection is a potential game-changer in almost any litigation involving ESI. It can uncover a "smoking-gun" document, or even evidence of spoliation...which may lead the court to issue severe—even terminating—sanctions.

Demonstrating the Need

The first step in conducting discovery of ESI is to demonstrate the need. To secure a forensic inspection of another party's hard drives or e-mail accounts, an attorney first must be able to show the court that such an inspection is needed. Generally, courts are looking for evidence that the opposing party failed to conduct an adequate search for documents in response to discovery requests.[3] To prove the failure, counsel may consider using depositions and interrogatories to explore the scope of the other side's document searches: What hard drives, e-mail accounts, and other electronic platforms were searched? What types of files were searched? What search terms were used? Or counsel may point to discrepancies and inconsistencies in document productions, such as the production of e-mail with missing attachments or metadata. For example, in *White v. Graceland College*, the federal district court granted in part a motion for a forensic inspection after the moving party revealed inconsistencies in the creation and sent dates of certain e-mail and attachments that the opposing party was unable to explain.[4] Furthermore, counsel should examine e-mail and correspondence that include multiple senders and recipients. Did some of the senders or recipients fail to produce their copies of the same e-mail? If so, this may demonstrate that those people did not conduct adequate searches of their e-mail (or improperly destroyed evidence). In *Advante International Corp. v. Mintel Learning Technology*, for example, the district court for the Northern District of California granted a forensic inspection after the plaintiff produced "materially-different versions" of the same e-mail, indicating that the e-mail may have been "altered."[5]

In addition, evidence of spoliation—whether negligent or intentional—can also provide a compelling basis for a forensic inspection.[6] This is especially true when there is reason to believe a forensic examination may be able to resurrect deleted or corrupted files. Even if the inspection does not result in the recovery of actual documents, it may uncover additional evidence of spoliation, for example, evidence that the user downloaded and ran software designed to erase files.[7] In the same vein, courts often grant forensic inspections when a party fails to issue a litigation hold, reasoning that lack of preservation efforts increases the chance that electronic data has been deleted and can only be recovered through a forensic inspection.[8]

While it is a common misconception that courts will order a forensic inspection only when the moving party can show intentional spoliation or bad faith, courts, in fact, regularly award inspections for negligent or inconsistent document searches—or even in the absence of any discovery misconduct whatsoever. As long as the potential benefit of the forensic inspection outweighs the burden, there is an argument to be made for the inspection.[9]

Planning for an Inspection

Once an inspection has been ordered, negotiated, or authorized, the next step is to make a plan. Forensic inspections generally are conducted pursuant to a protocol that sets out the scope of the inspection (i.e., what hard drives and e-mail accounts will be searched), the methods by which the forensic examiner will conduct the inspection, and the schedule for completing the inspection. Because many courts do not have extensive experience with forensic examinations, it is advisable to include a draft forensic inspection protocol with any motion to the court. This will help the court understand exactly what is being sought. Indeed, some courts will not even consider a motion for forensic inspection without first seeing a detailed protocol.

Katherine V.A. Smith is a partner in the Los Angeles office of Gibson, Dunn & Crutcher LLP, where she practices with the firm's labor and employment and litigation departments. Michael Holecek is an associate in Gibson Dunn's Los Angeles office, where he practices in the firm's litigation and appellate and constitutional law departments.

In *Thompson v. Workmen's Circle Multicare Center*, for example, the federal district judge held that "before [the court] could determine whether to grant plaintiff access to defendant's computers, she would need to obtain an expert forensic technician and submit a specific proposal identifying the expert, describing his credentials, and setting forth the precise nature of the inspection he intended to conduct."[10]

To draft a forensic inspection protocol that both fits the client's needs and will be more amenable to a court, an attorney should review protocols that have been adopted by other courts—a judge may be more comfortable adopting a protocol that is substantially similar to those that have been approved in the past.[11] The attorney should also confirm that the protocol is workable for his or her case and the types of devices at issue, often by showing the protocol to someone experienced in this area to ensure that it doesn't specify timelines or results that are unrealistic. The attorney should also be sure the proposed protocol is broad enough to cover all anticipated needs and identifies all electronic devices, hard drives, and cloud-based storage that may yield discoverable information. For e-mail, the protocol should identify all the relevant e-mail accounts for each party-affiliated witness and specifically request that each witness disclose his or her usernames and passwords.

The attorney should consider incorporating into the protocol steps for privilege and privacy review by opposing counsel. For example, the protocol may direct the forensic examiner to first send all of the inspection results to the opposing counsel for review and redaction. Although there may be situations when this type of provision is akin to the fox guarding the hen house, in other cases, these precautionary measures will make it difficult for the other side to oppose the inspection. In *Playboy Entertainment v. Welles*, for example, the district court overruled privacy and privilege concerns, reasoning that counsel "ha[s] an opportunity to control and review all of the recovered [documents]...and produce...only those documents that are relevant, responsive, and non-privileged."[12]

The goal should be to show the court that if it grants the motion for a forensic inspection, the inspection will proceed according to an orderly and self-executing plan. This will alleviate what is likely to be one of the court's primary concerns in granting such a motion: that it will have to spend its valuable time overseeing and intervening in the inspection process.

Choosing an Examiner

A forensic examination is only as good as the examiner. Accordingly, it is critical to choose a reliable and reputable forensic examination firm. This is true not only because the forensic examiner will play a crucial role in the forensic inspection but also because he or she may submit reports to the court, or even testify at a hearing or trial, regarding the results of the forensic inspection. The court will likely give the examiner's opinion significant weight since the court appointed the examiner on the basis of his or her subject-matter expertise. In addition, when disputes arise between the parties regarding the scope of the forensic inspection (for example, whether a particular forensic test or report is called for by the protocol), the forensic examiner may end up playing the role of a de facto mediator. Indeed, some courts formally appoint the forensic examiner as an "officer of the court."[13]

Thus, the attorney should take the forensic examiner selection process seriously. Courts often ask each party to submit a list of acceptable examiners. The attorney should diligently vet each examiner's credentials and capabilities, and be sure to run conflicts checks.

An attorney seeking a forensic inspection may also wish to retain a forensics consultant to help navigate the process. This individual is someone hired and paid independently, outside of the court-approved forensic inspection. This consultant can advise the attorney as to the likelihood of recovering useful data (i.e., whether the potential benefit of the forensic inspection is worth the expenditure of time and money), assist in crafting the forensic inspection protocol submitted to the court, and review and help make sense of the results of the forensic inspection. The attorney should consider engaging the forensic consultant early in the process to garner these benefits.

Who Pays?

While some courts require the moving party to pay for the forensic inspection, other courts split the cost between both parties. Other courts require the opposing party—the party whose conduct necessitated the inspection—to pay the full cost. In *Helget v. City of Hays*, for example, the district court held that the defendant should "bear the cost of the forensic examination" because the defendant "had an obligation to preserve this information… [r]egardless of whether it was destroyed intentionally or negligently."[14]

Whether an attorney should ask the court to force the other side to pay for the inspection will depend on the circumstances of the case. Certainly, the case for such an allocation will be stronger when there has been deliberate misconduct by the opposing party. However, when there is no evidence of bad faith, a party will likely appear more reasonable—and its motion will be easier to grant—if it offers to pay for some or all of the inspection.

Some courts prefer to shift the costs of the forensic inspection down the road, depending on the results.[15] For example, a court may initially require the moving party to pay for the inspection, but then shift the costs to the opposing party if the inspection ultimately reveals discovery misconduct. Alternatively, the court may initially require the opposing party to pay for the inspection and then shift the costs to the moving party if the inspection is not fruitful (although arguably the opposing party should still pay, because its conduct compelled the inspection in the first place).

Managing Expectations

Any attorney seeking a forensic inspection must be careful to manage expectations. Before moving the court for a forensic inspection, the attorney should carefully consider the costs and the realistic benefits. What documents are likely to come out of the inspection, and is it realistic that the inspection will uncover those documents? This is something a forensics consultant can help assess. For example, is the opposing party a large corporation that maintains sophisticated backup and storage systems? Or is it an individual who recently replaced his only computer and phone? An inspection in the former case is more likely to be fruitful, but also more expensive. If the scope of the forensic inspection will include e-mail, the attorney should consider whether they are Web-based e-mail accounts (like Gmail), or server-based e-mail accounts (like Outlook). Some Web-based e-mail accounts permanently erase deleted e-mail after a relatively short period of time, such as 30 days, making recovery of deleted e-mail unlikely.[16] Managing expectations regarding the outcome of the forensic inspection is therefore critical.

With increasing frequency, litigants are using forensic inspections of their opponent's hard drives and e-mail accounts to recover key evidence not produced in the ordinary course of discovery. Knowing how to get a forensic inspection—and then how to properly manage the inspection process—can provide a potent new weapon in the civil discovery arsenal. ■

---

[1] *See generally* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 562 (Dec. 2005).

[2] *See, e.g.*, Ceglia v. Zuckerberg, 2013 U.S. Dist. LEXIS 45500 (W.D. N.Y. Mar. 26, 2013).

[3] *See* Peskoff v. Faber, 244 F.R.D. 54, 65 (D.D.C. 2007).

[4] *See* White v. Graceland Coll. Ctr. For Prof. Dev. & Lifelong Learning, Inc., 2009 WL 722056, at *7 (D. Kan. Mar. 18, 2009).

[5] *See* Advante Int'l Corp. v. Mintel Learning Tech., 2006 WL 3371576, at *1 (N.D. Cal. Nov. 21, 2006);

see also, e.g., Ameriwood Indus., Inc. v. Liberman, 2006 WL 3825291, at *4-5 (E.D. Mo. Dec. 27, 2006) (ordering a forensic inspection when the requesting party identified an e-mail that the defendant should have produced but did not); Simon Prop. Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 641 (S.D. Ind. 2000) (allowing the plaintiff to mirror image the defendant's computers when there were "troubling discrepancies with respect to defendant's document production").

[6] *See* Ellis v. Toshiba Am. Info. Sys., Inc., 218 Cal. App. 4th 853, 861 (2013) (affirming a decision to order forensic examination when, according to the trial court, a lawyer seeking attorney's fees had "exercised extremely poor judgment to wipe and delete an original file of [her] timesheets"); Preferred Care Partners Holding Corp. v. Humana, Inc., 2009 WL 982460, at *14–15 (S.D. Fla. Apr. 9, 2009); Playboy Enter. v. Welles, 60 F. Supp. 2d 1050, 1052 (S.D. Cal. Aug. 2, 1999).

[7] *See* 1-800-East W. Mortg. Co. v. Bournazian, 2010 WL 3038962 (Mass. Super. Ct. July 18, 2010).

[8] *See* Klipsch Grp., Inc. v. Big Box Store Ltd., 2014 WL 904595, at *6-7 (S.D. N.Y. Mar. 3, 2014) ("authoriz[ing] plaintiff to undertake a forensic investigation into the state of defendants' computer systems" in part due to "defendants' failure to issue a timely or adequate [litigation] hold"); Ferron v. Search Cactus, L.L.C., 2008 WL 1902499, at *2-3 (S.D. Ohio April 28, 2008).

[9] *See* A.M. Castle & Co v. Byrne, 123 F. Supp. 3d 895, 899 (S.D. Tex. 2015); Brady v. Grendene USA, Inc., 2015 WL 4523220, at *9 (S.D. Cal. July 24, 2015) (denying a motion to compel forensic examination because the moving party was unable to establish that "such an examination is likely to yield emails that have been deleted or purged").

[10] *See* Thompson v. Workmen's Circle Multicare Ctr., 2015 U.S. Dist. LEXIS 74528, *5 (S.D. N.Y. June 9, 2015) (finding that the "plaintiff has not met the threshhold requirements for forensic examination of defendant's computers or other equipment because it is not clear that she has selected an expert, and she has not specified what tests her expert would perform").

[11] *See, e.g.,* Campbell All. Grp., Inc. v. Dandekar, 2014 WL 145037, at *3 (E.D. N.C. Jan. 13, 2014); Ameriwood, 2006 WL 3825291, at *6.

[12] *See* Playboy Enter. v. Welles, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. Aug. 2, 1999).

[13] *See id.*; Dodge, Warren & Peters Ins. Servs., Inc. v. Riley, 105 Cal. App. 4th 1414, 1421 (2003) (affirming an injunction that "require[d] the preservation of electronic evidence by prohibiting Defendants from destroying, deleting or secreting from discovery any of their electronic storage media and…allow[ing] a court-appointed expert to copy all of it, including computer hard drives and discs, to recover lost or deleted files").

[14] *See* Helget v. City of Hays, 2014 WL 1308893, at *6 (D. Kan. Mar. 31, 2014); *see also, e.g.,* Peter Kiewit Sons, Inc. v. Wall St. Equity Grp., Inc., 2012 WL 1852048, at *20 (D. Neb. May 18, 2012) (the producing party should pay for the forensic examination when it failed to conduct a good faith search for ESI); Peskoff v. Faber, 251 F.R.D. 59, 62-63 (D. D.C. 2008).

[15] *See, e.g.*, Fidelity Nat'l Title Ins. Co. v. Captiva Lake Invs., LLC, 2015 U.S. Dist. LEXIS 1350, *21 (E.D. Mo. Jan. 7, 2015).

[16] *See, e.g.*, https://support.google.com/a/answer/151128?hl=en (Google's e-mail retention policy); *see also* Brady v. Grendene USA Inc., 2015 U.S. Dist. LEXIS 97734, *26-27 (S.D. Cal. July 24, 2015) (denying a forensic inspection request in part because "[t]he defendants have not established through declaration or exhibit…that such an examination is likely to yield emails that have been deleted or purged").