Loyola Law School
Loyola Marymount University
Los Angeles

919 Albany Street
Los Angeles, California
90015

T 213.736.1028
C 818.648.8137
F 213.736.1001
www.lls.edu

LITIGATION STRATEGIES FOR DEALING WITH "DEEPFAKE" EVIDENCE IN FEDERAL COURT

Professor Rebecca A. Delfino
March 11, 2025

For a century, people have altered photographic images and audio recordings. But within the last three years, the advent of new computer aided- technologies has allowed people to take such manipulation to new heights-to create such convincing images and audios that it is nearly impossible to discern the real from the fake.

Modern "deepfake" technology combines genuine audio, pictorial images, or video footage with artificial intelligence, allowing the creator to make believable new footage or audio ostensibly depicting a person saying or engaging in conduct that the person never did or said. The deepfake creator generates an algorithm trained to recognize patterns in actual audio or visual recordings of a particular person, a process known as deep learning. As with doctored images, a piece of content can be altered by swapping in a new element--such as someone else's face or voice--and joining the two. Software exists to allow the editing of the video to make a person "say" whatever you want only by typing the text. The term "deepfake" emerged in November 2017 when a user on the website Reddit published fake videos along with the algorithm used to create them. Since then, deepfake technology has increased. It is now available through common mobile applications like FaceApp.

Perhaps the most famous example of a recent deepfake video depicts former President Barack Obama, whose image and voice were used by filmmaker Jordan Peele and BuzzFeed CEO Jonah Peretti to create a tongue-in-cheek public service announcement about the danger of deepfakes.

The presentation of deepfake evidence creates an emerging challenge for the legal system. How will litigators, judges, and juries determine whether evidence is real or fake? The presentation of deepfake evidence presents a unique challenge to our judicial system's core functions: adjudicating facts and finding the truth.

The current legal system provides tools for identifying and challenging potential deepfakes the opposing party seeks to present.

- **Propound Specific and Precise Discovery Requests**

Testing the authenticity of all video or audio evidence begins with discovery. First, request the production of the complete video or audio at issue and use modern civil discovery tools to investigate the authenticity.

Propound interrogatories to obtain specific information about the audio and video recordings, such as the source of the recording, the steps taken to create the recording, the details concerning the chain of custody, whether other similar recordings exist, and the identity of any

Professor Rebecca Delfino
Rebecca.Delfino@lls.edu

persons with knowledge about the content of the recording. Such interrogatories should seek the following:

> *For the video previously produced, please provide (1) the time, place, and date the recording was made; (2) the name and address of any individual depicted in or present at the time of recording; (3) the name and address of any individual under whose direction and upon whose behalf the recording was created; (4) the name and address of any other individual involved with the creation of the recording; (5) the steps undertaken by the identified individuals to create the recording; and (6) the name and address of any individual who has had possession or control of the recording (either the original or a copy) since it was created.*

The response to this interrogatory may be followed by requests for the production of metadata, interrogatories, or depositions of custodians or witnesses to the video's events.
If counsel suspects the video or audio was fabricated, the duty of competency may require counsel to engage forensic experts to evaluate the evidence. Depending on the video's content and the case's value, consider hiring an expert who can dig for forensic clues of the recording's origins.

- **Be Aware of Authentication Rules and Other Rules of Evidence**

Litigating authenticity under the Federal Rules of Evidence centers on the 900 series.

- **FRE 901(a)** states that the proponent of evidence "must produce evidence sufficient to support a finding that the item is what the proponent claims it is."
- **FRE 902** provides that certain items of evidence are "self-authenticating; they require no extrinsic evidence of authenticity to be admitted."

Additional sections of Rule 902 address electronically stored information.

- **FRE 902(13)** allows authentication of a record "generated by an electronic process or system that produces an accurate result" if "shown by the certification of a qualified person" that complies with specific requirements.
- **FRE 902(14)** allows authentication of data "copied from an electronic device, storage medium, or file if authenticated by process of digital identification, as shown by a certification of a qualified person" if authenticated "by process of digital identification, as shown by a certification of a qualified person" that meets those same requirements.

Some courts have permitted counsel to authenticate video or audio evidence under the "silent witness" theory. Under this approach, the foundation focuses on the automatic operation of the recording device. It does not consider a witness's observations of the recorded events because the "recording speaks for itself."[1]

---

[1] *State v. Moyle*, 532 S.W.3d 733, 738 (Mo. Ct. App. 2017) (discussing the silent- witness theory and stating that "[i]n determining whether a proponent of this type of video or photographic evidence has satisfied th[e] foundational standard, a trial court should consider... whether the recording in the medium presented at trial is a fair and accurate portrayal of the recording in its original form and has not been altered, tampered with or modified (or that any alteration or

Loyola Law School
Loyola Marymount University
Los Angeles

919 Albany Street
Los Angeles, California
90015

T 213.736.1028
C 818.648.8137
F 213.736.1001
www.lls.edu

Even though the silent witness theory relaxes the chain-of-custody requirements for authenticating videos, many courts may still require additional evidence or testimony to demonstrate authenticity and competency, including proof that the evidence was not altered. A trial judge may consider any evidence of editing or tampering before admitting a recording under the silent witness theory. Consequently, litigators can attack a deepfake, even if presented under the silent witness theory. For example, an expert witness who has identified an issue with a recording's metadata may be used to convince the trial court that the other side cannot rely on the silent witness theory but must present a chain of custody evidence to establish authenticity.

Other Rules of Evidence to Consider:

- **FRE 401 and 403**: In evaluating whether the recording is more prejudicial than probative, a lawyer may ask the court to consider if verifying the video's integrity causes undue delay and confuses the jury with irrelevant matters of a technical nature.
- **FRE 801, et seq.:** While a recording generally would not be considered a declarant for purposes of the hearsay rules, a lawyer should consider whether the individuals depicted in the recording are available to testify and whether it would be more advantageous to evaluate the reliability of such testimony. Additionally, a lawyer should analyze whether hearsay within the recording is not subject to an exception.
- **FRE 106:** and relatedly, the rule of completeness: Requiring the opposing party to produce the entire video or audio recording may offer data not initially available (or not produced during the discovery phase) that assists the lawyer in the evaluation of a recording's authenticity.
- **FRE 1002:** If an opposing party seeks to prove the recording's content, a lawyer should insist that the original recording be produced so it can be analyzed appropriately. Otherwise, in accounting for the original's absence, an opposing party may reveal some detail that speaks to the data's integrity.

- **Pretrial Motions in Limine:**

If you suspect your adversary will attempt to authenticate audio or video evidence without a witness to authenticate it, consider filing a pretrial motion to cast doubt on the authenticity. Raising this motion before trial will allow you to litigate the matter before the trial, saving time and resources.

If you raise credible concerns about the evidence, the judge is likely to conduct an evidentiary hearing to explore the creation of the evidence and its chain of custody. If the judge concludes the evidence has been exposed as a fake, it will likely be excluded. However, if the issue is too close to call, then the judge may allow the opposing party to offer it. Still, the court may also conclude that the process that created the evidence does not justify self-authentication under Rules 902(13) and (14). Instead, the judge will probably require the party to offer to present

---

modification is sufficiently explained and does not affect the reliability or accuracy of the evidence)").

Professor Rebecca Delfino
Rebecca.Delfino@lls.edu

a "qualified person" to testify about the evidence, how it was created, and how it was handled along the way.

- **Using Examination Techniques in Deposition and at Trial**

If you have not excluded potential deepfake evidence before trial, you must convince the jury that the video or audio is fake evidence. This is achieved first by deposing the individual your opponent offered to authenticate the evidence and later by cross-examining that witness during the trial.

Traditionally, jurors believed that the camera did not lie. However, given the increasing exposure of the public to technology, artificial intelligence, and the intentional manipulation of images in social media and entertainment, the public's perception of digital images has shifted. Increasingly, potential jurors have become more skeptical of the authenticity of digital images. If you have succeeded in convincing your judge that a witness is required to establish a recording's authenticity, then cross-examination is your chance to change the case's narrative and build the jury's skepticism about your opponent's evidence.

At a minimum, you will want to highlight what the witness knows about how the recording was made, collected, and passed on and significant gaps in the witness's knowledge. Consider such lines of inquiry as:

- ► Can the witness account for the video's whereabouts from inception to delivery?
- ► Did the witness create the technology that captured the recording and thus has an incentive to overstate its accuracy?
- ► Does the witness stand to gain if the video is authentic or to lose if it is inauthentic?
- ► Do portions of the recording not add up? Also, the witness's background and others in the chain of custody should be investigated.
- ► What is their technical sophistication?
- ► Have they altered videos before?
- ► Do their social media posts show videos altered or doctored?
- ► Do they own any applications for altering recordings?

When critical video integrity has been questioned, its authenticity will likely be the trial's fundamental question.

- **Using Expert Testimony**

Once jurors realize that the parties are disputing the veracity of a video or audio recording, the issue is likely to require expert testimony. Experts can be a powerful tool for explaining to a jury that evidence should (or should not) be trusted; they may help explain that evidence was developed using deepfake technology. If you argue that a recording is fake, you will want an expert who believes it is fake and can explain to the jury why.

- **Making a Record**

A lawyer who loses the argument to exclude a video may choose not to pursue the issue in front of the jury, especially if the video is not case critical. However, that does not mean lawyers

Loyola Law School
Loyola Marymount University
Los Angeles

919 Albany Street
Los Angeles, California
90015

T 213.736.1028
C 818.648.8137
F 213.736.1001
www.lls.edu

should abandon the issue entirely if the judge overrules the objection. Instead, preserving everything – the complaint and all forensic evidence collected is essential.

Technology and the law continue to evolve. Keep in mind that if technology unavailable at trial emerges and allows uncovering definitive evidence of a deepfake within one year of the judgment, previous ruling on the evidence may be set aside under Federal Rule of Civil Procedure 60(b). Therefore, lawyers should ensure that everything is preserved.

- **Final Thoughts**

As deepfake technology proliferates, it is becoming increasingly important for attorneys to learn how to use our legal system's existing tools for identifying and challenging questionable audio or video evidence.

Although these approaches are helpful, they do not resolve the matter. As deepfake technology proliferates, the judiciary, bar regulators, and the legislature must comprehensively address ethical questions and legal remedies. The federal judiciary should consider amendments to the FRE and the rules of procedure to expressly address the admission of deepfake evidence.[2] In addition, legislation may be drafted to strengthen the government's ability to punish (i.e., through copyright infringement, defamation, and criminal actions) those who use deepfake videos to conduct nefarious activities.[3] In the meantime, lawyers should vigorously deploy the tools available to preserve the judicial process's integrity by ferreting out and exposing potentially forged recordings.

[2] See Rebecca A. Delfino, *Deepfakes on Trial: A Call to Expand the Trial Judge's Gatekeeping Role to Protect Legal Proceedings from Technological Fakery*, 74 HASTINGS L.J. 293 (2023).
[3] See Rebecca A. Delfino, *The Deepfake Defense—Exploring the Limits of the Law and Ethical Norms in Protecting Legal Proceedings from Lying Lawyers*, 84 OHIO ST. L.J. 1068 (2024); Rebecca A. Delfino, *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act*, 88 FORDHAM L. REV. 887 (2019).