By Joseph Decker

Securing the Digital Artifacts Important to Employee Investigations

Corporate Counsel Roundtable

Many in-house counsel have their digital forensics team on speed-dial. That is because digital forensics provide the company's legal department and its outside counsel with concrete facts essential to understand the risks and the legal implications of employee activities in today's device-centric corporate environment.

Information and data stored in the company's computers—think more broadly than mere "*documents*"—are essential to understanding what is really going on in the corporation. Theft of company confidential information by an employee bent on using it for his or her new start-up, harassment of co-workers through text messages or emails, data breaches both internal and external, and violations of non-competition agreements, all can be gleaned from deleted web caches, file access history, and the registry files and logs tabulated by almost every digital device your company has. The evidence you need to relay to your outside counsel is right in your office. And that evidence can help make an airtight case that could be amenable to quick resolution. The company's computers and smartphones are eye-witnesses to employee misconduct after hours and out of sight. You have this evidence. This article will help you to use it.

Digital Forensics

Digital forensics is a forensic science, as recognized by the American Academy of Forensic Sciences. Lest we gloss over the over-used word "forensics," the word "forensics" denotes an investigative inquiry sufficiently rigorous to be admitted as evidence in a court of law. Forensics in this context means:

> The scientific examination and analysis of data held on, or retrieved from, ESI [electronically stored information] in such a way that the information can be used as evidence in a court of law. It may include the secure collection of computer data; the examination of suspect data to determine details such as origin and content; the presentation of computer based information to courts of law; and the application of a country's laws to computer practice. Forensics may involve recreating "deleted" or missing files from hard drives, validating dates and logged in authors/editors of documents, and certifying key elements of documents and/or hardware for legal purposes. The Sedona Conference Glossary: E-Discovery & Digital Information Management (3d ed. 2010), *available at* http://www.thesedonaconference.org.

The Sedona definition refers to types of digital evidence that may be very useful in proving a case in court or, for that matter, for justifying a corporate decision on employee conduct that may be challenged in a court or arbitration forum. The "origin" of a document, the re-creation of "deleted" data, and the creation/modified dates and "logged in authors" of documents exemplify digital evidence.

■ Joseph Decker, bit-x-bit's general counsel since 2010, graduated from the University of San Francisco School of Law in 1985 and became a litigator for Orrick Herrington in San Francisco handling trade secret cases. He moved to Pittsburgh in 1991 and most recently was a shareholder with Babst Calland. He taught Trade Secret Law at Duquesne Law School, and is an E-Discovery Special Master for the United States District Court for the Western District of Pennsylvania.

While this list only scratches the surface, in-house counsel can appreciate the import of having hard facts about such activity. If this technical-sounding evidence is presented in audience-friendly form, readily understandable even to the computer illiterate, and if it was easily understandable by counsel, the opposing party, or a court, its persuasive evidentiary value could hardly be overstated.

It has been over ten years since the Federal Rules of Civil Procedure have explicitly recognized the importance of all kinds of digital evidence, not just an electronic .pdf that looks like the familiar paper version of a document. The 2006 Advisory Committee Notes to Rule 34, the rule that governs document requests and responses, state the scope of ESI goes well beyond the electronic equivalent of paper documents:

> But it has become increasingly difficult to say that all forms of electronically stored information, many dynamic in nature, fit within the traditional concept of a "document." Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule 34(a) is amended to confirm that *discovery of electronically stored information stands on equal footing with discovery of paper documents* (emphasis added).

Courts early on recognized that computer hard drives, external USB drives, and forensic images thereof may need to be produced or examined in cases involving alleged theft of trade secrets, for example. *See Balboa Threadworks, Inc. v. Stucky,* 2006 WL 763668, at *3 (D. Kan. Mar. 24, 2006) ("Courts have found that such access is justified in cases involving both trade secrets and electronic evidence, and granted permission to obtain mirror images of the computer equipment which may contain electronic data related to the alleged violation."); *Physicians Interactive v. Lathian Sys., Inc.,* 2003 WL 23018270, at *10 (E. D. Va. Dec. 5, 2003) (granting plaintiff limited expedited discovery to obtain mirror images of defendants' computer equipment containing electronic data relating to defendants' alleged attacks on plaintiff's file server).

What Specific Digital Evidence Is Available?

It has taken time for courts around the country to describe specifically, in published opinions, the types of electronic evidence derived from hard drives and USBs that can persuade a court to grant preliminary relief such as an injunction or temporary restraining order. *See, e.g., Bimbo Bakeries USA, Inc. v. Botticella*, 613 F.3d 102 (3d Cir. 2010). In *Bimbo Bakeries,* the former employee allegedly stole the secret "nooks and crannies" recipe for Thomas English muffins and brought it to his new job at a competitor. Digital evidence in the *Bimbo* case included the employee's accessing of numerous secret documents from company computers in the several days prior to his departure from the company.

> The company's computers and smartphones are eye-witnesses to employee misconduct after hours and out of sight. You have this evidence.

The court in *Boston Scientific Corp. v. Lee*, 2014 WL 3851157 (N.D. Cal. Aug. 4, 2014) provided a glimpse into a typical array of important digital forensic evidence in a trade secret theft case. The defendant, Lee, the former employee who allegedly took trade secrets, went from Boston Scientific Corp. ("BSC") to Nevro. Lee allegedly took over 300,000 BSC documents containing BSC's trade secret spinal cord simulation research.

Digital evidence figured prominently in *Boston Scientific*. Mr. Lee used two computers in his new job at Nevro, as well as flash drives and cloud storage. Nevro engaged a digital forensics expert who took possession of one of the Nevro computers that was used by Mr. Lee, imaged and preserved it, and changed the passwords to Nevro's cloud storage and webmail. There also was evidence that a Kingston flash drive had been plugged into BSC's computers and also into a Nevro computer, giving rise to an inference that BSC documents had been uploaded to Nevro's computers.

Specific and detailed evidence is demanded under the new Defend Trade Secrets Act (DTSA), 18 U.S.C. Section 1836(b) *et seq.* The DTSA provides federal jurisdiction and *ex parte* seizure remedies in cases involving alleged trade secret theft. The DTSA's seizure provisions impose heavy evidentiary burdens on plaintiffs seeking to seize and retrieve purloined trade secrets and enjoin former employees. The DTSA requires a showing of "specific facts" of the "items," such as flash drives, which contain the allegedly stolen trade secret. Plaintiffs must prove who possesses those items and their location, and also that the defendant will "evade, avoid or refuse to comply" with a TRO, that the defendant will destroy, move, or hide the trade secret if served with notice, and that the seizure order is necessary to prevent propagation or dissemination of the trade secret.

Identifying and Preserving the Digital Evidence Still in Your Office

It is clear from experience and from the cases above that digital artifacts are essential witnesses to questionable employee conduct. They paint the picture that is crucial in employee investigations. And this evidence remains in your office after the employee leaves. You will not need a subpoena, a lawsuit, document discovery, or the sheriff to retrieve it. Here are some of the artifacts that can paint a persuasive picture.

Artifacts of Interest

"Last Access" list. Assembling a list of the documents "last accessed" by an employee from his or her work computer is telling. The Windows operating system records the file name and file path of documents accessed by a computer user. Such data includes the date and time that a file was first accessed and last accessed, the location from which it was last accessed, and whether it is still in that location. It will be readily apparent whether the employee is accessing sensitive company documents that ordinarily would not be part of the employee's job, whether the employee is running her own side-business, accessing company documents from an unauthorized USB flash drive, accessing and uploading documents to Dropbox, or covering tracks by deleting documents on the employee's

personal, competitive projects that he does not want managers to know about.

USB insertions. Personal computers typically collect and store the name, model, and serial number of USB drives used on the machine, as well as the first and last time they are plugged in. Matching the dates and times of USB insertions with the accessing of confidential company documents can be persuasive evidence of copying and removal of that document. Knowing the serial number of the USB drive is valuable when trying to determine if the drive is in the company's possession, or must be retrieved, or for determining what other non-company devices the USB was inserted into, perhaps for the purpose of uploading company data.

Internet evidence browsing cache. Forensic extraction of the employee's internet browsing history from the company computer often reveals not only the websites and searches that have been conducted, but also the accessing of cloud storage for possible exfiltration of company information, and the use of webmail accounts.

Deleted data. Deleted data can often be resurrected from the "unallocated space" on the computer hard drive. Unallocated space is not organized, so an effective set of keywords must be used to explore this space. However, it frequently is the case that webmails sent from the user's personal account, or fragments of webmails, can be recovered and reconstructed. If employees are emailing company data to their personal webmail accounts, or communicating with other employees about matters adverse to the company, such evidence may well still be present in unallocated space.

The files that the employee has been accessing, the flash drives or USB storage devices that have been used on company computers, the usage of cloud storage such as Dropbox, or emailing company documents "home" to personal webmail accounts, can be powerful evidence of activities that are of concern.

Preservation

The general counsel's office should communicate directly with the information technology (IT) department at the first sign that an employee's activities may be violating company policies, confidentiality agreements, non-competition agreements, or an employee's duty of loyalty. Employing a "crime scene" mentality is appropriate—figuratively speaking, surrounding the devices with yellow "crime scene tape" is a necessary and urgent first step in an investigation. Indeed, the removal of company data and trade secrets for the benefit of a competitor should be treated as criminal in nature, which in fact it is. This approach includes the following:

- Direct IT to suspend all automatic deletions of the employee's email or other electronic documents immediately.
- If the employee has already exited the company, suspend all "re-purposing" of the ex-employee's computers and other devices. For company smartphones, make sure to obtain the employee's passcode prior to employment termination, and make sure to place the smartphone on "airplane mode," so that it cannot be remotely wiped. ("Airplane mode" can be set even without knowing the passcode.)
- Create a full forensic image of the company devices used by the employee. The imaging should be performed with industry-standard forensic tools, such as EnCase or FTK, ideally by a certified computer examiner. Larger companies may have such persons on-staff. If not, engage a certified examiner. A full forensic image of the entire hard drive will include the "unallocated space" on the hard drive, which contains deleted data. You likely will need to examine deleted data. Be careful of terminology. Sometimes a "ghost" image or "clone" is created, which may not include unallocated space.

> The DTSA's seizure provisions impose heavy evidentiary burdens on plaintiffs seeking to seize and retrieve purloined trade secrets and enjoin former employees.

Mistakes to Avoid

One of the most frequent missteps in gathering and preserving electronic evidence and digital artifacts is the temptation to send in the IT department to "poke around" and see what can be found regarding suspicious activity. This temptation should be resisted until the evidence is properly preserved. As mentioned above, the computer's operating system records first and last file access dates, and it may be important to associate those dates with company activity, an employee's last day in the office, or the insertion of a USB device. The accessing of documents by the IT department could hinder the ability of a forensic examiner to associate dates and times that are important to the analysis. Therefore, before the digital evidence is explored, a full forensic image of the device should be created so that the evidence is definitively preserved.

Likewise, the computer should not be "reassigned," even if a separate user account is created. The continued use and operation of a computer by someone with a separate user profile can cause important data in unallocated space to be overwritten and lost to forensic retrieval. The ability to conduct an effective digital forensic investigation is dependent on preservation of fleeting electronic evidence.

Conclusion

Computers and digital devices are the instrumentalities that, in almost all cases, are used when an employee is engaging in conduct adverse to the company. The digital artifacts created and maintained by the company devices constitute powerful, persuasive, contemporaneous evidence that bear witness to such activity. Such artifacts are essential to informed decision-making by in-house and outside counsel. They allow corporate managers to make sound and informed decisions, and allow outside counsel to carry heavy evidentiary burdens successfully, cross examine witnesses effectively, and make a strong showing when asking a court for extraordinary relief such as the retrieval of company trade secrets and injunctions from the dissemination of confidential and proprietary company data.