



P.O. Box 5337
Arlington, VA 22205

Notices Solely on the Internet are Difficult to Authenticate in Court

Public notices in newspapers remain the best manner of delivery to ensure that notices remain independent, accessible, verifiable and archivable.

Challenges that threaten to move public notices from newspapers to an online forum create numerous problems, specifically problems with authentication in court. Federal Rule 902 specifically validates that newspapers in print are self-authenticating in federal court.

Litigants now sometimes wish to introduce printed copies of material they found online, which creates challenges for courts and sometimes results in complications for lawsuits. Foundations for digital evidence are rooted in the identical foundations of admissibility and authentication as used for paper evidence: 1) relevance, 2) authenticity, 3) hearsay, 4) best evidence and 5) the probative value must outweigh any prejudicial effect.

Fed. R. Evid 901(a) provides the standard for the admissibility of evidence, requiring a foundation that the evidence is what the proponent claims it to be. To authenticate digital evidence, the court must additionally consider who created the evidence, what processes and technology were used and the chain of custody throughout the entire digital evidence lifecycle. To establish those facts, human witnesses may need to appear to attest to the creation, the processes and the technology.

In Nevada, the standard for admissibility of evidence (Sec. 52.015) is similar to the federal rules.

Challenges to digital evidence in legal proceedings are abundant. Courts have used strict, somewhat strict and lenient criteria to determine the admissibility of digital evidence in legal proceedings. As a whole, there appears to be no uniformity as to which standard will be applied.

However, the courts provide some guidance as to why websites are difficult to authenticate:

- **Digital information may be created easily without any verifiable record of who did so.** Authorship and chain of custody can be difficult to prove. Each record in the digital life cycle must be authenticated for validity.
- **Digital information can be changed, often without detection.** Digital records may be altered, manipulated or damaged after creation. Viruses can attack. Further, hackers can alter websites and change information, covering their tracks by changing audit log records.
- **The data may not be reliable.** It is critical to assess whether the information presented was correctly configured and maintained to ensure the accuracy as posted on the website.
- **Websites are dynamic and may display different content to different users.** Often websites change their content slightly so every word on the page may appear different to different users. Different browsers may present the information differently.