TRANSPERFECT
LEGAL SOLUTIONS

Amber Heard, Johnny Depp & Metadata

June 20, 2022

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.

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.

"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.*

TRANSPERFECT
LEGAL SOLUTIONS

Ephemeral Messaging and the Duty to Preserve

January 28, 2022

Short, often informal messages have become an increasingly prevalent form of business communication. Whether by sending a simple text message or using a communication application like WhatsApp, Slack, or MS Teams, employees conduct more business in less formal ways than ever before. This article will discuss the rise of ephemeral messaging platform use, a case where the technology was misused that resulted in sanctions, and ways in which practitioners can avoid sanctions themselves.

Ephemeral Messaging Explained

Ephemeral (or disappearing) messaging applications enable users to automatically delete messages after they are received. These platforms not only delete messages and related metadata from all devices and servers, but many also apply end-to-end (E2E) encryption to messages sent within them. This means that nobody, *including forensics professionals and the platform itself*, can read these messages besides the sender or recipient.

While there may be substantial business benefits to the use of ephemeral messaging applications, the medium also raises significant e-discovery challenges. Courts have begun to grapple with the discovery implications of ephemeral messaging, as evidenced by a 2019 decision out of the Western District of Arkansas, *Herzig v. Arkansas Foundation for Medical Care, Inc*.

Herzig v. Ark. Found. For Med Care, 2019 WL 287106

Herzig v. Ark. Found. For Med Care was a wrongful termination matter. After making an initial production of text messages, Plaintiffs installed Signal—an E2E encrypted messaging app—on their mobile devices. They configured the app to delete all messages after the recipient reads the message. Plaintiffs made this change after they were well aware of their duty to preserve documents, and only disclosed it to the Court and Defendants toward the end of discovery. The initial production showed that Plaintiffs had numerous communications with one another and with Defendant employees, but only produced some of those messages. Following Defendants' successful motion to compel, Plaintiffs produced several more communications, but, suspiciously, the dates of communications ended the day one of the Plaintiffs downloaded Signal.

Plaintiffs argued that their duty to preserve did not allow Defendants to see all of their communications, only responsive communications, and that the Defendants had not shown that the communications that disappeared were responsive or that their destruction was in bad faith. The Court disagreed, finding that Plaintiffs used Signal to intentionally and in bad faith destroy and withhold ongoing communications about the litigation.

The Court inferred that Plaintiffs were intentionally deleting responsive communications based on, among other reasons, Plaintiffs' reluctance to produce responsive messages during the initial request for production and the manual setting to delete the subsequent Signal messages after they were read. Not helping their argument, both Plaintiffs were information technology professionals who were expected to be aware of the technical capabilities of Signal. As a result, the Court held that both Plaintiffs had the requisite knowledge to produce and retain responsive communications, and that they intentionally used Signal to withhold responsive data in bad faith. While the Court found that the Plaintiffs' conduct was sanctionable, it did not actually issue sanctions, as it dismissed their case on the merits instead.

Three Steps to Avoid Sanctions

Herzig demonstrates that litigants cannot use ephemeral messaging applications to sidestep their duty to preserve responsive communications. The *Herzig* court found that manually configuring these applications to destroy responsive messages while under the duty to preserve was an intentional act of bad faith. With that context in mind, here are three steps practitioners can take to avoid sanctions when ephemeral messages are in scope for discovery:

1. Ephemeral messaging is not an end-around for a litigant's preservation obligations. Attorneys should be aware of the use of ephemeral messaging applications and include language in the litigation hold and preservation memos. Turning off auto-delete functions for email and other systems is standard across IT departments, and should apply to messaging applications as well. As in *Herzig*, a sudden switch from permanent to ephemeral messaging applications, or suddenly switching on the auto-delete function of an ephemeral messaging application, will look suspicious in the event of a discovery dispute.

2. Organizations should utilize ephemeral messaging platforms that allow them to meet their legal obligations. In some instances, an organization may need to ensure that it has the ability to turn the auto-delete functionality off and on as needed. For example, regulated industries have requirements that pertain to data preservation, retention, and archiving. Understanding these requirements will help you know when ephemeral messaging may be in direct violation of those regulations.

3. As with any other business communication tool, policies and guidelines should be in place to govern the use of ephemeral messaging applications. Asking about your client's policies during your initial investigation and your opponent's policies during pre-trial conferences will help you structure your discovery requests.

Moving Forward

While there are clear business benefits to the use of ephemeral messaging applications, there are also ways they can be misused—either intentionally or otherwise—in a way that can put an organization at odds with its preservation obligations. Attorneys should be aware of this risk and take active steps to ensure that their clients do not use these applications in a sanctionable manner.

TRANSPERFECT
LEGAL SOLUTIONS

Best Practice Mobile Device Collection: iPhone Versus Android

July 1, 2022

It is safe to say that most of the world's adult (and child) population owns or has access to a mobile phone. These devices are capturing all kinds of private and sensitive data—some of which is generated by the user, while other data is generated by an app or the device itself.

But data is inherently fragile and can easily and inadvertently be deleted or overwritten when improper collection methods are employed. Utilizing scraping tools and unsound forensic methods coupled with ill-prepared practitioners may create authentication issues and, in the worst case, cause data to be destroyed or changed, opening the door to spoliation motion practice.

When it comes to mobile devices, the best method is one that is forensically sound and equips counsel with the tools and data needed to authenticate individual pieces of evidence. A mobile device can reveal key information during a forensic collection, including dates, times, locations, and who a person might be communicating with—in or outside an organization.

That said, not every mobile device is created equal. Apple iPhones and Android phones all act differently, and what can or cannot be collected often depends on the underlying operating system.

Mobile Devices

Ninety-eight percent of mobile phone users have either an iPhone or Android device. Both devices have their own unique challenges, multiple versions, various operating systems, and constant updates. As mobile devices are updated and the operating systems change to make them more secure and increase functionality, digital forensic technology is also being updated.

iPhone

The iPhone is the friendlier of the two because there are several options available to collect a full image of the device. Unlike the Android device, an iPhone can only collect full and specific artifacts or types of data. For example, text messages cannot be specifically targeted at collection. Rather, this information is parsed out from the full image.

The iPhone, like any computer, also overwrites data that the user identifies for deletion, but later versions of the iPhone operating system overwrite data with greater frequency. When it comes to preservation and collection, knowing deleted mobile data is frequently overwritten can be the difference between having the deleted message and not. When it is time for collection, key factors in the deletion of data are the passage of time, movement of data on the device, and software updates. Even then, deleted data that is able to be restored is often incomplete.

Mobile device collection also has a logistical challenge in that no one wants to be without their phone for any period of time. There are three options when it comes to collecting mobile devices and they are the same three options for any data source: in a digital forensics laboratory, on-site with a digital forensics examiner, or using a remote collection kit sent directly to the owner or administrator of the phone.

For iPhones, you can also collect through an iTunes backup or from iCloud. These options are sometimes helpful when deleted data is in question, as earlier backups are occasionally stored.

Android

Android devices run on the Google ecosystems, but there are a great number of hardware choices from multiple manufacturers. Another challenge with Android is that these devices are open source, meaning anyone can modify a device. Modifications may include adding storage through a microSD card or changing the rules for how data is stored on the device. This could present significant challenges for digital forensics examiners during a collection.

Unlike the iPhone, Android collections can target specific sets of data. For example, should you only need text messages or messages from another application that is stored on the phone, those can be surgically collected. But, remember that no one wants to be without their phone, so collecting all of the data at the first collection is the most efficient use of your client's time and money.

A common pain point with mobile messaging apps is how to review the conversation outside of the device. In the device, the messages appear in colored bubbles clearly identifying the sender and conversation thread. Once that message is removed from the device, the bubbles and colors are gone and the message thread appears in an Excel or other non-user-friendly reporting platform.

Using an application like Relativity can help. With scripting, a more linear report is generated, whereby the reviewer can visualize the messaging thread and see the colors and bubbles, restoring the conversation to a similar view to how it existed on the mobile device.

Ephemeral Messaging

Ephemeral Messages—generated in platforms like WhatsApp, Telegram, WeChat, and Signal—can quickly disappear, either manually or automatically. These applications are used by both Apple IOS and Android users. What makes them ephemeral is that the user can choose to have the message automatically deleted after a specific amount of time. Users can also choose to delete ad hoc. When this option is set or actions taken, the messages are deleted and cannot be retrieved.

In WhatsApp, for example, we can collect data from the device itself, but in instances where data is deleted, there are options to potentially collect the data from the cloud using cloud-based exports and API connectors.

Each application is different, and while some applications store data on the device, others only store data in the cloud. There are a number of factors that account for the success of being able to collect from these types of applications; after all, they were created with the idea that the data would be read and deleted without any artifacts or remnants left behind.

Mobile devices abound, and while mobile device collection can be challenging, they contain a significant amount of evidence and should always be requested in discovery. Preserving the device early and having a digital forensics examiner create a preservation collection image of the device is a best practice. Also keep in mind that a mobile device is the primary gateway to a wealth of information in the cloud.