BUSINESS INSIGHTS FOR THE LEGAL PROFESSIONAL

Opinion

January 10, 2014

Technology: To image, or not to image, that is the question

Avoid a Shakespearean tragedy when deciding whether to image hard drives

By Gareth Evans, Danielle Serbin

If computers, hard drives and e-discovery had existed in 17th century England, and if Shakespeare's character Hamlet — the son of the Danish King in the eponymous play — had also been legal counsel for the Kingdom of Denmark, what would he have said in contemplating whether to image or not to image the hard drives of the castle's computers for a legal hold?

Perhaps some of the same things as in his "To be or not to be" soliloquy.

"Whether 'tis nobler in the mind to suffer the slings and arrows of outrageous fortune or to take arms against a sea of troubles, and by opposing end them?" Should I suffer the slings and arrows that opposing counsel and the court may cast my way if I don't extract and preserve an exact copy of every bit of information on a custodian's hard drive? Or will a targeted extraction and copying of particular files be sufficient?

"To die, to sleep, to sleep perchance to dream; aye, there's the rub, for in that sleep of death, what dreams may come, when we have shuffled off this mortal coil, must give us pause." If I image the drives, will I only suffer other problems — and unnecessarily so if there was really no need to undertake the imaging — such as incurring the costs of making images and the potential impacts of over-preservation, including the costs of storing, processing, searching and reviewing the data?

To image, or not to image, that is the question.

Unlike Hamlet's decision, contemplating whether to make an image is rarely a matter of life and death. Nevertheless, it can be very important.

A "forensic," "mirror" or "physical" image — all three terms are used — is an exact copy of a storage device, replicating all of its data bit for bit, including all active files and the remnants of "deleted" files. When a file is deleted, it is not actually erased, but the space that it occupied becomes "unallocated" space, i.e., space that can be overwritten with new data. Until unallocated space is overwritten with new data, it may contain deleted files or fragments that can be retrieved using forensic techniques. Similarly, "slack" space — the space between the end of a file and the end of the disk cluster in which it is stored — can hold fragments of "deleted" files.

Using the right tools and techniques, a technician or forensic analyst may restore and extract, either in whole or in part, deleted and older versions of files from traditional hard drives for lawyers' review. (This may be difficult or impossible to do from solid state drives,

however, as the operating system may physically clear blocks of data no longer in use to ensure optimal performance in writing data.)

Additionally, a forensic analyst can conduct a forensic examination of the data that may reveal information such as Internet activity (e.g., websites visited, searches conducted, etc.); whether a thumb drive or external hard drive was connected and data copied to it; whether documents were altered or deleted; and whether the custodian used any applications to "wipe" data from the drive.

Forensic examinations have featured prominently in high-profile murder trials, revealing illicit affairs, searches for undetectable poisons and other methods of doing away with the victim. If Hamlet had the assistance of a forensic examiner, he might have been able to prove that his uncle Claudius had conducted a Google search for the poison he used to kill Hamlet's father, marry Hamlet's mother and usurp the throne. Instead, Hamlet had to rely upon a play to induce Claudius to reveal his treachery ("the play's the thing wherein I'll catch the conscience of the king"). Forensic examinations may also reveal the theft of trade secrets, efforts to forge or falsify documents, and efforts to destroy evidence and cover one's tracks.

When might you image a drive or other storage media instead of selectively copying files?

There are generally two sets of circumstances when imaging may be required or prudent: (1) When information relevant and important to the case can only be uncovered through some form of forensic recovery or examination; and (2) in high-stakes matters where a party wants to ensure the highest level of defensibility, particularly where the scope of the issues may evolve or change.

Cases involving thefts of intellectual property or trade secrets, criminal or regulatory enforcement actions, and cases where there is evidence that a custodian attempted to destroy relevant information can be good candidates for imaging at least some custodians' hard drives. It is also not uncommon in very high-stakes litigation for a party to make images of at least some key custodians' hard drives as part of an effort to minimize risks.

Nevertheless, as The Sedona Conference states in its *Commentary on Legal Holds*, obtaining a forensic image "is not, nor should it be, the default method of collection and preservation." In most cases, there will simply be no need for data that can only be obtained through a forensic examination.

The costs of making images — usually several hundred dollars per hard drive — may not seem like much in small quantities. But they add up quickly. Some large cases involve hundreds of custodians. Large companies that are regularly involved in litigation can have many thousands of employees subject to legal holds at a given time. If you were to image all custodians' drives, it could mean costs in the six- to seven-figure range.

Consequently, Hamlet in all but exceptional circumstances may decide not to image the castle's drives. "And thus the native hue of resolution is sicklied o'er with the pale cast of thought, and enterprises of great pith and moment with this regard their currents turn awry, and lose the name of action."

Hamlet's soliloquy ends with the approach of Ophelia. "Soft you now, the fair Ophelia! — Nymph, in thy orisons [prayers] be all my sins remembered." Let's imagine Ophelia as an e-discovery technician. In her forensic images, may every file, and every keystroke, be remembered.

About the Authors

Gareth Evans

Gareth Evans is a partner at Gibson Dunn. His practice focuses on complex litigation, including information technology, data privacy and e-discovery.

Danielle Serbin

Danielle Serbin is an associate at Gibson Dunn. Her practice focuses on complex litigation, including information technology, data privacy and e-discovery.