

Amber Heard, Johnny Depp, & Metadata

TransPerfect Legal Solutions



Thanks to the trial between Amber Heard and Johnny Depp, we have a timely reason to talk about e-discovery metadata. What happens on the rare occasion when forensic data collections and trials of cultural relevance overlap?

On May 26, 2022, the e-discovery world was riveted by the testimony given by Depp's expert witness, Norbert (Bryan) Neumeister, USA Forensic CEO. Neumeister was called to testify about the authenticity of certain photos that Heard entered into evidence. The examination quickly turned to the meta- and EXIF data contained in those photos. The issues with digital evidence addressed in Neumeister's testimony show the value of keeping defensible forensic collections in mind at the outset of a matter so that issues with authentication do not detract from a client's case at trial.

"I have never met a lay person who had heard of the best evidence rule."

Much of Neumeister's testimony concerned the authentication of certain photographs detailing Heard's alleged injuries.

Authenticating evidence entails proving that the photographs are what the party says they are, so the jury can rely on them for evidence. Digital evidence, like these photographs, can be easily modified using filters and editing software. One way to expose a modified file is by examining the metadata attached to the file at the time of collection.



@TransPerfectLegalSolutions



@TSLegal

Richard Corvinus,* TLS Senior Manager of Forensic Technology and Consulting, watched the testimony closely and had some important observations for litigants with respect to the forensic collection of cell phone data and presentation in trial.

“The definition and universal explanation of metadata in digital forensics is data about data. The EXIF data is just a different format of metadata that is attached to a video or digital image file, but it is metadata,” Corvinus explained.

Here, Corvinus disagreed with Neumeister’s classification that EXIF data was something different than metadata, rather than a subcategory.

“The EXIF data travels with the file and will contain some information about the file and its data. While the images in the trial depicted a portion of the EXIF data showing the photo was taken with an Apple iPhone, the software is listed as ‘Photos 3.0,’ which indicates that the image did not come directly from the Apple iPhone, but passed through editing software first. The EXIF data for an image taken with an Apple iPhone is actually quite voluminous. Some of the data it will contain are dates and times relating to the image, camera settings, and geolocation data about where the photo was taken,” Corvinus continued.

After watching Neumeister’s testimony closely, Corvinus had three major observations related to forensic collections and authentication of cell phone data that would be helpful for any attorney or e-discovery professional to keep in mind.

The Best Evidence Rule

Collecting images or other data from a cell phone is not a DIY project; it is a task for an experienced forensic professional.

When presenting evidence at trial, the best evidence rule comes into play. This means that if the original item of evidence cannot be found, there must be an acceptable excuse for its absence and substitution with another source. For the photos Neumeister discussed, the best possible source would have been the Apple iPhone 6 that was used to take the images. Collection from the actual device would allow for verification of the images using not only the EXIF data but also elements of the phone’s operating system.

“Now, I have never met a lay person who had heard of the best evidence rule,” Corvinus notes, “but Heard’s attorneys surely were aware of it and could have engaged a digital forensic examiner to extract the images in the most defensible manner.”

“On the one hand,” Corvinus said, “authentication of digital photographs is complicated and so forensics professionals must take all the appropriate steps to avoid any potential wildcards. On the other hand, the defense in this case was hurt by the fact that the plaintiff tried to submit these enhanced or potentially enhanced pictures as evidence themselves. Collection best practice will always be to keep the original source of the data, as that will present the cleanest information forensically.



@TransPerfectLegalSolutions



@TSLegal



"It is almost universally impossible to assign intent in a computer crime."

"While not perfect," Corvinus added, "opening up a backup using a forensics tool provides at least some level of verification. This aspect of the case is focused on what sounds like an iTunes backup of her iPhone 6. It really is not something that could be authenticated because it's not the way we would forensically collect. So, while the evidence doesn't show that anybody intentionally enhanced the image, there is no way to eliminate the possibility that someone did."

"In this case, because it is difficult to authenticate pictures off of a phone, collecting this data in a forensically sound manner is even more important in order to gain the trust of the jury. The best solution is to go back to the original backup on the original computer it was created on. That said, the most important thing is to keep matters of authentication at the forefront of your mind when dealing with digital photographs that may become evidence in a legal proceeding," Corvinus said.

As a result of using backups of backups, instead of the iPhone itself, unnecessary doubt was cast on the provenance of the photographs at trial. That doubt may have weighed on the jury's mind as it reached its decision.

Proving Intent in a Computer Crime

Metadata and EXIF data can tell you what happened to a file, but in Corvinus's experience, "It is almost universally impossible to assign intent in a computer crime." The exercise for counsel presenting the evidence becomes putting together enough context to reduce doubts about that intent.

Heard's team argued that the pictures of Heard's bruises were accurate representations of how she appeared at the time they were taken. Depp's team countered that, not only were the photos inaccurate, they were deliberately altered by Heard to make the injuries appear worse.

Intent, being a mental state, is nearly impossible to assign using electronic evidence, but intent can be inferred from the evidence nonetheless. Depp's team's use of Neumeister's testimony was meant to challenge the validity of the photographic images presented by Heard's team. The presentation of files depicting how they were processed through photo software capable of editing the photos presented the jury with the possibility that they had been altered.

"If somebody wants to make a file look like it was created at a different time, you can change those dates and times. That's why collecting from the original source is most important, because now I would get that master file table entry and I'd be able to see the file name, dates, and times. I'd also be able to see the metadata inside the file, and I'd have three sets of dates and times to correspond and authenticate that file to the level that I can at that point in time," Corvinus said.

However, without said information, the subject of Heard's intent when saving the digital photographs becomes an open issue that Depp's team was able to use to attempt to sow doubt in the jury's mind.



Prepare Your Witness to be an Expert, not an Advocate

While not calling into question Neumeister's qualifications, Corvinus noted that Neumeister often crossed the line between expert and advocate. Neumeister opened his testimony by making the statement, "Data is data; it doesn't take a side," to support his status as a subject matter expert. However, when faced with cross examination about the evidence, Neumeister frequently became visibly agitated when he was restricted from testifying in certain areas. Generally, Neumeister did not seem to appreciate being limited to yes or no questions by Heard's team when he thought important context was being left out.

Providing context on cross examination is not the expert's job; it is the attorney's job.

A good expert knows that it is the opposition's job to use cross examination to muddy the waters as to his or her testimony. Similarly, they know that a good attorney will clarify any major issues upon redirect. Arguing with opposing counsel is fruitless and can leave a bad impression on the jury.

Defensible Data Collection

Ultimately, effective presentation of evidence at trial starts with defensible forensic data collections at the very beginning of the matter. The average cell phone owner—or attorney for that matter—doesn't know what they don't know about forensic collections. The Depp/Heard trial is another great reminder that keeping matters of authentication at the forefront of your thinking at the outset of a matter will reduce or even eliminate issues at trial.

After all, data is data; it never takes sides.

**Corvinus is a highly skilled digital forensic examiner with over two decades of experience in investigations, litigation support, digital forensics, evidence handling, lab operations, e-discovery support, memory forensics, and incident response. A multi-certified expert witness in both Federal and New York State Courts, his expertise is more likely to appear in technical journals than on TMZ.*