MOBILE DEVICES
NEW CHALLENGES FOR ADMISSIBILITY OF ELECTRONIC EVIDENCE

As mobile devices, social media, and web archives change the nature of digital evidence, will the courts be able to address the increasing complexity?

BY LUCY L. THOMSON

The Changing Digital Evidence Landscape

In the future, the most important evidence may be created on a mobile device. Information technology has caused a paradigm shift in the way individuals and organizations communicate—and create, collect, share, and store—data and information. Advanced technologies ranging from mobile devices to satellites¹ are providing sophisticated ways to document daily events, resulting in an expansive collection of invaluable records. Millions of people are now creating documentation that may become “evidence” in cases around the world.

Observers on the scene can now document the details of events with photographs, video, and audio recordings from their cell phones and cameras, and postings of real-time commentary (often transmitted through their mobile devices) on websites such as YouTube, global social media sites, and Twitter and in email and text messages—previously unavailable real-time, up-to-the-minute recordings. Now in court proceedings, traditional eyewitness testimony can be greatly enhanced and corroborated by introducing digital evidence. Adding to the layers of complexity, web archives are being created by global organizations; regular captures are being made of websites, and the digital material is being saved and preserved for the future.²

The widespread use of mobile devices has created unprecedented challenges in legal proceedings as the courts decide how to properly authenticate digital information under the current judicial rules and procedures. Although the basic legal requirements for establishing a foundation for admissibility of evidence in US courts are well-established, their applicability to digital data and devices from which electronic evidence is generated raises many difficult evidentiary issues and questions. As a result, courts have applied widely different standards for similar types of evidence when computer-generated information and digital images are presented in court.

Twenty-First Century Foundations of Digital Evidence

Court rules require that for evidence to be admissible, it must be authenticated. In the simplest terms, this means that data and information must be shown to be what the proponent claims that it is.³ The foundations for digital evidence are based on established principles of authentication and admissibility that originated with the use of “paper” evidence. The five separate foundations are:⁴

- **Relevance**—the evidence must be relevant to the claims asserted, i.e., it must have “any tendency” to prove or disprove a consequential fact in the litigation.
- **Authenticity**—a process for establishing that digital data or a document is what it represents.
- **Hearsay**—an out-of-court statement introduced for the truth of the matter asserted; it applies if the proponent plans to use the record’s contents as substantive evidence. The evidence must not be hearsay, or it must be admissible under a hearsay exception.
- **Best Evidence**—this standard applies if the document’s terms are at issue; there are no “origins” of digital evidence.
- **Probative Value Must Outweigh**
Any Prejudicial Effect—a court may exclude relevant evidence under Rule 403 if its probative value is substantially outweighed by the danger of unfair prejudice, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.

While US courts have been admitting computer records into evidence since the 1970s when computer systems became available for business and some personal use, “traditional” foundations for electronic evidence have focused on the relationship between the information and the computer. Documents were admitted based on the assumption that information produced from a computer is inherently reliable.

The standard for the admissibility of evidence generally has a low bar under Fed. R. Evid. 901(a). It is only necessary to establish a foundation from which the fact-finder (a jury) could legitimately infer that the evidence is what the proponent claims it to be; for example, that a letter is genuine or a photograph is accurate. The trial judge looks only to the proponent’s evidence to assess the rational sufficiency of the foundational evidence, a question of law. The opponent may have controverting evidence. Thus, for digital evidence to be admissible, it must be shown only to be arguably or colorably authentic.

Now that the nature of digital evidence is significantly different from the early days of mainframe or stand-alone computers, traditional foundations for computer records may no longer be adequate to address the complexities
THE FAILURE TO UNDERSTAND HOW TO APPROPRIATELY AND EFFECTIVELY AUTHENTICATE ELECTRONIC EVIDENCE HAS RESULTED IN ADVERSE RULINGS BY FEDERAL COURTS.

require advance planning to systematically document these key aspects of the electronic evidence.

Advanced Technology Trends
Much of today’s information is created in electronic form (“born digital”), and a large percentage is never printed. Consider the challenges to authentication presented by each of the following technology developments that have taken place in recent years:

- A mobile transformation is upon us. The proliferation of mobile devices results in the creation and transmission of huge amounts of digital information through a variety of devices, including laptops, smartphones, and tablets. New and enhanced functionalities of these devices also expand significantly the types of data that are created, particularly with mHealth, mBanking and global e-commerce.
- In many cases, email and social media have become predominant means of communication, along with text messages, chat groups, and blogs. Millions of people are members of social networks, where complex relationships between and among individuals and businesses are documented in a constantly changing tapestry of text, audio, and photographic images. Few rules govern the attribution of these data to their sources, and changes to the information are often not logged or documented.
- The trend toward consumerization of information technology—often referred to as Bring Your Own Device (BYOD)—means that individual users will be permitted to connect their personal consumer devices, including laptops and mobile devices, to company networks and use them for both business and personal reasons.
- Because of cost reductions and increased efficiencies, many organizations are outsourcing their information technology to cloud service providers. Outsourcing data storage and analysis to third parties adds another layer of complexity to the authentication process. Furthermore, information systems are international in scope as a result of globalization and industrial consolidation.
- Web archives consist of collections of many websites with material created in the past, which presents significant challenges for establishing a foundation for admissibility. A foundation for each “layer” of evidence must be provided separately, including the chain of custody.

Challenges to Digital Evidence in Legal Proceedings
The failure to understand how to appropriately and effectively authenticate electronic evidence has resulted in adverse rulings by federal courts. For example, in Lorraine v. Markel American Insurance Co., 241 F.R.D. 554 (D. Md. 2007), the court denied a motion for summary judgment due to the failure to provide admissible evidence and properly authenticate computer-generated evidence. In Vinhnee v. American Express Travel Related Services Company, Inc., 336 B.R. 437 (9th Cir. BAP 2005), the court of appeals affirmed the trial court’s decision not to admit computerized records because of the lack of foundation for business records and an authentication foundation to assure the accuracy of the records.

There are several challenges that can be made to the authenticity of digital records:

- Identity Management Challenge: Who Is the Author of the Records? Courts look for ways to tie the author to the digital information offered into evidence. Whether a message, document, video, or photo was included in an email or...
posted on a website, it is important for the proponent to provide testimony about who the author is.

- **Is the Computer Program That Generated the Records Reliable?** Was the output of the computer what it is purported to be?

- **Were the Records Altered, Manipulated, or Damaged After They Were Created?** Changes to photographs and videos can be made using Photoshop or graphic design programs, while hackers can alter websites, change databases, and other electronic media. Often they cover their tracks by changing audit log records.

- **Incompleteness and Integrity.** Is the evidence the entire record or conversation? In a challenge to the authenticity of email transcripts, “instant messages,” and “chats,” a court held that “obvious omissions” in some of the communications go to the weight rather than the admissibility of the evidence. *U.S. v. Lebowitz*, 647 F. Supp. 2d 133 (N.D. Ga. 2009). However, a Nebraska federal court excluded entirely a “cut-and-paste” version of chat room conversations, finding that the omissions made the evidence “not authentic.” *United States v. Jackson*, 2007 WL 1381772 (D. Neb. 2007).

To address these issues, the courts have created three approaches to determine the admissibility of digital evidence. While they were created in the context of websites, they are applicable to information from all types of digital evidence.

- **Strict.** A witness with personal knowledge must testify that the information can be attributed to a particular person or organization. The testimony will address, e.g., who maintained a website where information was posted and who authored the document.

- **Somewhat Strict.** Whether linking the information to the website’s sponsor is required depends on the circumstances, such as the proponent’s incentive and ability to falsify evidence—in some cases, it is necessary to prove that the website owner actually posted the information.

- **Lenient.** A web page is introduced through a screen shot—testimony from the person who created the screen shot is required stating that the image “accurately reflects the content of the website and the image of the page on the computer at which the [screen shot] was made.” The party seeking to introduce the evidence does not need to show who authored or sponsored the information.

There appears to be no uniformity as to which standard will be applied. Courts often make a cursory assessment and admit evidence such as email based on its appearance; does it have “indicia” of reliability (familiar format, signature line, company identified, etc.)? From a technology standpoint, using the lenient standard based on the appearance of a website or email is not a reliable indicator of whether the evidence is authentic. The data can be easily forged or altered by a hacker, developer, or a layperson. When forwarding an email, the sender can edit the message. Such alterations are often not detectible by the recipient.

The content of a website introduced into evidence may not be authentic for several reasons, including: (1) It can be forged by saving the website to a local computer hard drive. The content can then be redisplayed in a browser, modified by a text editor, and printed from a substituted URL. (2) Websites are dynamic and may display different content to different users. Websites that have been infected with a virus may display malicious content to the user only once. (3) The website may change its content slightly in seconds, so it may not be possible for the witness to preserve every word of the page. (4) A hacker attack can make a website statically or dynamically display any content the hacker wishes to present.

**Authentication of State Official Records**

Web pages can be generated from official government websites; they are self-authenticating and admitted as evidence, even though in a major report published in 2007 by the American Association of Law Libraries (AALL) casts serious doubt on the authenticity of official records obtained from state websites. In 2011, the Uniform Law Commission passed the Uniform Electronic Legal Material Act (UELMA) to address these shortcomings. It will not be until states pass UELMA, and official publishers authenticate online legal material, that this problem is fully addressed.

**Information From Social Media Sites**

The explosion of participants in social networking venues such as Facebook, MySpace, and LinkedIn has resulted in the creation of information that is outside the knowledge and control of any specific person or organization. Courts generally apply a stricter standard to authentication of information from social networking sites because of the absence of restrictions on who may create or update a profile. Anyone can create a social network profile anonymously, using a pseudonym, or in someone else’s name. Because one or many people may post messages on a social networking site, courts cannot necessarily attribute a particular message to the person who owns the site. Determining who made a post is particularly difficult if the person made the post from a public computer such as in a library or a hotel.

**Authentication Criteria**

In order to demonstrate that the digital evidence is what the proponent claims it to be, the foundation must take into account not only the legal requirements of procedure and evidence, but must also include an evaluation of each of the key components of the information system from which the evidence...
was generated. The rigor with which an evidentiary foundation must be established depends on the purpose for which the electronic information is being offered into evidence, whether there is any reason to believe the evidence is not authentic, and the extent to which the data and information can be corroborated.

Purpose for Offering the Evidence

Decisions about admissibility will usually turn on the purpose for which the evidence is being offered. The complexities of modern business information systems and global communications technology make it essential that litigators and the courts understand the context in which each piece of digital data is created, stored, and transferred. Often the accuracy of the information is not at issue, and the evidence may be properly admitted for a valid purpose, such as:

- for the truth of the matter asserted
- to show knowledge, notice, or intent
- habit
- motive, intent, scheme, or plan
- whether the alleged acts actually occurred
- mental state
- attitude
- exact numbers or patterns, probabilities, and trends.

Likelihood the Evidence Has Been Altered or Falsified

Has a challenge to the authenticity of the evidence been made? If fraud, forgery, or destruction of evidence is a central issue in the case, a jury would decide issues about electronic evidence just as it would in a similar case involving paper documents. It will be necessary to consider whether the information system was correctly designed, configured (firewalls, audit and logging), and maintained (patches). Evidence of the information security safeguards in place is one aspect of a showing that the data have not been changed or falsified. Many computer systems have sophisticated audit logging systems to track and record information about users and their transactions, as well as integrity checks and information security built in to ensure the data are accurate, important for authenticating electronic evidence. Forensic analysis may be required to assess the more sophisticated aspects of device and information system operations.

How Can the Electronic Evidence Be Corroborated?

Corroborated is an essential tool for the successful presentation of electronic evidence. This can be done through a combination of witness testimony and documentary and physical evidence that address particular points in the case, and take into account the content and context of the evidence. For example, consistent testimony by unrelated witnesses about a particular event can indicate reliability.

Chain of custody. Documentation for each piece of evidence should be created and maintained to record each step in the digital evidence life cycle to the extent practicable. Thereafter, issues relating to chain of custody and the need to maintain careful documentation of the collection and maintenance of digital information must be addressed. Actions taken in response to or consistent with an email, text message, or social media post can provide indicia of reliability. If the purported author/sender was the only one likely to know the information in a message, it may be assumed to be accurate.

A Deeper Understanding of New Technologies Is Needed

In the digital age, there are many ways to cast doubt on the authenticity of electronic evidence. Although the courts continue to grapple with the authenticity of digital evidence, including email, websites, website information, and social media, most courts—on whatever grounds—have found the information admissible. Indeed, notwithstanding the genuine risk of unreliability due to hacking or other malicious changes, the courts continue to admit such information into evidence. As the volume of digital evidence continues to grow exponentially and its importance to the outcome of cases remains critical, a deeper understanding of the nature of these records will be required to make meaningful decisions about its authenticity. Sound and informed information governance practices must be adopted to determine whether the evidence fulfills the legal requirements for authenticity, reliability, and integrity.

MOBILE DEVICES AND ENERGY

BY GREGG MARYNIAK

When people think about the potential for mobile devices to impact the energy world, what often comes to mind are things like using one’s cell phone to remotely control home systems, like heating, cooling, and lights. These are certainly useful gadgets, but probably don’t rise to the level of transformational change. However, the proliferation of small mobile devices is now outpacing traditional desktop and laptop computers, and we are seeing technology develop in new directions to keep pace with market needs. As mobile customers worldwide demand improved battery life, this demand is helping spur better energy storage systems (such as the use of nanotechnology to make high surface area electrodes).

The transformational impact created by cell phones and other small mobile devices may well be the driving trend observed by Jonathan Koomey of Stanford University, which is now referred to as Koomey’s Law. Koomey related the increase in energy efficiency in computing to the decrease in energy cost per computation. Mobile devices by virtue of their reliance on small batteries will push this trend beyond present limits.

Gregg Maryniak is the chair of energy and environmental systems at Singularity University.