



Don't Believe Everything You Hear

Digital recordings don't show the same signs of tampering

In 1975, Gerald Ford was president of the United States, the Vietnam War was coming to an end, Jimmy Hoffa was reported missing, and with the release of the first microcomputer, the Altair 8000, the home computer revolution commenced. This was also the year the Federal Rules of Evidence (FRE) were enacted, which is why it is not surprising the FRE did not contemplate digital technologies or the role they would play in litigation.

In the mid-1970s, audio recordings were entered into evidence primarily in the form of magnetic audiotape recordings. If an individual was going to falsify the evidence, he might splice a tape or make a new recording from the original recording. To remove portions of the tape or to add new tape, the falsifier would make a physical cut in the tape, add or remove the segment in question, and then put the tape back together with splicing tape. If the falsifier attempted to introduce this recording into evidence, upon examination, the splice would be visible or there would be a resultant dropout of sound, making it difficult or impossible for the falsifier to convince the court that the recording was genuine.

If the falsifier doctored the original recording and then transferred it to another tape to circumvent the problems associated with splicing, he would have other issues with which to contend. This rerecording or copy tape would be, at minimum, a second-generation recording, and deterioration in the quality of the recording would be expected. This deterioration, depending on the extent, might be an indication of tampering.

Additionally, the copy tape would not have the expected magnetic artifacts, called event signatures, that are caused by the energizing and de-energizing of record and erase heads on an audiotape recorder. These event signatures could be used by an expert to determine if a recording was made in a manner consistent with the protocol described by the person who made the recording, and could provide clues as to whether the recording had been edited during production.

With digital audio recordings, however, event signatures are weaker in amplitude, if they exist at all, and with editing software, the artifacts can be removed entirely. Digital recordings also obviate the need for splicing. Because digital information can be so easily manipulated without physical signs of tampering, producer Michael Perna believes we have entered an era in which,

"you can't believe anything you see or hear anymore."

As the proliferation of digital technologies continues, it may become increasingly difficult to distinguish between fiction and reality. Many current editing programs include tools such as spectrograms—the same tools used by experts to determine if an audio recording is authentic. As these products become more sophisticated, we can only expect the problem to become more pronounced.

In response, courts may find that, because digital audio recordings lack the indicia of trustworthiness magnetic audiotape recordings have, the probative value of digital

As the proliferation of digital technologies continues, it may become difficult to distinguish between fiction and reality.

recordings is so diminished, their introduction into evidence should be curtailed.

Attorney Richard Weissman believes part of the solution may lie in requiring the proponent of the recording to provide stronger foundational evidence before an audio recording is deemed admissible. Fausto Tito Poza, an audio forensic consultant, believes the types of expert witnesses may

evolve from those with linguistic backgrounds to those with backgrounds in computers, sound engineering or editing, and computer hacking.

With the bar to admissibility so low and the functionality of digital technology so advanced, the chasm between is a Pandora's Box that the drafters of the FRE could not have anticipated. In becoming aware of the magnitude of the problem, the technology community has an obligation to move forward responsibly as we continue to design products that have such a compelling impact on the public.

Perhaps the answer lies in serial numbers, time coding, or additional metadata being compiled in editing software. Or, just as there are disposable cameras, perhaps we can create a disposable recorder designed specifically for individuals in anticipation of litigation. The recorder might have an internal time/date stamp that cannot be modified so that, even if the person making the recording took the recording off the recorder for editing and then put it onto a disposable recorder, the time/date stamp would preclude the fabricator from falsely testifying as to when the recording was made.

To listen to two recordings to see if you can tell which, if either, was manipulated, go to www.comptalk.com and click on the Resources tab. ☒

Robin Springer is the president of Computer Talk (www.comptalk.com), a consulting firm specializing in the design and implementation of speech recognition and other hands-free technology services. She can be reached at (888) 999-9161 or contactus@comptalk.com.