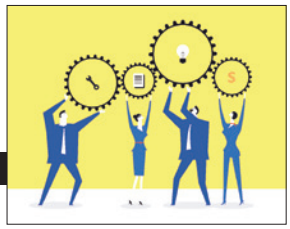
DAILY REPORT
A SMART READ FOR SMART READERS
An ALM Publication

PRACTICE FOCUS: E-DISCOVERY

IN-HOUSE GEORGIA
THE NEWS RESOURCE FOR EXECUTIVE LAWYERS



Top Five Tips for Using Forensics to Win the Case

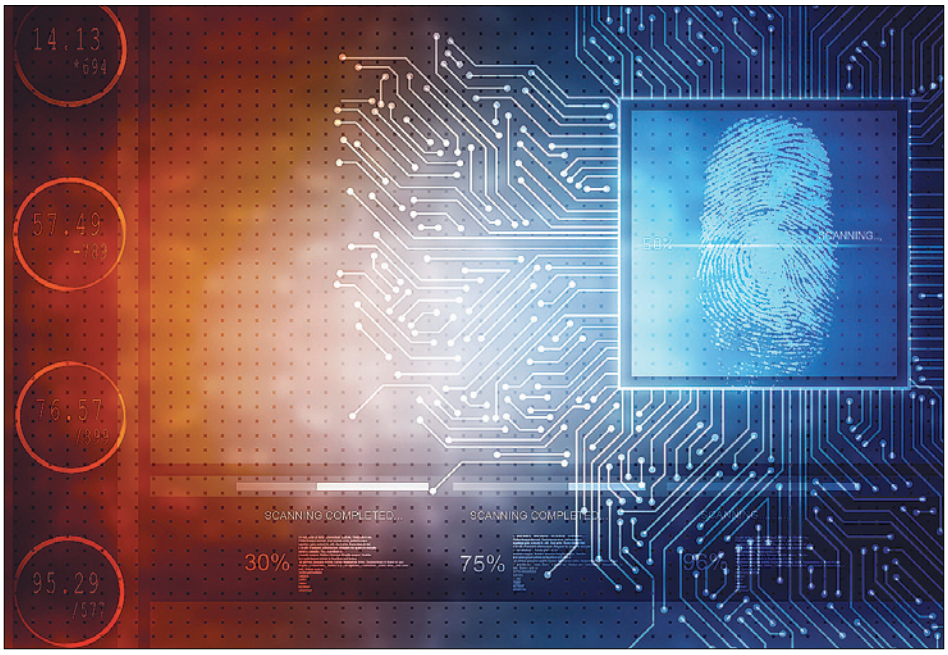
By Lea C. Dearing

FORENSIC EVIDENCE is playing an ever-expanding role in the outcome of nearly every kind of dispute. From laptops and smartphones, to tablets, flash drives and Fitbits, the amount of discoverable electronic information is changing the legal landscape—and how parties win cases.

In-house counsel plays an important role in this rapidly developing field. Below are five tips you can put into practice to boost your company's e-discovery success.

1. Create/Review Policies

Put policies in place that give you undisputed access to and the right to use the data on company devices. Privacy plays an important role in e-discovery when an employee's work devices and personal devices are not kept segregated. Protect your company's ability to collect, access and use all available information through clear provisions in your company handbook, employment agreements and training materials by notifying employees that all computer usage on company devices is subject to review.



SHUTTERSTOCK

2. Work With Your HR and IT Teams

Collaborate with your HR and IT teams to establish policies and procedures for handling departing employee's devices. This plan should include a mechanism for logging the device for chain-of-custody purposes and to secure the device to prevent alteration or destruction of forensic evidence. Also, plan for imaging the device, either internally or externally, before review. Understandably, companies do not want to take devices like computers out of circulation for extended periods of time. Likewise, companies do not want to image

every computer of all departing employees. However, a fair balance can be reached by identifying positions that automatically go into a preservation protocol and others that are evaluated on a case-by-case basis.

3. Get Ahead of the Information Curve

Many in-house counsel know how to preserve and protect data but may lack the understanding of what kinds of information can be mined from the devices. There is a treasure trove available for those who know where to look. Potential sources of valuable information include:

Internet Search History. This shows what websites the employee visited during or near the time of resignation. You can learn whether the employee visited a cloud-based file-sharing website, such as Dropbox. Then, investigate whether that activity was consistent or inconsistent with prior behavior. This type of activity is a possible red flag that company information was taken surreptitiously by the departing employee.

Attachment History. Most devices log all other devices that have been attached. The report gives attachment times and dates, as well as a serial number of the device. You can analyze this data to determine whether the employee regularly attached devices or not, and use the serial numbers to determine if the attached devices were returned by the employee as part of his or her obligation to return all company property. If there are missing devices, it could be a red flag. Note: In many instances, employees are simply removing personal information; therefore, it is important to use the Attachment Report in conjunction with a LNK file analysis (see below).

LNK File Analysis. This shows what files a user was accessing and when. Used in conjunction with the Internet Search History and Attachment History reports, this valuable tool helps illustrate what files an employee potentially transferred outside the company. It may also show that the employee's activity was completely benign. Be sure to have the LNK File Analysis scrubbed by someone who is familiar with the departing employee's roles and responsibilities to determine if he or she was accessing documents that were used regularly in the normal course of job duties or if there was unusual activity that raises red flags. This should be done even if it was not in conjunction with an attachable device or via access to a website, like Dropbox.

Slack Space. This is the where deleted files reside on a device until they are overwritten or deleted by a specific tool designed to clean up the back-end of the device. Often, forensic examiners can fully recover large amounts of recently deleted data if it is important to know what files resided on a device before it was turned in.

In many instances, employees "clean up" their machines before returning them. Restoring the data often gives helpful insight into the employee's activities leading up to resignation, including data such as contact lists, prospect lists, agendas, etc. This data can be used to monitor an employee's compliance with restrictive covenants, if any apply.

Geo Location Reports. Many types of devices record location information tied to date and time stamps. This information can come from Wi-Fi connectivity information, Google Maps and many other places. If you suspect your employee may be moonlighting on company time, use this information to check the whereabouts of your company devices.

4. Find a Forensic Partner

It is important for in-house counsel to have a trusted relationship with a forensic examiner. Just like having a go-to lawyer, in-house counsel should also have a go-to examiner lined up and ready to go. Independent examiners are also an option or those that work as part of a larger e-discovery team that offers end-to-end e-discovery services, including collection, review and production services. No matter your chosen partner, ensure that you have direct access to the examiner who completes the forensic work. Direct communication is invaluable to understanding the significance of the reporting that is generated by the various forensic tools. The reports can be unwieldy, but with a little guidance the least tech savvy among us can pinpoint the important information.

5. Put it All Together

Combine the forensic results with more readily available sources of information to develop a robust picture of a departing employee's activities preresignation. Examine the employee's email activity to determine if company information was forwarded to a personal account. Keep the account active and monitored to determine whether third parties continue to communicate with the employee (often accidentally, via autocomplete mistakes) postresignation. View public social media profiles, such as LinkedIn and Facebook, for public announcements and activities, including key timeline events.

There is a wealth of electronic information that can help a company determine whether it will litigate. Using these tools will give you an edge in determining when to litigate, ultimately providing a more compelling and complete story--the key ingredient to winning the case.

Additional information, including "Electronic Evidence: Where to Find the Smoking Gun," is available at https://www.bfvlaw.com/electronic-evidence-where-to-find-the-smoking-gun/

Lea C. Dearing is a partner attorney at Berman Fink Van Horn. She concentrates her practice on business litigation, noncompete/trade secrets and labor and employment matters.