# e-Discovery and Trade Secrets Law: Limitations on Discovery

## By Scott A. Carlson and Patrick E. Zeller

Discovery requests can often seem to border on being overly intrusive and to go beyond the scope of the dispute. That intrusiveness, however, reaches a higher level when an opponent seeks to obtain information that may include trade secrets, proprietary content, or other sensitive information. Intrusiveness can peak when a party seeks discovery through the use of an inspection of another party's computer system, often through a request for a forensic image of a hard drive. In the trade secrets litigation context, this presents an extraordinary challenge. On one hand, the party requesting the inspection is often looking for its own trade secrets and related evidence located on its opponent's computers. But inevitably the opponent will say, "Wait a minute: *our* trade secrets are on there," and it will not want the computers inspected. Such is the tension faced when e-discovery law meets trade secrets law.

### Forensic Inspections

Requests for inspections of computer systems or electronically stored information (ESI) arise in many ways. Some inspections simply seek access to a system to perform general searches for files. Others may be more intrusive and may request a forensic copy of a laptop hard drive or server. These forensic copies are typically a complete copy of the entire hard drive and are known by many names including mirror images, forensic images, complete images, bit-stream images, or bit-stream copies. All of these forensic copies cover the entire contents of the hard drive, including, generally: (1) the files created by a user (word processing files, e-mail, spreadsheets, etc.); (2) files that run the various applications, programs, and operating system on the computer, including log files, Internet history, etc.; and (3) information related to files that have been "deleted," including the potential recovery of partial or complete copies of deleted files.

These "deleted" files exist because of the manner in which computer operating systems store files. When files are deleted by a user, they are not removed from the hard drive; instead, the operating system simply no longer keeps track of them. Over time, these deleted files may be overwritten completely or in part because of the addition of new files and continued use of the computer involved. Often these "deleted" files are of interest in trade secrets and other types of litigation, and these files can only be obtained through a computer forensic examination.

#### *Before the 2006 Amendments to the Federal Rules of Civil Procedure*

Traditionally, most litigators thought of Rule 34 inspections as mechanisms to inspect property—to perhaps photograph or take measurements at the site of an accident, for example. Alternatively, an inspection request might be used to allow an expert to inspect a vehicle involved in an accident. In the earliest days of Rule 34, few would have contemplated "inspecting a computer hard drive." That being said, Rule 34 has long provided a mechanism for a party to obtain an inspection of certain items, including "data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form. . . ."[1]

Prior to the 2006 amendments to the Federal Rules of Civil Procedure, courts struggled with how to handle Rule 34 requests when it came to computer hard drives. When faced with Rule 34 inspections, a computer hard drive was typically viewed in one of two ways: (1) as simply a "tangible thing" and it was, therefore, subject to inspection under the plain language of the rule, or (2) it was the functional equivalent of a filing cabinet and should only be subject to inspection in limited circumstances.

For example, in *Advante Int'l Corp. v. Mintel Learning Tech.*,[2] the defendant Mintel accused the plaintiff Advante of withholding, concealing, or destroying evidence and filed a motion to compel for authorization to examine Advante's computer systems. The court began by noting that "electronic storage of information presents discovery issues not encountered in earlier times" but noted that it is well settled that "electronic evidence is no less discoverable than paper evidence."[3] The court acknowledged that inspection of hard drives may be appropriate in some cases but denied defendant Mintel's motion to compel.

> The mere fact that this case involves electronic data does not change the basic concepts or rules of the discovery process. Had Mintel made the same basic accusations in an earlier age, its claims of incomplete document production, inconsistencies, or even perjuring destruction of evidence, would not automatically entitle it to an order permitting it to enter Advante's offices to rummage through filing cabinets and desks. The relief Mintel is asking for here is no different and not more warranted.[4]

Also, defendant Mintel had not presented any concrete evidence of its allegations of discovery misconduct. Thus, the court denied the motion to compel.[5]

#### *After the 2006 Amendments to the Federal Rules of Civil Procedure*

As part of the 2006 Amendments to the Federal Rules of Civil Procedure (the so-called e-discovery amendments), the Advisory Committee noted the inherent tensions associated with the inspection of hard drives containing ESI. Specifically, the Advisory Committee noted that

> [i]nspection or testing of certain types of electronically stored information of a responding party's electronic information system may raise issues of confidentiality or privacy. 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*, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from the inspection or testing such system.[6]

Essentially, one cannot substitute a request for documents with a request for an inspection that would allow a party to send in an expert to routinely perform its own searches for documents. Put another way, courts should proceed with caution when considering providing a party with a right to the electronic equivalent of rifling through its opponent's office file cabinets—which is often the electronic equivalent of rooms full of file cabinets that contain both relevant and irrelevant information.

That being said, trade secrets cases are among those that often *do* require an inspection of a hard drive. The reason is that often it is not just the particular word processing document or e-mail that is important to a trade secrets case. Instead, trade secrets cases typically are won or lost on evidence about "how" a particular computer was used, not "what" documents are on it. For example, a forensic inspection may produce evidence that a CD had been burned on a particular day and that system logs show files containing trade secrets were copied onto a CD and deleted from the original laptop. Or it may show that an employee, just prior to quitting to join a competitor, utilized his company laptop to upload his former employer's proprietary information onto a thumb drive, USB drive, or another computer network. In other cases the inspection may show that sensitive information was copied from company servers to a company laptop but then quickly deleted to give the appearance the files were never downloaded and never existed on the laptop. All of these types of evidence, as well a plethora of other kinds of evidence, can be obtained through a forensic examination of an opponent's computer hard drive and may be the most critical evidence in a case.

## Limiting Discovery and Protecting Trade Secrets and Other Information During Inspections

Courts and parties are continually seeking to strike a balance between the need for discovery of ESI and the need to protect against unnecessary access to irrelevant but often proprietary and sensitive information, including trade secrets. As the type of information and the technology involved change from case to case, so must the balance of discovery and protection change. Focusing only on technology, the balance struck in allowing access to a single workstation may change when that workstation is connected to a large network. Concerns associated with the inspection of a single hard drive may be dramatically different than those associated with the inspection of a server. Additional issues may arise when a party wants to look at a hard drive that is also the entry point for a person to utilize social networking sites, personal e-mail, or information contained in "the cloud" of remote computer systems.[7]

Regardless of the technologies or the requests, courts and parties are often dissatisfied with a simple granting or denying of a particular request. Instead, a proper balancing of interests often leads to defined limitations on an inspection request. None of the limitations identified below are perfect solutions, and each must be considered based upon the facts in any particular case. These limitations hopefully do, however, provide a starting point for crafting the appropriate limitations for any particular matter given both the technology at issue and the information sought.

### *Protective Orders*

Perhaps the simplest, and also perhaps the most dissatisfying, limitation on an inspection is the protective order. Parties can simply be told, "Don't worry; we'll enter a protective order and then whatever the inspector finds will be protected." While protective orders are common and sometimes are effective, they are inherently limited because of their focus on what one "does" with the information found, as opposed to "access" to the information in the first place. But courts are highly motivated to move in this direction—the idea of a protective order is simple and judges understand them. And in many cases, there is no way to place limitations on the scope of an inspection: all you can do is put in place a protective order.

### *Independent Experts*

Some courts have sought to limit inspections through the use of an independent expert. The precise application of this approach can and has varied widely in different cases, but it has certain common elements. First, it contemplates an expert who is engaged by and reports to the court, as opposed to the parties. Second, it necessarily requires a fairly precise notion of what the expert will be searching for. Third, it requires a considerable amount of the court's time and attention in managing the inspection and sometimes even involves the review of material and providing the results to the parties; these factors can cause courts to contemplate the appointment of a special master. The demands associated with the use of an independent expert are not often easily met or recognized at the time the independent expert is appointed.

Probably the most cited case supporting the use of a court-appointed forensic expert is *Playboy Enterprises, Inc. v. Welles*.[8] In that case, the court accepted the notion that e-mail messages might be able to be recovered through the inspection of a forensic image of the defendant's computer.[9] The court's order indicated that it would appoint an expert, that the expert would sign a protective order, and that any disclosure as a result of reviewing the information on the hard drive would not waive the attorney-client privilege if that privilege applied to the disclosed

**Scott A. Carlson** is the founder and chair of Seyfarth Shaw's national e-discovery practice group. Mr. Carlson advises clients on a broad array of e-discovery and related issues, utilizing his experience as a litigator along with his technical background, which includes a B.S. in Computer Science and Mathematics. He can be reached at scarlson@seyfarth.com. **Patrick E. Zeller** is vice president and deputy general counsel for Guidance Software, Inc. He writes and speaks regularly on topics related to e-discovery, digital evidence, and the intersection of law and technology. He can be reached at patrick.zeller@guidancesoftware.com. Mr. Carlson and Mr. Zeller are both adjunct professors at The John Marshall Law School, where they teach a course entitled E-Discovery, Computer Forensics, and Digital Evidence.

material.[10] The expert would image the hard drive and search for e-mails that could be recovered, which would then be provided to defendant's counsel to review for further production.[11]

### *Limiting Inspection*

Another method courts and parties have used to constrain access to electronic records is to attempt to "limit" or "define" the scope of an inspection. In some cases, a requesting party has been required to revise its request to specify a narrower and less intrusive request. Under pressure from a court, a litigant can sometimes fashion a particular search protocol that truly focuses on the relevant information.

For example, in *MSC Software Corp. v. Altair Engineering, Inc.*,[12] plaintiff MSC asked an individual defendant to produce "all hard drives, thumb drives, or USB drives from any and all personal (non-Altair) computers for inspection and imaging."[13] Notwithstanding the broad request, what MSC was actually seeking was the contents of a specific folder from the defendant's computers that might have been contained on these hard drives, thumb drives, or USB devices.[14] The individual defendant provided MSC the contents of the folder but would not give MSC access to the drive itself because it contained confidential information.[15] The court found that forensic imaging was inappropriate due to the sensitive nature of the case and MSC's overly broad discovery request.[16] The court did allow, however, a limited inspection in which defendant Altair's expert was to examine the hard drive for the folder itself and then provide the results designated as "Attorney's Eyes Only."[17]

Yet another example arose in *Sterle v. Elizabeth Arden, Inc.*[18] In that case, plaintiff Sterle sued defendant Arden alleging wrongful termination in violation of the Age Discrimination in Employment Act of 1967 (ADEA).[19] Plaintiff sought production of certain employee ranking reports that counsel for Arden had claimed could not be located.[20] In light of the failure to locate the records, the court issued an inspection order for a forensic computer consultant to inspect the defendant's computers.[21] The parties disagreed over how the consultant was to conduct the inspection and, when the consultant arrived to conduct the inspection, he was denied access to many areas of the computer system.[22] Counsel for Arden then filed a motion for a protective order to prevent the inspection of the defendant's computer system based largely on a theory that the plaintiff's attorney's instructions to the consultant threatened Arden's private or privileged information.[23] The court rejected this argument and found that Arden had not established good cause for a protective order, as the inspection order was drafted so that relevant information could be found and content and time limits were imposed to limit the inspection to searches for the missing reports and only for the year prior to the plaintiff's termination.[24]

### *Defined Court-Ordered Searches*

If there are limits that can be imposed to properly balance the interests of the parties, it is important to make clear what the protocol is that will be used. In some instances, an appropriate balance might lead to a court ordering a party to conduct a particular search of its own computers and to provide the search results to its opponent. This approach has some appeal in cases where the disclosure of the underlying information is particularly problematic and the material sought can be clearly identified.

For example, in *Daimler Truck North America, LLC v. Younessi*,[25] plaintiff Daimler sued a former executive for breach of the duty of loyalty, breach of a confidentiality contract, and common law duty not to convert confidential and proprietary information. Daimler had requested to search Cascadia's computers for communications between Younessi (defendant and former employee) and Hebe (former CEO of both Daimler and Cascadia).[26] Cascadia asserted that the subpoena calling for this search was unduly burdensome and would require disclosing trade secrets to a competitor.[27] Upon balancing Cascadia's interest in maintaining its trade secrets against Daimler's interest in prosecuting its case, the court determined that discovery was warranted and denied Cascadia's motion to quash in part.[28] The court looked to *Playboy Enterprises, Inc. v. Welles*[29] for guidance on how to handle the search and protect Cascadia's trade secrets. The court ordered Cascadia to search its *own* computers, rather than to produce them for copying, because Daimler was a direct competitor and Cascadia was a third party to the suit.[30]

### *Special Considerations for Subpoenas*

As noted in the *Daimler* case above, inspections for ESI can be obtained through the use of a Rule 45 subpoena. However, as with any subpoena, in addition to the general tension associated with inspections, inspections of nonparties should raise heightened concerns for the burdens placed on the nonparties. The 2006 Advisory Committee Notes to Rule 45 provide as follows:

> Rule 45(a)(1)(B) is also amended, as is Rule 34(a), to provide that a subpoena is available to permit testing and sampling as well as inspection and copying. As in Rule 34, this change recognizes that on occasion the opportunity to perform testing or sampling may be important, both for documents and for electronically stored information. Because testing or sampling may present particular issues of burden or intrusion for the person served with the subpoena, however, the protective provisions of Rule 45(c) should be enforced with vigilance when such demands are made. Inspection or testing of certain types of electronically stored information or of a person's electronic information system may raise issues of confidentiality or privacy. The addition of sampling and testing to Rule 45(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a person's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.[31]

In *Integrated Service Solutions, Inc. v. Rodman*,[32] plaintiff Integrated Service Solutions, Inc. (ISS) served nonparty VWR with a subpoena that included all VWR computers. In particular, ISS sought a VWR laptop that was assigned to defendant Dennis Rodman's wife while she worked for VWR and that Dennis Rodman used during the time.[33] VWR, one of ISS's competitors, voiced concerns over giving ISS "direct access" to its IT system, and over the subpoena's reach into VWR's confidential information.[34] Accordingly, VWR offered to conduct the search itself or have a third-party

expert perform the search, and the parties agreed to have PricewaterhouseCoopers (PWC) conduct the search.[35] PWC performed the analysis based on an ISS "checklist" and billed ISS.[36] PWC submitted the search hits to VWR counsel, who concluded they were not relevant to the litigation.[37] VWR counsel informed ISS that the analysis was complete and that (1) there was no evidence of wiping on the drive, (2) most of the search terms did not result in hits, and (3) none of the hits were relevant to the litigation.[38]

As a result of what was apparently a sufficiently vague protocol, ISS then sought an order compelling VWR to produce a full report from PWC and provide direct access to the files identified in the search.[39] Ultimately, the court concluded the parties had not agreed that ISS would obtain the files regardless of relevance and found nothing to indicate bad faith or unreliability on VWR's part or to suggest that VWR was withholding relevant evidence.[40] Thus, the court denied ISS access to the files, stating, "[w]e will not require this nonparty, VWR, to permit ISS to thumb through an electronic file drawer to double-check VWR's document review on this point."[41] But the court did allow ISS to seek, through VWR, a report of the search from PWC "to confirm the search terms were applied properly."[42]

In *Gonzales v. Google, Inc.*,[43] a civil action had been filed against the U.S. attorney general challenging the constitutionality of the Child Online Protection Act. Thereafter the attorney general subpoenaed Google seeking all the URLs in its database and then, in a later version of the subpoena, just a sampling of the URLs.[44] The subpoena also initially sought all search queries entered on the search engine for 60 days, but it was later narrowed to a one-week period. The purpose of the subpoena was to collect information for a study on the effectiveness of filtering and blocking software.[45] Among other concerns, Google objected that trade secrets would be disclosed. The court acknowledged that a statistically significant sample from Google's index "may permit competitors to estimate information about Google's indexing methods or Google's users."[46] The court determined that the government demonstrated a substantial need for the information from Google based on its market share but not for disclosure of both the URLs and search queries. Thus the court granted a motion to compel only as to the 50,000 URLs and issued a protective order for the information submitted by Google.[47]

## Conclusion

Inspection of computer systems and electronically stored information is an important part of the civil discovery process. While the balancing of interests between the right to relevant information and the risk of disclosure of sensitive nonrelevant information is complex, the courts have sufficient flexibility to balance those interests. The difficulties lie in clearly identifying the information sought and understanding the technology involved to fashion appropriate limitations on discovery steps. Courts have limited time and resources, and parties will proceed optimally if they effectively define appropriate discovery limitations and, perhaps more importantly, clearly explain the material discovery and trade secret issues to courts overseeing discovery processes. ■

## Endnotes

1. Fed. R. Civ. P. 34.
2. 2006 WL 1806151 (N.D. Cal. June 29, 2006).
3. *Id.* at 1.
4. *Id.*
5. Later, after Mintel presented evidence that some e-mails had been tampered with, the court granted Mintel's motion to examine Advante's systems, provided the parties agreed on a protocol for producing and disclosing any resulting information. Advante Int'l Corp. v. Mintel Learning Tech., 2006 WL 3371576 (N.D. Cal. Nov. 21, 2006).
6. Fed. R. Civ. P. 34, Advisory Comm. Notes.
7. Defining "the cloud" is well outside the scope of this article and would take a book to explain. However, in the broadest terms "the cloud" refers to a shift in the concept of computer storage from local controlled servers to storage places on the Internet ("in the cloud") that are accessed through a web browser with the user not knowing precisely where his or her data are stored.
8. 60 F. Supp. 2d 1050 (S.D. Cal. 1999).
9. *Id.* at 1054.
10. *Id.* at 1055.
11. *Id.*
12. 2008 U.S. Dist. Lexis 105570 (E.D. Mich. Dec. 22, 2008).
13. *Id.* at 21.
14. *Id.* at 21–22.
15. *Id.* at 22.
16. *Id.*
17. *Id.*
18. 2008 WL 961216 (D. Conn. Apr. 9, 2008).
19. *Id.* at 1.
20. *Id.*
21. *Id.*
22. *Id.* at 3.
23. *Id.* at 6.
24. *Id.*
25. 2008 WL 2519845 (W.D. Wash. June 20, 2008).
26. *Id.* at 1.
27. *Id.*
28. *Id.* at 2.
29. 60 F. Supp. 2d 1050 (S.D. Cal. 1999).
30. *Younessi*, 2008 WL 2519845, at 4.
31. Fed. R. Civ. P. 45, cmt. (2006).
32. 2008 WL 4791654 (E.D. Pa. Nov. 3, 2008).
33. *Id.* at 2.
34. *Id.*
35. *Id.*
36. *Id.*
37. *Id.* at 3.
38. *Id.*
39. *Id.*
40. *Id.*
41. *Id.* at 4.
42. *Id.*
43. 234 F.R.D. 674 (N.D. Cal. 2006).
44. *Id.* at 678.
45. *Id.* at 679.
46. *Id.* at 684.
47. *Id.* at 686–87.