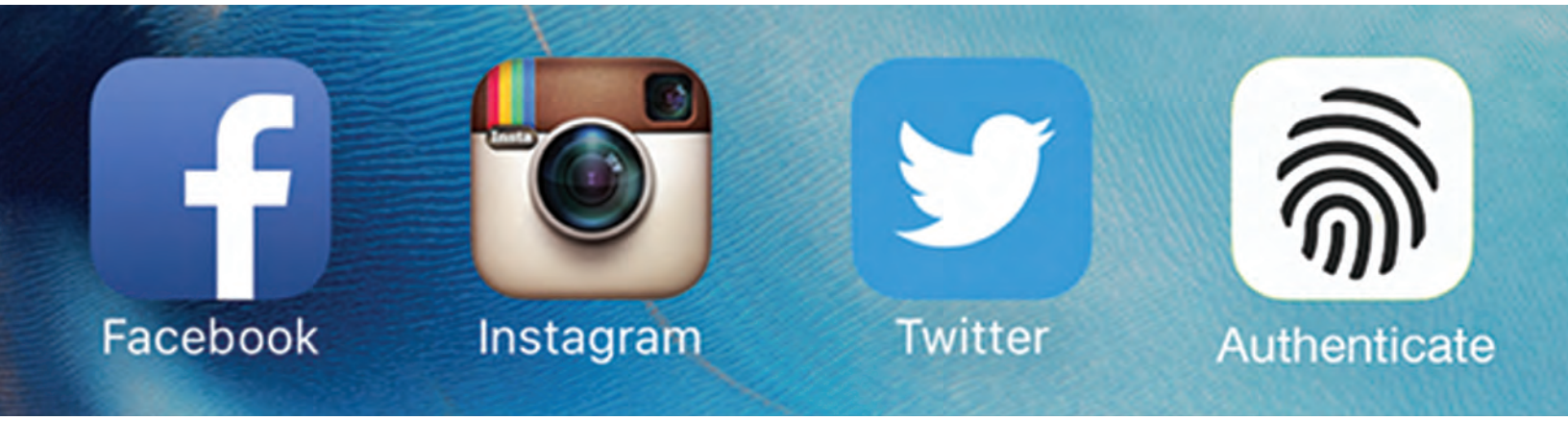
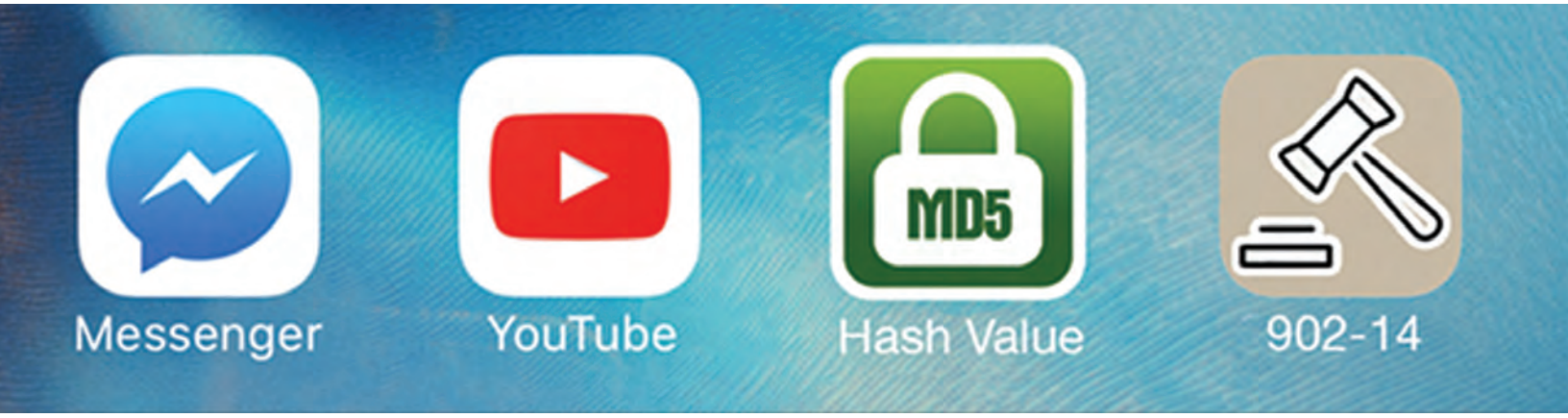


THE LANDSCAPE FOR INTERNET AND SOCIAL MEDIA EVIDENCE HAS CHANGED WITH PROPOSED AMENDMENTS TO FEDERAL RULE OF EVIDENCE 902.14

Thom Kramer Marshall Investigative Group



Over the past 30 years, there have been several milestones within the insurance defense investigative industry. In the late 1980s, the availability of consumer and prosumer video cameras changed claims investigations. We could document an individual's physical activities and compare this activity to his or her alleged claim. In the 1990s, video-camera technology grew, and the cameras became smaller.

With the explosion of smartphone technology in the past decade, we still engage in surveillance to validate a questionable claim; however, in many cases, these individuals are doing all the work with their own cameras and willingly providing details of their private lives on social media. Sometimes this internet and social media evidence may be fleeting – here today, gone tomorrow. If you can locate the data, questions of authenticity may arise when you seek to admit it as evidence.

Finding evidence is one thing, but capturing and authenticating this information can make or break a case. Internet-presence evidence can determine the validity of a claim. Plaintiff attorneys in some cases cannot control what their clients or associates post online. We have all had cases where we say, "I can't believe this person is putting this online for the world to see." At this point, the plaintiff's attorney may have to discredit the information and to eliminate it as evidence.

Up until now many people believed they could simply take a screenshot of the desired social media postings, copy the URL (web address) and consider that as evidence for negotiations or a trial. Five years ago that would have been sufficient. Now there is a good chance a screenshot could be thrown out. A screenshot is a one-time, static image, and these images are limited and are not searchable because they have no relevant metadata.

The Federal Rule of Evidence 902.14 recognizes the importance of collected Internet / social media information and its impact as evidence. What does this mean for the world of insurance defense litigation?

The amendments to Rule 902 that went into effect December 1, 2017, highlight the importance of using best practices for collecting electronic and internet-based evidence. The new rules make it clear that a certification must be provided by a "qualified person" who can attest to the accuracy or reliability of the collection process that produced the exhibit or establish that the exhibit is accurate. Hence, it is important that parties to litigation not only use defensible collection methods and tools, but also an experienced *e-discovery* practitioner, information technology practitioner, or forensic expert when collecting electronic evidence.

According to Rule 901(a), to prove electronic evidence is authentic, a proponent must provide supporting evidence that the electronic item is what the proponent claims. Federal Rule of Evidence Rule 901(b) gives advice on how to ensure evidence is authentic, such as the testimony of a knowledgeable witness.

In its current form, Rule 902(4) states that certified copies of public records, government documents, and newspapers are self-authenticating and do not require evidence of authenticity. Rules 902(11) and (12) allow the use of a qualified foundation witness to certify the authenticity of business records, but an opponent is given "a fair opportunity" to challenge both the certificate and the underlying record.

The proposed amendments to Rule 902 would add two new subdivisions that set forth a procedure for authenticating certain electronic evidence without the testimony of a foundation witness. The following items of evidence are self-authenticating and require no authenticity in order to be admitted in a trial (Cornell Law Institute https://www.law.cornell.edu/rules/fre/rule_902):

(13) Certified records generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person who complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11); and

(14) Certified data copied from an electronic device, storage medium, or file, if authenticated by digital identification, as shown by a certification of a qualified person who complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

The first amendment (paragraph 13) allows self-authentication of machine-generated information. The second amendment (paragraph 14) allows self-authentication of data from an electronic device (i.e. establishing that the copy of a Facebook profile was identical to the profile content using an industry-standard methodology for metadata collection including MD5 hash values.)

WHAT ARE MD5 HASH VALUES?

The MD5 hashing algorithm is a cryptographic function that accepts a message of any length as input and outputs a 32 character hexadecimal string value. This value authenticates the original message. If the same hexadecimal string is run through the hashing algorithm, the result will be the same. As every piece of data is unique, it is converted into an equally unique hash string.

The intent of these amendments is to pacify the need for a witness at trial, pursuant to Rule 901, to certify the authenticity of electronic documents.

The Federal Rules Advisory Committee found that in many cases, a party hires an expensive authentication witness, and then the opposing side either designates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. Instead of calling a live witness, proposed Rules 902(13) and 902(14) allow the proponent to present a certificate by a qualified person to verify the authenticity of the electronic evidence.

The big question is, who is a qualified person? It is recommended that the individual who collects this information be certified or under the supervision of an individual who is certified in the collection of electronically stored information using a specific mining and authenticating software, and who can provide an affidavit on the collection of this information.

The Advisory Committee's notes clarify that certification under this rule can only establish that the proffered item is authentic. The opponent may object to the admission of the internet content as evidence on other grounds, including hearsay or relevance. It will be important and interesting in the next year to see how this information is used. Stay tuned!

Thom Kramer is director of marketing and business development at Marshall Investigative Group and has been involved in the insurance investigative industry for more than 25 years. Thom has been a featured subject matter expert at trade conferences, association meetings and on national and syndication television shows including CBS's The Early Show and Real TV.