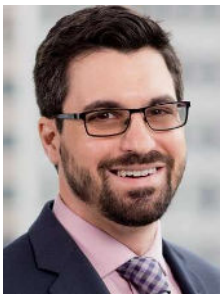
The Other Side Says Your Evidence Is A Deepfake. Now What?

By **Matthew Ferraro and Brent Gurney** (December 21, 2022)



Matthew Ferraro

Brent Gurney

In several recent high-profile trials, defendants have sought to cast doubt on the reliability of video evidence by suggesting that artificial intelligence may have surreptitiously altered the videos.

These challenges are the most notable examples yet of defendants leveraging the growing prevalence in society of AI-manipulated media — often called deepfakes — to question evidence that, until recently, many thought was nearly unassailable.

There are two central concerns about deepfakes in the courtroom. First, as manipulated media becomes more realistic and harder to detect, the risk increases of falsified evidence finding its way into the record and causing an unjust result.

Second, the mere existence of deepfakes makes it more likely the opposing party will challenge the integrity of evidence, even when they have a questionable basis for doing so. This phenomenon, when individuals play upon the existence of deepfakes to challenge the authenticity of genuine media by claiming it is forged, has become known as the "liar's dividend," a term coined by law professors Bobby Chesney and Danielle Citron.[1]

Attorneys and scholars have for years warned of the dangers to the judicial process of highly believable yet phony media.[2] Recent experience has revealed the extent of these threats, particularly to cast doubt on accurate evidence.

For example, in August, Joshua Christopher Doolin, who is scheduled to stand trial in March 2023 in the U.S. District Court for the District of Columbia[3] on assault and other charges related to the Jan. 6, 2021, riot at the U.S. Capitol, refused to stipulate that open-source videos of the Capitol cited by the prosecution were authentic.[4]

The government sought in a motion in limine[5] to authenticate videos of the defendant accessible on YouTube pursuant to Federal Rule of Evidence 901(a).

Doolin objected, despite what he conceded was the low threshold for establishing authenticity, because, "given the recent technological advances, relying on open-sourced media with no evidence of a chain of custody should not even meet this low threshold."

Doolin argued that the "widely available and insidious" technology to create deepfakes "allow people to appear to say just about anything."

He cited 2017 deepfakes of former President Barack Obama and a 2019 manipulated video of U.S. House of Representatives Speaker Nancy Pelosi as grounds for the court to deny the government's request "until they can support the circumstantial evidence they claim to possess."[6]

The government responded that circumstantial evidence provided a prima facie basis to believe that the open-source video was authentic. This included "several distinctive

comparison points" with surveillance footage from the U.S. Capitol Police, body camera footage from the Metropolitan Police Department, and the open-source video.[7]

The government did not dispute that the deepfake technology of which Doolin warned exists, only that his "argument goes to the weight of the video evidence, not its admissibility."[8]

The court has yet to rule on the motion in limine.[9]

A second example involves another Jan. 6 defendant, Guy Reffitt, who was convicted at trial in District of Columbia federal court on five counts: transporting a semiautomatic pistol in furtherance of civil disorder; obstructing an official proceeding; entering or remaining in a restricted building with a firearm; obstructing officers during a civil disorder; and obstruction of justice through force or the threat of force.[10]

During his trial, prosecutors showed jurors several pieces of digital evidence, including messages, photos and videos of the riot that Reffitt shared with his family and with members of the Texas Three Percenters group.[11]

FBI Special Agent Stacy Shahrani testified for the prosecution about her analysis of the defendant's electronic devices, including a 360-degree video from a helmet-mounted camera Reffitt wore on Jan. 6,[12] on which Reffitt could be heard shouting that he was "packing heat"[13] and declaring his intention to "take the Capitol" and "pull legislators out by their hair."[14]

On cross-examination, Reffitt's counsel asked Shahrani if she had heard about deepfakes.[15] Shahrani said she had heard of deepfakes but was "woefully underprepared to answer any questions on it."[16]

The government objected. The judge asked the defense counsel for his good faith basis for the questions, allowing the questioning to proceed after Reffitt's counsel said he was going to ask Shahrani if any of the government's digital exhibits had been altered.[17]

Shahrani said she was aware of deepfakes from her work on FBI child pornography investigations.[18] Asked if she had any reason to believe any of the images introduced into evidence were deepfakes and if she had checked the videos to see if they were, Shahrani said there was no reason to believe the images were deepfakes and that she "check[s] for things that are there, not for things that are not there. So no, [she] wasn't checking for it."[19]

Reffitt's counsel asked no further questions of Shahrani. Subsequently, Reffitt was convicted of all charges and sentenced to more than seven years in prison.[20]

Third, according to press reports, during the November 2021 homicide trial of Kyle Rittenhouse in Kenosha, Wisconsin, the prosecutor sought to play for the jury footage on an iPad of the defendant fatally shooting Joseph Rosenbaum. The prosecutor indicated he would use the pinch-to-zoom function on the iPad to present a larger image to the jury.[21]

Rittenhouse's counsel objected, arguing that the iPad uses artificial intelligence and "logarithms" — presumably, he meant algorithms — "to create what [the algorithms] believe is happening. So this isn't actually enhanced video, this is Apple's iPad programming creating what it thinks is there, not what necessarily is there."[22]
The attorneys and Wisconsin circuit court Judge Bruce Schroeder argued over the objection

for ten minutes. The prosecutor said jurors would understand that zooming in on Apple products is routine and does not affect the integrity of the image, arguing the defense should have to present expert testimony that the image was adulterated.[23]

Judge Schroeder sided with the defense, ruling that the prosecution had the burden of proving that the Apple iPad does not use artificial intelligence to manipulate footage.

The judge gave the prosecution a 15-minute recess to locate an expert to testify that the zoomed-in image was "in its virginal state."[24] The prosecution did not produce a witness to testify to the veracity of the zoomed-in media and instead showed the jury "the original, zoomed-out clips on a Windows machine hooked up to a large TV in the courtroom" that did not fill the entire screen, according to The Verge.[25]

Rittenhouse was subsequently acquitted of all charges.[26]

Finally, in March 2021, a Pennsylvania district attorney charged a woman for online harassment and alleged publicly that the defendant disseminated deepfake videos[27] of members of her daughter's cheerleading team in states of undress and drinking and vaping, in violation of team rules.[28]

But two months later, the police dropped the deepfake allegation, conceding that there was insufficient evidence to show that the videos were faked.[29]

It appears that they were not, and that the students and their parents claimed they were deepfakes to avoid embarrassment.[30]

While the prosecutors abandoned the deepfake allegations prior to trial, this episode points to the dangers of litigants' claims about cutting-edge manipulation running ahead of the facts.

Approaching the Challenges of Deepfakes

In light of these examples, how should courts and litigants approach the challenges of deepfakes?

The Federal Rules of Evidence set the standards for the authentication of multimedia evidence, and courts will apply them or their state analogs when assessing questions around AI-manipulated media, such as deepfakes. Where litigants have genuine concern about the veracity of media, they can challenge admissibility under various rules of evidence on the basis that the evidence may have been faked.

As an initial matter, Federal Rule of Evidence 901 requires that the proponent of evidence show that such evidence is what it purports to be.[31] The rule then provides a nonexclusive list of ten examples of how this can be done, including by introducing testimony of a witness with knowledge that an item is what it is claimed to be and by using the distinctive characteristics of the evidence itself "taken together with all the circumstances."[32]

Evidence, such as open-source video, can also be compared with "an authenticated specimen by an expert witness or the trier of fact."[33]

Two Federal Rules of Evidence, 902(13) and 902(14), aim to simplify the process of admitting video created with verified-capture tools.[34]

Rule 902(13) allows for the authentication of a "record generated by an electronic process or system that produces an accurate result," if "shown by a certification of a qualified person" in a manner set forth by the rules.[35]

Rule 902(14) allows for the authentication of "[d]ata copied from an electronic device ... by a process of digital identification, as shown by a certification of a qualified person."[36]

Both rules require advance notice and an opportunity to challenge the record. Specifically, they require the proponents to meet notice requirements of Rule 902(11), which states that "[b]efore the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record — and must make the record and certification available for inspection — so that the party has a fair opportunity to challenge them."[37]

If the certification requirements are met, a party need not call a testifying witness at trial to establish authenticity. But if an expert is needed, judges will need to weigh competing expert testimony over the authenticity of media.[38] The evidence must still comply with other rules of evidence concerning admissibility, such as for hearsay.[39]

As is always the case, the American Bar Association's Model Rules of Professional Conduct are clear that an attorney may "not knowingly ... offer evidence that the lawyer knows to be false," like a deepfake.[40]

If he or she comes to know that evidence offered by a client or witness is false, the lawyer "shall take reasonable remedial measures," including disclosing that fact to the court.[41] And an attorney "may refuse to offer evidence ... that the lawyer reasonably believes is false," such as a video he or she reasonably believes to be manipulated.[42]

But the possibility that deepfake media may be submitted as unadulterated evidence does not give litigants carte blanche to baselessly question evidence. According to the ABA's Criminal Justice Standards for the Defense Function, "[d]efense counsel should not make objections without a reasonable basis."[43]

If litigants raise such questions without a good faith basis, they risk undermining "the public's understanding of and confidence in the rule of law and the justice system," in the words of the Model Rules of Professional Conduct.[44]

Doing so may violate professional rules against making frivolous arguments, baselessly denying factual contentions, or engaging in harassing, delaying or costly motion practice.[45]

At the same time, counsel must balance their ethical duties with zealous advocacy in challenging evidence when there is good reason to do so. Under the Criminal Justice Standards for the Defense Function, defense counsel's investigation of the merits of criminal charges should

> include evaluation of the prosecution's evidence (including possible re-testing or re-evaluation of physical, forensic, and expert evidence) and consideration of inconsistencies, potential avenues of impeachment of prosecution witnesses, and other possible suspects and alternative theories that the evidence may raise.[46]

As it is, litigants will need to contend with the mere publicized existence of deepfakes and the doubts that can arise in the minds of jurors, even without egging on by counsel.

Riana Pfefferkorn, a research scholar at the Stanford Internet Observatory, has warned[47] of the potential for what she terms the "reverse CSI effect," which is "the phenomenon of jurors demanding high-tech evidence even in run-of-the-mill cases, thanks to the popular TV police procedural."[48]

Likewise, jurors

> may accord little weight to a video unless the proponent either proves the positive — by showing the video was captured via a video-authentication tool and thus should be considered authentic — or proves the negative, by using the latest detection technology (possibly at great expense) to satisfy the jury that the video is not a deepfake.[49]

Best Practices in a Post-Truth Age

How can litigants prepare for litigation in a post-truth age? In light of recent experience, consider the following best practices.

For Litigants Proffering Evidence

Follow Federal Rules of Evidence 902(13)-(14).

Rule 902(13) allows for the use of a certification to authenticate evidence generated by an electronic process or system, such as the contents of a website, data generated by a smartphone application, or records from a security system.

As Gregory P. Joseph, the past president of the American College of Trial Lawyers, has written, "[t]o make the certification more persuasive to the Court, it may be useful to point out other indicia of reliability in the certification."[50]

For example, if a litigant wants to authenticate the contents of a website, the certification may point out the website's distinctive design, that contents on the webpage remain on the site for the court to verify, that the owner of the website has published the same contents elsewhere, and the period of time the information was posted on the site, among other things.[51]

Likewise, Rule 902(14) authorizes a certification to authenticate a digital copy of data taken from a device or system, such as a mobile phone or hard drive.

As Joseph writes, this certification will be the product of technology; law enforcement often uses a device called Cellebrite, while other tools may be more discriminating and will limit extraction to certain categories of information, e.g., text messages or images.[52]

Do not take any evidence for granted.

Be prepared for challenges of what used to be relatively unassailable evidence. Be able to address questions regarding the evidence's chain of custody.

Provide circumstantial evidence to help establish the authenticity of open-source imagery and video.

Circumstantial evidence can provide context of where and when imagery or video was

taken, how it originated and whom it depicts.

This was the tack taken by the government in the Doolin case, and it is consistent with how some commentators have argued courts should approach proffered digital media.[53]

Prepare forensic witnesses to address questions around deepfakes.

While Reffitt was convicted, it would have behooved the government to prepare Shahrani for questions on deepfakes.

One imagines she could have assessed the evidence for indicia of AI manipulation and testified that, in her professional opinion, the evidence was not manipulated, instead of claiming on the stand that she "wasn't checking for" deepfakes and was "woefully underprepared to answer any questions on it."[54]

Be knowledgeable about the technology you are using.

In the Rittenhouse trial, prosecutors were caught flat-footed when defense counsel asserted that AI manipulated the pinch-and-zoom function on the prosecutor's iPad.

Knowing that similar questions may arise in the future, litigants should be prepared to explain the seeming magic of digital technology.

For Adverse Parties

Review disclosed evidence in advance of the trial.

As noted, the Federal Rules of Evidence require advance notice, disclosure and the opportunity to challenge records. Parties should leverage these opportunities to review media evidence for possible manipulation.

If media is questionable, consider retaining an expert to explain why it may be inauthentic.

As Pfefferkorn wrote, "the deepfakes arms race is sure to spawn a cottage industry, albeit a modestly-sized one, of expert witnesses who can assess disputed videos."[55]

It may be necessary, depending on the facts, for one or both parties to retain those experts.

Have a good faith basis to question any evidence.

As seen in the Reffitt case, judges will press litigants for the good faith basis for their questions about whether media evidence is a deepfake.

Attorneys should only engage in that line of questioning if they have a good faith basis to probe the veracity of the proffered evidence.

All attorneys must act consistent with the Rules of Evidence and with their duties under the Model Rules as public citizens with "special responsibility for the quality of justice" to zealously represent their clients, while not recklessly undermining the idea of epistemic truth in an era riven by heedless doubt.[56]

Matthew F. Ferraro is counsel at WilmerHale. He is also a senior fellow at the National Security Institute at George Mason University's Antonin Scalia Law School.

Brent J. Gurney is a partner at WilmerHale.

[1] Bobby Chesney & Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753, 1785-86 (2019).

[2] See, e.g., Matthew F. Ferraro & Suzanne E. Spaulding, Disinformation and Deepfakes, in The ABA Cybersecurity Handbook 391, 419-22 (Jill D. Rhodes et al. eds., 3d ed. 2022); Deepfakes, in The American College of Trial Lawyers Handbook of Electronic Evidence (Brent J. Gurney et al. eds., 2022); John Channing Ruff, Note, The Federal Rules of Evidence are Prepared for Deepfakes. Are You?, 41 Rev. Litig. 103, 108-14 (2021); Agnieszka McPeak, The Threat of Deepfakes in Litigation: Raising the Authentication Bar to Combat Falsehood, Vand. J. Ent. & Tech. L. 433, 435-40 (2021); Matthew F. Ferraro, Jason C. Chipman & Stephen W. Preston, Identifying the Legal and Business Risks of Disinformation and Deepfakes: What Every Business Needs to Know, 6 Pratt's Priv. & Cybersecurity L. Rep. 142, 151-52 (2020); Riana Pfefferkorn, "Deepfakes" in the Courtroom, 29 B.U. Pub. Int. L.J. 245, 275 (2020); David Dorfman, Decoding Deepfakes: How Do Lawyers Adapt When Seeing Isn't Always Believing?, 80 Or. State Bar Bull. 18, 22 (Apr. 2020); Riana Pfefferkorn, Too Good to Be True?, 73 NW Lawyer 22 (Sept. 2019); Matt Reynolds, Courts and Lawyers Struggle with Growing Prevalence of Deepfakes, ABA J. (June 9, 2020), https://www.abajournal.com/web/article/courts-and-lawyers-struggle-with-growing-prevalence-of-deepfakes; Theodore F. Claypoole, AI and Evidence: Let's Start to Worry, Nat'l L. Rev. (Nov. 14, 2019), https://www.natlawreview.com/article/ai-and-evidence-let-s-start-to-worry.

[3] Scheduling Order at 1, United States v. Doolin, No. 21-cr-00447 (D.D.C. Sep. 2, 2022), ECF No. 151.

[4] Def.'s Resp. to United States Mot. in Lim. Regarding Authentication of Certain Video Evid., United States v. Doolin, No. 21-cr-00447 (D.D.C. Aug. 5, 2022), ECF No. 135.

[5] Gov't's Mot. In Lim. Regarding Authentication of Certain Video Evid., United States v. Doolin, No. 21-cr-00447 (D.D.C. July 23, 2022), ECF No. 126-1.

[6] Def.'s Resp. to United States Mot. in Lim. Regarding Authentication of Certain Video Evid. at 2-3, United States v. Doolin, No. 21-cr-00447 (D.D.C. Aug. 5, 2022), ECF No. 135.

[7] Govt's Reply to Def's Resp. to United States Mot. in Lim. Regarding Authentication of Certain Video Evid. at 1, United States v. Doolin, No. 21-cr-00447 (D.D.C. Aug. 12, 2022), ECF No. 140.

[8] Id. at 2.

[9] See Docket Sheet, United States v. Pollock, No. 21-cr-00447, https://www.courtlistener.com/docket/60041704/united-states-v-pollock/?page=2 (last visited Dec. 7, 2022).

[10] Verdict Form, United States v. Reffitt, No. 21-cr-00032 (D.D.C. Mar. 8, 2022), ECF No. 123.

[11] Robert Legare, Guy Reffitt, First January 6 Defendant to Stand Trial, Found Guilty On All Charges, CBS News (Mar. 9, 2022), https://www.cbsnews.com/news/guy-reffitt-january-6-capitol-riot-guilty/; Emily Zantow, No Regret, Says Man Who Reported Capitol Rioter Dad to FBI, Courthouse News Serv. (Mar. 3, 2022), https://www.courthousenews.com/capitol-riot-defendants-son-does-not-regret-reporting-father-to-fbi/.

[12] @JordanOnRecord, Twitter (Mar. 3, 2022, 11:54 AM), https://twitter.com/JordanOnRecord/status/1499427918799421443 (describing video played in courtroom).

[13] @JordanOnRecord, Twitter (Mar. 3, 2022, 12:04 PM), https://twitter.com/JordanOnRecord/status/1499430480701267970 (quoting video played in courtroom).

[14] @JordanOnRecord, Twitter (Mar. 3, 2022, 12:01 PM), https://twitter.com/JordanOnRecord/status/1499429894698242048 (describing video played in courtroom). See also https://www.wusa9.com/article/news/national/capitol-riots/opening-arguments-capitol-riots-trial-guy-reffitt-three-percenters/65-21e60bf8-498e-4600-8b5a-0188df3a9f96.

[15] Tr. of Jury Trial at 876, United States v. Reffitt, No. 21-cr-00032 (D.D.C. Apr. 12, 2022), ECF No. 139.

[16] Id.

[17] Id. at 876-77.

[18] Id. at 878.

[19] Id.

[20] Hannah Rabinowitz, Jan. 6 Rioter Who Carried Gun to US Capitol and Threatened Nancy Pelosi Gets More Than 7 Years in Prison, CNN (Aug. 1, 2022), https://www.cnn.com/2022/08/01/politics/guy-reffitt-sentencing/index.html.

[21] Nicholas Bogel-Burroughs, Rittenhouse's Lawyers Argue that Zooming In On a Video Could Distort the Image, N.Y. Times (Nov. 11, 2021), https://www.nytimes.com/2021/11/10/us/kyle-rittenhouse-video-zoom.html.

[22] Sean Hollister, Judge Buys Rittenhouse Lawyer's Inane Argument that Apple's Pinch-to-Zoom Manipulates Footage, The Verge (Nov. 10, 2021, 9:18 PM), https://www.theverge.com/2021/11/10/22775580/kyle-rittenhouse-trial-judge-apple-ai-pinch-to-zoom-footage-manipulation-claim.

[23] Bogel-Burroughs, Rittenhouse's Lawyers Argue.

[24] Id.

[25] Hollister, Judge Buys Rittenhouse Lawyer's Inane Argument. See also AppleInsider Staff, Defense in Kyle Rittenhouse Trial Argues Apple 'AI' Manipulates Video Footage, Apple

Insider (Nov. 11, 2021), https://appleinsider.com/articles/21/11/11/defense-in-kyle-rittenhouse-trial-argues-apple-ai-manipulates-video-footage ("Apple does not employ AI resizing algorithms that interpolate imagery in the way Richards suggests, and zooming features have been available on Apple's modern portables since the first iPhone.").

[26] Bill Hutchinson & Emily Shapiro, Kyle Rittenhouse Acquitted On All Charges, ABC News (Nov. 19, 2021), https://abcnews.go.com/US/jury-reaches-verdict-kyle-rittenhouse-homicide-trial/story?id=81108654.

[27] Vinny Vella, A Bucks County Woman Created 'Deepfake' Videos to Harass Rivals on Her Daughter's Cheerleading Squad, DA Says, Phila. Inquirer (Mar. 12, 2021), https://www.inquirer.com/news/bucks-county-raffaela-spone-cyberbullying-deepfake-20210312.html.

[28] See, e.g., id.; Kim Bellware, Cheer Mom Used Deepfake Nudes and Threats to Harass Daughter's Teammates, Police Say, Wash. Post (Mar. 13, 2021), https://www.washingtonpost.com/nation/2021/03/13/cheer-mom-deepfake-teammates/; Good Morning America, Cheerleader's Mom Sent Deepfake Videos to Allegedly Harass Daughter's Rivals: Police, ABC News (Mar. 15, 2021), https://www.youtube.com/watch?v=6o-MC4jSYWc.

[29] Drew Harwell, Remember the "Deepfake Cheerleader Mom"? Prosecutors Now Admit They Can't Prove Fake-Video Claims, Wash. Post, (May 14, 2021), https://www.washingtonpost.com/technology/2021/05/14/deepfake-cheer-mom-claims-dropped/.

[30] Id. (quoting student claiming video was a fake); Ruff, The Federal Rules of Evidence are Prepared for Deepfakes, at 118.

[31] Fed. R. Evid. 901(a).

[32] Fed. R. Evid. 901(b)(4).

[33] Fed. R. Evid. 901(b)(3).

[34] Ruff, The Federal Rules of Evidence are Prepared for Deepfakes, at 123-24.

[35] Fed. R. Evid. 902(13).

[36] Fed. R. Evid. 902(14).

[37] Fed. R. Evid. 902(11).

[38] Ferraro et al., Identifying the Legal and Business Risks, at 151; Pfefferkorn, "Deepfakes" in the Courtroom, at 254; Claypoole, AI and Evidence; Reynolds, Courts and Lawyers Struggle.

[39] See Gregory P. Joseph, Self-Authentication of Electronic Evidence: New Rules 902(13)-(14) (unpublished), https://www.txs.uscourts.gov/sites/txs/files/Self-Authentication%20of%20Electronic%20Evidence%20-%20New%20Rules%20-%20G.Joseph.pdf.

[40] Model Rules of Prof'l Conduct r. 3.3(a)(3).

[41] Model Rules of Prof'l Conduct r. 3.3(b). See also ABA, Criminal Justice Standards for the Defense Function (4th ed., 2017), Standard 4-7.6(b), https://www.americanbar.org/groups/criminal_justice/standards/DefenseFunctionFourthEdition/ ("Defense counsel should not knowingly offer false evidence for its truth . . . or fail to take reasonable remedial measures upon discovery of material falsity in evidence offered by the defense, unless the court or specific authority in the jurisdiction otherwise permits.").

[42] Model Rules of Prof'l Conduct r. 3.3(a)(3) (emphasis added). See Pfefferkorn, "Deepfakes" in the Courtroom, at 273-74.

[43] Standards for the Defense Function, Standard 4-7.6(e).

[44] Model Rules of Prof'l Conduct preamble ¶ 6.

[45] Model Rules of Prof'l Conduct r. 3.1, 3.3(a)(3); Fed. R. Civ. P. 11(b)(1), (2), (4); Standards for the Defense Function, Standard 4-7.6(d), (e); Pfefferkorn, "Deepfakes" in the Courtroom, at 274.

[46] Standards for the Defense Function, Standard 4-4.1(c).

[47] Pfefferkorn, "Deepfakes" in the Courtroom, at 270.

[48] Id.

[49] Id. at 270-71.

[50] Joseph, Self-Authentication of Evidence, at 3.

[51] Id.

[52] Id. at 5.

[53] See McPeak, The Threat of Deepfakes in Litigation, at 448-49. See also Ruff, The Federal Rules of Evidence are Prepared for Deepfakes, at 125 ("On the whole, a body of circumstantial evidence should be sought when authenticating video. When the fair and accurate representation standard has been used, that body of circumstantial evidence should speak to the origins of the video. Video with indeterminate origins should not be authenticated.").

[54] Tr. of Jury Trial at 876-78, United States v. Reffitt, No. 21-cr-00032 (D.D.C. Apr. 12, 2022), ECF No. 139.

[55] Pfefferkorn, "Deepfakes" in the Courtroom, at 265.

[56] See Ferraro & Spaulding, Disinformation and Deepfakes, at 419-22.