Four Keys to Litigating a Modern Trade Secret Case

DAVID A. PEREZ AND HEATH L. HYATT

David A. Perez is chair of the Business Litigation group and cochair of Real Estate Litigation, and Heath L. Hyatt is an associate in the Business Litigation group, at Perkins Coie LLP, Seattle.

It happens more often than we think. An employee connects an external storage device to a company computer or server and starts downloading thousands of sensitive business documents. Then the employee, whether disgruntled, headed to a competitor, or both, pockets the storage device and walks out the door. Eventually, the company learns, or suspects, what the employee has done and calls you to contain the damage. It's a classic trade secret misappropriation case.

Four critical, and recurring, considerations should be kept in mind in a modern trade secret case. First, retain an expert to get a handle on the computer forensic evidence as soon as possible. Don't let the other side know more about the file transfers than you do. Second, don't assume evidence will be preserved—the folks copying or moving files often try to cover their tracks through deletions. That can cut both ways. Third, never underestimate the importance of early equitable relief for a plaintiff or avoiding such relief if you are defending. A restraining order can hobble a defendant early and color the rest of the litigation, but the request also provides a defendant the opportunity to cast doubt on an overreaching plaintiff's case—so tread carefully. And, fourth, define the trade secrets early. An inability (or unwillingness) to articulate one's trade secrets will damage the plaintiff's credibility, and for a defendant, it is critical to understand the plaintiff's trade secrets to narrow discovery.

Computer Forensics

Part of the inhumanity of the computer is that . . . it is completely honest.

—Isaac Asimov

Modern trade secret cases are often won (or lost) on computer forensic evidence. Gone are the days of employees sneaking photocopied documents out of the office in a briefcase. Today, there are seemingly endless ways to transfer files from a company computer with just a few clicks. But these clicks leave behind many clues that plaintiffs and defendants can use to their advantage. Uncovering and understanding these clues take time (and money), but it is often worth the significant investment.

Knowing the computer forensic evidence inside and out will help build your case narrative, provide opportunities to bolster your witnesses' credibility (not to mention your own), discredit other witnesses, avoid surprise evidence or a counter-narrative that you weren't aware of, and may tip you off to spoliation. Dig in. Learn the whole story. It's worth it.

Plaintiffs can unearth clues from questions such as these: Did the employee plug that external storage device into any other computers? If so, which ones? When? What else was the employee doing while it was plugged in? Did the employee recently

Published in *Litigation,* Volume 49, Number 1, Fall 2022.

install some kind of file-transfer program on the company computer? Did the employee have the company's business plans open on a personal computer as the employee created his own "new" plans? Did the employee search online for "how to wipe an external storage device" to cover his tracks? Has the employee even been "working" recently? Or was the employee quietly reviewing which documents to steal?

Defendants, meanwhile, can uncover clues that could support their defense or provide an innocent explanation from questions such as these: Does the employee often work at 3 a.m.? Maybe an otherwise suspicious file transfer is routine. Does the employee regularly work from home? Sure, taking confidential files home might be a violation of company policy, but that might not make the file transfer nefarious. Has the employee copied a large number of files before for some work purpose?

Whether you are prosecuting or defending a trade secret case, invest in a solid computer forensic expert, even if you aren't sure what you are going to find. Your expert can show you the well of available clues, explain whether those clues are reliable, and filter out any forensic "noise." But this well of clues can be both deep and wide. Get creative with the computer forensic evidence, think outside the box. What kind of story can you tell?

To truly learn the computer forensics (and uncover all the relevant clues that you might need for your case), the computer forensic investigation must be a collaborative one. Although you are not an expert in computer forensics, you are an expert in the facts of your case. You never know how some forensic clue may make or break your case. The clues might not seem relevant until after you've conducted more discovery. By the time the investigation is finished, your computer forensic expert should be high up on your speed dial.

Knowing the forensic evidence inside and out will also ensure you aren't surprised, in a motion, at a deposition, or at trial, by evidence (or a counter-narrative) that you were not aware of. Nothing hurts a witness's or an attorney's credibility more than going out on a limb on a seemingly straightforward factual assertion, only to have that limb cut down with objective forensic evidence. Check the computer forensics against witness testimony. For example, if the employee testifies under oath that she regularly works from home to explain away the mass copy to an external storage device, then look at a list of all the documents opened on the employee's personal computer in the last year (your computer forensic expert can generate this list for you) to discover how many are work-related. Even uncovering a small lie can have an outsized impact on the witness's credibility.

Finally, a full examination of the forensic evidence also will tip you off to any spoliation. Spoliation is common in modern trade secret cases. It seems so easy to "delete" electronic evidence without anyone knowing. Most of us have no idea how many clues we leave behind on our computers and how long those clues survive. Even if the defendant wiped the external storage device clean of all forensic clues, a computer forensic expert can still look at the computers and tell you if and when each device was last plugged in, maybe more. While the external storage device might be "clean," evidence of the misappropriation may remain.

Once you have fully developed the forensic evidence, think through how and when to use the evidence you've uncovered for maximum effect. Of course, both sides want to put forward their best evidence and tell a compelling story. But you may choose to spring a fact in a deposition to catch the deponent off guard with computer forensic evidence the witness wasn't prepared for. Or you may decide to lead a hostile witness down a certain path at trial, locking the witness into her story, and then spring your trap. However you decide to use these forensic clues, you need to know about them first.

Evidence Preservation

More than once, I've wished my life had a delete key.

—Harlan Coben

It is very tempting and quite easy for a defendant to delete evidence of misappropriation. A defendant can do this in all sorts of ways. External storage devices are easy to wipe and even easier to "lose." A defendant can change file names to conceal their nature or alter metadata to make the files appear irrelevant. But evidence loss can be innocent too. External storage devices can be tiny—easily disappearing at the bottom of a briefcase, getting tossed in a drawer, or just simply going missing. Many computer forensic clues overwrite themselves or are replaced with new data. Never assume that evidence has been or ever was preserved. The longer you wait to preserve the evidence, the more likely it is that the evidence is lost, one way or another. The consequences for either party can be devastating.

Plaintiffs must ensure preservation of everything from the moment the problem is identified. This includes not only their own evidence but, most importantly, the defendant's evidence. Even if the plaintiff hasn't filed a lawsuit yet, consider a written instruction to the soon-to-be defendant to preserve everything. This should be part of the first communication with the defendant. If nothing else, this instruction provides a clear line for what would constitute spoliation, should something nefarious happen after that instruction. Don't wait until formal discovery to request files or data from the defendant's electronics. Instruct the defendant to preserve everything immediately. Again, it's not just the devices or computers that the company knows or suspects were directly involved in the misappropriation that you need to worry about. Did the defendant plug the storage device containing company files into another computer? Preserve that other computer. Did the defendant share any files with third

parties? Preserve evidence of that transfer too. Did the defendant text anyone about the misappropriation? Preserve those text messages. Did the defendant search for file-transfer software or how to conceal a file transfer? Preserve that web search history.

As to its own evidence, a company should immediately review all the devices given to the employee and identify any software that could evidence misappropriation. Preserve that too. The best way for the plaintiff to ensure everything is preserved is to image everything on all of the potentially relevant electronics as soon as possible through a neutral forensic expert.

Defendants, on the other hand, should focus on preserving their own evidence immediately, even if the plaintiff hasn't said anything. It's much less likely that the plaintiff will lose evidence. Defendants want to avoid spoliation remedies or dings to their credibility for failing to preserve evidence. And never, ever instruct your client to just delete misappropriated files.

Spoliation sanctions can be damning and hobble the spoliating party, particularly if they lead to an adverse instruction. But even if there are no formal sanctions, missing evidence hurts a client's credibility. Deleting evidence is never worth it. Even "innocent" losses can be devastating. For example, if two friendly employees were texting around the time that they both improperly downloaded the company's files, but they both deleted those texts, a fair inference would be that the two employees were discussing or coordinating their misappropriation efforts. But maybe they were just complaining about the company and didn't want the company to see those text messages. That's the problem with spoliation: The evidence is gone.

If you learn about your client's spoliation or other loss, strongly consider disclosing that information, with your client's consent, to opposing counsel and the judge. Proactive disclosure of evidence losses has many benefits. It can help mitigate any damage to your client's credibility (and yours), and it lets you control the narrative and the context. How did it happen? What have you done to recover or replicate the missing evidence? That's a much better position than responding to the other side's disclosure of deletions that you tried to hide. It's simply not worth it for a party to gamble on whether the other side will discover the deletions (forensic experts are really good at finding these things out).

The best way to avoid spoliation and missing evidence is to instruct your client immediately on the importance of preserving everything. Often the storage devices or other electronics used in misappropriation cases are mixed-use devices—personal devices with company information on them. Don't let your client fail to preserve those just because it is your client's devices, not the company's device. Some of these mixed-use devices may be everyday devices such as personal computers and even personal phones. If it's related to the company, the trade secret, or the case, preserve it. If personal or external storage devices are involved, have your client immediately bring everything the client can find to your office for safekeeping and forensic imaging. Instruct your client not to plug in anything, to just hand the devices over to you. If a defendant plugs in a device that contains trade secrets or misappropriated files, even if it is just to see what is on that device, it plants a devastating forensic clue.

Early Injunctive Relief

Do not wait to strike till the iron is hot; but make it hot by striking.
—William Butler Yeats

Every plaintiff in a trade secret case must decide whether and when to seek an injunction. Obviously, if the plaintiff believes the defendant is misappropriating trade secrets—after all, that's why the lawsuit was filed—then the next question is whether the evidence is clear enough, and the harm of misappropriation bad enough, to justify immediate injunctive relief. Such an order could prevent irreparable harm, such as a disclosure of the plaintiff's trade secrets to a close competitor.

Evidence preservation is another reason to seek a restraining order. If the defendant is actively deleting or destroying evidence, a restraining order is often necessary to stop those deletions. An injunction focused on evidence preservation is often accompanied by expedited discovery focused on preservation and spoliation. For instance, the defendant may be deposed early—often without prejudice to depose the witness again—to answer questions about what happened with the allegedly misappropriated files and what evidence has been destroyed and by whom. These early depositions can be incredibly useful in getting the "unvarnished facts" before the defendant's attorney has had a chance to develop and rehearse case themes.

Early spoliation depositions present several other advantages. For example, they can lock defendants into answers that may later prove problematic or contradictory. Because these depositions likely would occur before document discovery, the plaintiff will have an opportunity to corroborate or contradict the testimony from the spoliation deposition and re-raise the issue at the defendant's regular deposition. Perhaps most important of all, these early depositions can help build a case for spoliation sanctions.

Early injunctive relief is a high-risk/high-reward endeavor. The potential upside for the plaintiff can be tremendous: Having marshaled the damning evidence necessary to craft a compelling complaint, and getting that story (and evidence) in front of a judge early can color the case from the beginning. If the evidence is strong enough, the plaintiff should file its request for a temporary restraining order at the same time it files the complaint.

Temporary restraining orders are, by their nature, expedited affairs. A defendant often can't marshal the same evidentiary precision that the plaintiff can—because the plaintiff has been

working with a forensic expert for days or weeks, while the defendant may still be looking for the right counsel. That's why the time between the filing of the plaintiff's motion for a temporary restraining order and the court hearing a few days later is often the most vulnerable moment in a defendant's case.

The downsides for a defendant can be devastating. An early order can hobble a corporate defendant's ability to bring on a new executive, force the disclosure of reams of information on an expedited basis, and cause significant harm to the defense's credibility. Simply put, if the plaintiff presents compelling forensic evidence sufficient to get an early injunction, the judge is already convinced that trade secrets were misappropriated or that evidence has been destroyed, or both. Any such order casts a pall over the defense from that point forward.

Seeking early equitable relief does not come without risks to the plaintiff; on the contrary, an early hearing presents the defense with a great opportunity to push back against an overzealous plaintiff's counsel. All too often, plaintiffs rush into court, pounding the table for an injunction, only for the defendant to poke hole after hole in the plaintiff's allegations.

Credibility is easily spent and notoriously hard to earn. The best way for a defendant to damage the plaintiff's credibility and scuttle the case before it gets off the ground is to successfully oppose a premature request for a temporary restraining order. This is especially true if the plaintiff overstates the case and the facts to the judge. Overstating a case provides an excellent opportunity for the defendant to cast doubt on the plaintiff's motives, the plaintiff's credibility, and the merits of the entire case.

Define Trade Secrets Early

Great stories happen to those who can tell them.

—Ira Glass

It is easy to get lost in the excitement of the misappropriation part of the case and to take proving your trade secrets for granted. To prove protectable trade secrets, the plaintiff (and you) will need to explain those trade secrets to the judge, jury, and even the defendant. Trade secrets are often inherently complicated or challenging for a layperson to understand. If you can't understand your client's trade secrets or if client witnesses are unable to explain them, you have a big problem.

Start working with your client immediately to educate yourself on the trade secrets, but also prepare the client to explain the trade secrets to the judge or fact finder in an easily digestible way. This may mean crafting one or a series of analogies, retaining an outside expert, creating graphics, or something else. It takes longer than you think to prepare to explain your trade secrets. If the defendant is smart, you will need to define them very early in your case.

Defendants should consider asking plaintiffs through one or more interrogatories to define the trade secrets at issue as early as possible in the case, preferably as part of initial interrogatories. Do not settle for boilerplate objections about the request being premature. It's not. An early definition will narrow discovery to only those trade secrets allegedly misappropriated, even if the defendant was aware of other trade secrets. If you receive anything but full answers, press the plaintiff on this right away, and consider moving to compel as soon as possible. You are entitled to know what the trade secrets are that your client is accused of misappropriating. Nothing hurts the plaintiff's credibility more than an inability (or unwillingness) to specifically identify the trade secret at the heart of the case. Pressing this issue early may catch a plaintiff flat-footed and give a defendant a rare opportunity to control the pace of the litigation.

But defendants must be wary here too. It is an easy trap for a defendant to demand too much specificity from the plaintiff, more than courts require, and refuse to produce any information until satisfied with the plaintiff's response. Be reasonable. Don't risk the plaintiff turning the tables back on you and running to the court for relief. Keep your credibility intact. Sometimes there is value in defending against a vague or murky identification of a trade secret. Plaintiffs, not defendants, have the burden of proving what they claim is a trade secret. So, if you don't understand the plaintiff's claimed trade secret, there is a good chance the fact finder won't either.

Once the plaintiff defines the trade secrets, you'll need plenty of time to thoroughly discuss the purported trade secrets with your client, mount your defense, and prepare for an effective Rule 30(b)(6) deposition. Save time in that 30(b)(6) deposition to clarify any questions about or ambiguities in the claimed trade secrets, and try to narrow the scope of the trade secrets as much as possible. The clearer and more defined the trade secret, the better your chances of defending the case (and the more limited any possible injunction against your client will be). The plaintiff will likely supplement once or twice throughout discovery. That's fine. Reopen the 30(b)(6) deposition, if needed. But insisting that the plaintiff define the trade secrets at issue early will give you the vast majority of what you need to mount a defense.

The challenges to defining or talking about trade secrets aren't limited to plaintiffs. Defendants will want to show why something is not a trade secret. Is the information publicly available? Is the defendant's work different from what the plaintiff is claiming as a trade secret? Is the trade secret valuable?

As you prepare for and litigate your next trade secret case, remember these four key considerations that apply regardless of which side of the case you are representing: know the forensic evidence inside and out; make sure to preserve everything; never underestimate the power of early equitable relief; and define the trade secrets at issue early. ■