OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXIV NUMBER VII
AUGUST 2017
www.mnbar.org

Bench&Bar OF MINNESOTA

LITIGATING SPORTS CONCUSSIONS

WHAT YOU NEED TO KNOW ABOUT THE SCIENCE AND THE LAW

Ethical Considerations in Working with Aging Clients

Happy Birthday, Whistleblowers: Minnesota law turns 30

Plus

Are Title Company Kickbacks Harming Your Clients?

By Mark Lanterman

Digital evidence: New authentication standards coming

As it is now written, Federal Rule of Evidence 902 pertains to self-authenticating records such as newspapers and public records that require no external evidence to be made admissible at trial. Soon, the rule will encompass digital records generated by electronic processes in addition to records preserved directly from electronic devices or files, such as emails. This December, new amendments to Rule 902 will affect the standards for the admissibility of digital evidence. Newly proposed paragraphs 13 and 14 of Rule 902 will remove authentication hurdles for electronic evidence, whether it consists of an electronic document, file, or raw data. The proposed text of rule is as follows (emphasis added):

> The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:
>
> ***
>
> (13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces *an accurate result*, as shown by a certification of a *qualified person* that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).
>
> (14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if *authenticated by a process of digital identification*, as shown by a certification of a *qualified person* that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

MARK LANTERMAN is the chief technology officer of Computer Forensic Services. A former member of the U. S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security and forensic experience and has testified in over 2,000 cases.

With this change, digital evidence, and the story it tells, have many foundational questions out of the way. Without knowing how courts will apply the rule, however, I think that there is one caveat that will impact litigants—chain-of-custody/acceptable collection practices. With these upcoming changes in mind, it is clear that proper evidence collection and acknowledgment of best practices are critical. In this article, I will describe issues pertaining to proper digital evidence handling and the increased need for digital forensic professionals in light of these upcoming amendments.

A focus on best practices

The rules being implemented this December will greatly ease the burden of authenticating digital evidence and allow for a more cohesive system of evidence collection. These amendments largely serve to replace live testimony from any number of witnesses for the purpose of authentication with an affidavit from a certified person who can reliably attest to the evidence's authenticity. These new amendments underscore the court's increasing reliance on expert witnesses in preserving and bringing forth digital evidence.

Digital evidence is undeniably a prominent feature in the courtroom. In a growing number of situations, pieces of electronically stored information are the basis of investigations within organizations, for law enforcement, and in litigation. This degree of importance requires an equally high degree of care. Issues of authentication and proper evidence handling are particularly pertinent, since digital evidence is extremely susceptible to alteration and mishandling if not done properly by a qualified individual.

To illustrate, I will describe a typical, though always frustrating, situation that I encounter when assisting an organization or company responding to an incident involving digital evidence. Let's start here: Your company has a summer internship program. Each summer, one or two interns join your team and are assigned a number of different tasks that require varying degrees of access to your company's data. At some point during the internship period, it is discovered that one of these interns has been attempting to send confidential client data to a personal email address without prior authorization. IT is subsequently alerted and they are asked to handle the situation. Their first step is to retrieve the systems issued by the company to the offending party.

In an effort to deduce what exactly has occurred (i.e. what kinds of information were shared, with whom, and how many times), the IT person logs into the system with the intern's user credentials one day after the incident has been reported. The IT person clicks around on the intern's issued computer, trying to figure out what has transpired. This is not best practice. Although it is well-meaning, simply turning on a computer or electronic device permanently alters the state of the data. Think of it like a crime scene. Just as law enforcement wouldn't want to go snooping through a scene without taking proper precautions to ensure evidence will not be contaminated, digital evidence requires the same degree of care.

In reality, the IT person has unknowingly altered date and time stamps, overwritten useful deleted data, and skewed the original digital narrative of the intern's activity. In this instance, the intern's computer has been mishandled, making authentication an even greater hurdle down the road. While this evidence potentially held information that would have made the details of this event crystal clear, the IT person's involvement has made things murkier, and possibly not self-authenticating under the proposed additions to Rule 902.

So what should the IT person have done instead? Turn off the system as

quickly as possible and find a digital forensic expert for forensic preservation. While IT departments promote cybersecurity and technology policies, it is important to differentiate between IT services and digital forensics. The former is proactive or precautionary, and the latter is reactive (e.g. used in litigation).

Therefore, using forensic methodologies that leave the "crime scene" unaltered, so to speak, is key for ensuring compliance with Rule 902. Adhering to best practices in the collection of digital evidence is emphasized in the upcoming additions to Federal Rule 902. Relying on digital forensic professionals is necessary in ensuring the usability of digital evidence, as well as taking advantage of the lower burdens for authentication for it under Rule 902.

Digital evidence is an unbiased witness

Standardizing methods for the collection of electronically stored information is a big step toward recognizing the value of digital evidence as an unbiased witness. As society begins to move further away from "hard copies," this addition demonstrates the law's flexibility in accommodating our digital age. Unlike other types of information that may be collected for a trial, digital evidence is capable of presenting an unbiased record of activity. Admittedly, electronic evidence is not necessarily a complete repository of critical data, but think of the one device that most likely goes everywhere with you—your smart phone. I would argue that, for most of us, smartphones hold the most information about our day-to-day lives and much can be gleaned about our plans, intentions, and daily lives by reviewing their contents. The recent controversy over whether or not people should be forced to unlock their phones using a fingerprint illustrates exactly how protective people are of what is stored on their phones. With good reason, I often refer to phones as being like "snitches in our pockets." It doesn't matter how someone appears, how someone acts, or how convincing someone's story may be—digital evidence doesn't lie. Geolocation, text messages, emails, fitness applications, web browsing history, phone call logs, social media apps, and photos are only some of the ways that our phones offer glimpses into our lives. All of this information would be self-authenticating under the proposed 902(13), so long as it is certified by a qualified person.

Furthermore, the sheer volume of electronically stored information is constantly growing—creating an ocean of potentially useful data. As more and more is always being created, gathered, and stored on the vast number of diverse devices, litigants are presented with a huge amount and variety of potential evidence to use in court. Law enforcement is also faced with the problems posed by an influx of new technology, as data must be extracted from a variety of devices utilizing a number of different methods and tools. It would seem that as more emphasis is placed on digital evidence, it has become correspondingly difficult to gather, authenticate, and present in court. The revised Rule 902 responds to these issues for litigants by lowering the authentication hurdles.

Digital evidence can be open to interpretation

As an expert witness, I am frequently called upon to validate and explain digital forensic findings and their significance given the particulars of a case. Revealing hidden artifacts of long-forgotten digital activity is one thing—but constructing reliable narratives based on these facts and explaining their significance? Quite another. Questions of admissibility are only the beginning in establishing the value of electronic evidence. Making testimony understandable can be very difficult when computer lingo is a factor. And let's face it—computer people don't always have reputations for being effective communicators. And this is especially problematic, since oftentimes one piece of digital evidence can be the key that unlocks an entire case.

If it can be uncovered and related in an understandable way to a judge or jury, digital evidence is absolutely critical. Apart from the processes of uncovering data and ensuring its admissibility, the purpose of a digital forensic examination is to uncover a usable and understandable timeline, or narrative of digital activity. Ideally, forensic evidence is presented in such a way that it makes sense to everyone, not just the IT people in the room. Digital forensic experts are ultimately tasked with effectively explaining why a piece of evidence is significant, or possibly critical, in a case.

The expansion to include digital evidence in Federal Rule of Evidence 902 marks a definitive movement toward the standardization of data collection and authentication. No doubt, this will impact practitioners in federal court immediately, but also state court practitioners, as states commonly adopt rules that substantially track the federal rules. As such, this change underscores the need for digital forensic expert witnesses who can attest to both the authentication and significance of electronically stored information in both state and federal courts. While these changes go into effect on December 1 of this year, in reality, they are in place now. Following best practices for digital collection is now pertinent for any case going to trial after this date. ▲