State of New York
Court of Appeals

OPINION

No. 7
In the Matter of M.S.

Erie County Department of Social Services,
Respondent;
M.H., &c.,
Appellant.
(And Another Proceeding.)

Emily S. Wall, for appellant.
Madison L. Ozzella, for respondent.
David J. Pajak, attorney for child G.H.
Center for Integrity in Forensic Sciences, Brooklyn Defender Services et al., Just Making a Change for Families, amici curiae.

WILSON, Chief Judge:

Appellant M.H. has a daughter, M.S., and a son, G.H. Family Court found that she abused M.S. and derivatively abused G.H. The court's findings were entirely based on videos that appeared to show M.H.'s former live-in boyfriend, D.K., sexually abusing M.S. Family Court determined that M.H. had abused both her children by failing to protect them

from D.K. Because the foundation offered for the videos was insufficient, we hold that Family Court erred in admitting the videos into evidence and therefore reverse.

I.

In February 2022, Erie County filed concurrent Family Court article 10 petitions against M.H. and D.K., alleging they had abused both children. In three videos bearing timestamps showing dates in May, June and July 2019, D.K. appears to be engaged in sexual contact with M.S. on the couch in the living room. M.S. was 14 in 2019. In one of the three videos, M.H. can be seen leaving the room a few minutes before D.K. is shown touching and caressing M.S.

The videos were not discovered in the family home or on any camera or computer belonging to D.K. or M.H. Instead, in the course of an FBI investigation into persons suspected of trading child pornography, the agents executed a search warrant on B.W., who lived in Syracuse. In the course of questioning by FBI Agent Martin Baranski, B.W., though not under oath or in any sworn statement, said (according to Agent Baranski's recollection) that he had been "hack[ing] into security web cameras for the past few years." B.W. further stated that in 2019 he had "hacked into a security camera" which showed what he thought was an adult male sexually abusing the man's 15-year-old stepdaughter. B.W. claimed that he "watched a lot of the security camera footage of this house" and saw "a lot" of interactions between the individuals depicted in the videos. He told Agent Baranski he had saved some videos from that camera in a particular location on his computer, along with a screenshot that contained details about the security camera login information, including a possible name, email and IP address.

Searching a digital copy of B.W.'s computer, Agent Baranski found three videos that appeared to show an adult male sexually abusing a young girl; the videos contained timestamps indicating they were recorded around the summer of 2019. Based on information from the screenshot on the suspect's computer and other investigative work, Agent Baranski was able to identify D.K.'s name and workplace; he then relayed that information to New York law enforcement. After attempting to match photographs of D.K. and M.S. to people shown in the videos, state police called M.H. and told her they "wanted to speak to her regarding her daughter with some internet usage." They met with her in person and provided her with screenshots of two people taken from the videos. M.H. told police that the screenshots depicted D.K. and M.S. After accompanying M.H. to her home, police then informed M.H. that the videos appeared to show D.K. sexually abusing M.S. and M.H. gave consent to search her home and take photographs. Police then searched the home, took photographs and spoke to M.S. They asked M.H. to take M.S. and G.H. to the Children's Advocacy Center for interviews. During the interviews, M.S. denied that she had any sexual contact with D.K. M.S. said "she was 'conflicted' and 'confused' by the allegations and description of the video" and, after being asked whether "anyone had ever touched her, with or without her consent," M.S. said that had not occurred. G. H., who was 12 at the time of the interview, "did not seem to know anything about why" he was being interviewed. G.H. "denied that he had ever been touched inappropriately or that his sister had ever confided in him that someone had hurt her." That same day, during a consensual search of the family's home, police officers took several pictures of the living room which appeared to match details shown in the videos. Although, pursuant to search warrants, the

police obtained D.K.'s computers (both work and home) and cameras, no evidence from those devices was offered at trial.

On Erie County's motion, the children were removed from M.H. and placed with their maternal grandparents and a stay-away order was issued directing that D.K. have no contact with the children. By the time of the dispositional hearing in November 2022, the children had been placed in a non-kinship foster home. During the pendency of these proceedings, M.S. turned 18 and aged out of foster care; G.H., who is now 16, remains in foster care.

At the hearing, neither M.H. nor D.K. testified, but M.H. joined D.K.'s objection to admitting the videos. M.S. and G.H. each was separately represented by counsel. Neither child testified. Erie County's sole evidence of abuse was the videos obtained from B.W. Erie County attempted to lay the foundation for the videos through the testimony of Agent Baranski and Gary Mahoney, one of the state police officers who searched the home. Agent Baranski testified as to how he came to find the videos and his delivery of the videos to the New York state police. Investigator Mahoney testified that the living room he saw at the house "matched the living room in the video" and noted that he observed cameras in the house and, in M.H. and D.K.'s bedroom, there were sex toys of the kind depicted in the videos. He identified M.S. and D.K. in screenshots taken from the videos.

Based on Agent Baranski's chain of custody testimony, Investigator Mahoney's personal observations of the location depicted in the video and M.H.'s identification of D.K. and M.S. in screenshots taken from the videos, Family Court held that Erie County had laid a sufficient foundation to admit the videos. Crediting the "technical experience

and expertise" of Agent Baranski, Family Court held that his testimony indicated there were "no signs" that the videos had been "manipulated or altered." In its order of fact-finding, Family Court gave "great weight" to the videos in both proceedings and determined that both M.H. and D.K. had abused M.S. and, in M.H.'s case, derivatively abused G.H.

By the time of the dispositional hearing, it was undisputed that M.H. had completed a parenting class, obtained "suitable income and housing," and moved out of D.K.'s home into her own residence. At the hearing, the court issued a stay-away order of protection against D.K. in favor of both children. Over the objection of M.H. and of both children (who both asked to be returned to M.H.'s care), and five days before M.S.'s 18th birthday, Family Court also ordered both children to be placed in foster care and that M.H. have only agency-supervised visits with them. Upon turning 18 five days later, M.S. aged out of foster care and moved in with a family friend. A later dispositional order set out the conditions with which M.H. had to comply to have her son returned to her care.

On appeal, M.H. argued that (1) an insufficient foundation had been laid to admit the videos; (2) the finding of abuse against her was not supported by a preponderance of the evidence; (3) the facts supporting the abuse finding as to M.S. could not sustain a finding of derivative abuse against M.H. with respect to G.H.; and (4) the dispositional order setting the conditions for G.H.'s return to her care was not in G.H.'s best interests. The Appellate Division affirmed, with Presiding Justice Whalen in dissent (229 AD3d 1040 [4th Dept 2024]). The court held that any uncertainty with respect to the videos went to the weight, not admissibility, of the evidence (*id.* at 1042-1043). As to the abuse and

derivative abuse findings, the court held that Family Court could infer from the evidence "that the mother knew or should have known about the abuse and did nothing to prevent it" (*id.* at 1043), and that the facts surrounding M.S.'s abuse "were 'so closely connected with the care of' [G.H.] so as to justify the finding of derivative abuse" (*id.*). The court held there was record support for Family Court's dispositional order as to G.H. (*id.* at 1044).

We granted leave to appeal.

II.

On appeal to our Court, M.H. raises the four issues identified by the dissent below: (1) Family Court erred in admitting the videos,[1] because they were not properly authenticated; (2) the finding of abuse against her was improper because, in her view, actual knowledge is required to sustain a finding of abuse under Family Court Act § 1012 (e) (iii) (A); (3) Family Court's finding of derivative abuse as to G.H. was improper because there was no evidence that any sexual abuse was ever directed at G.H. and he did not meet the statutory definition of an abused child; and (4) the dispositional order placing G.H. in foster care (and setting conditions for his return to M.H.) was not in his best interests. Because we agree the videos were not properly authenticated, and therefore should not have been received into evidence, we have no reason to reach the other issues M.H. raises.

[11] The videos at issue were destroyed by Family Court order in August 2024, a month after M.H. moved for leave to appeal to this Court. Destruction of evidence before the exhaustion of the appellate process (and any subsequently ordered proceedings below) should not be countenanced.

It is the burden of the party moving to introduce evidence to make "a sufficient threshold showing of reliability" (*People v Price*, 29 NY3d 472, 482 [2017]). Reliability can be demonstrated "by proof that the offered evidence is genuine and that there has been no tampering with it" (*People v McGee*, 49 NY2d 48, 59 [1979]). With respect to video evidence, we held in *Patterson* that a video may be authenticated through (1) "testimony of a witness to the recorded events or of an operator or installer or maintainer of the equipment that the videotape accurately represents the subject matter depicted" or (2) testimony (expert or lay) establishing that the video "truly and accurately represents what was before the camera" (*People v Patterson*, 93 NY2d 80, 84 [1999] [internal citation omitted]). The authentication requirement applies to civil as well as criminal proceedings (*see Zegarelli v Hughes*, 3 NY3d 64, 69 [2004] [applying *Patterson* standard for authentication of videotape in civil context]). Proper authentication of evidence vindicates the basic principle that evidence which is not what the proponent claims it to be can prove nothing at all (*Price*, 29 NY3d at 476 ["In order for a piece of evidence to be of probative value, there must be proof that it is what its proponent says it is"], quoting *United States v Sliker*, 751 F2d 477, 497 [2d Cir 1984]).

A comparison to the facts in *Patterson* shows why the videos here were not properly authenticated. In *Patterson*, the trial court admitted into evidence a surveillance video that purported to show a robbery inside a grocery store (*People v Patterson*, 242 AD2d 740, 741 [2d Dept 1997], *revd* 93 NY2d 80 [1999]). Neither the parties who witnessed the crime or the store owner (who had died from unrelated causes before trial) testified as to the authenticity of the video (*id.*). The police obtained the video directly from the store

owner just two weeks after the crime and kept it secure in police custody, unaltered, until the trial (*id.*). The trial court held the video was sufficiently authenticated by the testimony of officers who identified one of the defendants on the video and confirmed that the video accurately depicted the "physical layout" of the store, which he had personally photographed (*id.*). Even so, we held that the video was not properly authenticated because of a lack of foundation and failure to provide a full chain of custody (*Patterson*, 93 NY2d at 85).

The foundation here is even more lacking than the one we held insufficient in *Patterson*. Whereas in *Patterson*, the store owner "who himself inserted the videotape into the store surveillance system" provided the video directly to the police (*Patterson*, 242 AD2d at 741), here the person who allegedly created the videos, D.K., provided no evidence or testimony, and B.W., the child pornographer with no connection to the family who claimed to have hacked into D.K.'s cameras, likewise never testified.[2] Instead, Agent Baranski offered hearsay testimony as to what B.W. had told him.[3] In *Patterson*, the "unaltered" feed of the footage from the grocery store was provided by the store owner

[2] There is a discrepancy between the testimony of Agent Baranski, that B.W. told him he hacked into camera feeds (as opposed to the computer itself), and Family Court's finding that B.W. "had hacked [D.K.'s] computer and downloaded the video from there."

[3] Judge Singas's assertion that B.W. would never provide authentication testimony without a cooperation agreement (Singas J., dissenting op at 7-8) is at odds with the fact that B.W. voluntarily spoke with the FBI and turned over to them evidence, including incriminating material. Indeed, Agent Baranski testified, based on his discussions with the assistant U.S. attorney on B.W.'s case, that B.W. "was not given any cooperation agreement." Furthermore, the record does not show any effort by the County to secure authentication evidence from B.W., whether by live testimony, deposition or affidavit.

(242 AD2d at 741). Here, there was no continuous video, only snippets excerpted from a longer, unrecovered feed of the camera by B.W., who told Agent Baranski he had watched many days of video but did not explain what or how he selected and what he omitted or deleted. Agent Baranski did not testify that B.W. told him the videos were unaltered. The store owner in *Patterson* was a businessperson with no apparent ulterior motives (*id.*). B.W., in contrast, faced criminal prosecution at the time he provided the information leading to the discovery of the videos here, and had created the versions of the videos he delivered to the police by extracting them from a larger video or feed.[4] Finally, the video in *Patterson* was obtained by the police two weeks after the crime (*Patterson*, 242 AD2d at 741); here, there was a roughly two-and-a-half-year period between when the videos were stolen and snipped by the child pornographer and when they were recovered by the FBI. This long gap in the chain of custody of a key piece of evidence—65 times as long as the gap in *Patterson*—raises further doubts about the authenticity of the videos.

Our dissenting colleagues misinterpret the significance of our observations about B.W.'s motivations and technical abilities. Those points are made to show the weakness of the authentication evidence proffered here when compared to *Patterson*, not to make any conclusion about whether the videos here are altered or not. One dissent describes the possibility that the videos in question were fabricated as "ridiculous" and "outlandish"

[4] Traders of child pornography splice and edit videos to enhance their appeal to persons interested in child pornography (*see* Amicus Br. of Center for Integrity in Forensic Sciences at 15-16). Moreover, the suspect's ability to hack into computers and cameras of far-away people, with whom he had no connection, suggests he possessed the technical savvy to manipulate video images (*id.*).

(Troutman, J., dissenting op at 8), but the possibility that the shopkeeper in *Patterson* could have altered the videotape in question in the two weeks before delivering it to the police is even more remote. Regardless, the likelihood of the alteration is beside the point. The question at issue is whether the proponent of the evidence has done enough to establish its reliability. Here, the confluence of factors—including the bizarre circumstances surrounding the discovery of the videos and the long time period between their creation and their recovery—raise doubts about their authenticity, and the agency simply failed to carry its burden to dispel those doubts.

Even if were we to bypass the authentication rules and ask, instead, the irrelevant and abstract question whether phony videos could be created by 2022, when the videos here were obtained by law enforcement, the technology to make realistic manipulated videos was widely available then.[5] Even on its own terms, one dissent concedes that as of

[5] Judge Singas hinges most of her dissent on the claim that video manipulation using deepfake technology was "impossible" around the time the videos were recovered (Singas, J., dissenting op at 5). Again, that point is not germane to whether the video here was properly authenticated. But for those interested in the accuracy of her claim, we echo her invitation to readers to see for themselves (*id.* at 4). Open-source tools capable of making "deepfakes" were widely available as of 2017, when the term "deepfake" emerged after videos depicting celebrity pornography were routinely circulated on social media sites; artificial intelligence only bolstered the abilities of lay persons to make these videos (*see* Cade Metz, *Internet Companies Prepare to Fight the 'Deepfake' Future*, NY TIMES [Nov. 24, 2019] available at https://www.nytimes.com/2019/11/24/technology/tech-companies-deepfakes.html [last accessed Feb. 10, 2026]; Kevin Roose, *Here Come the Fake Videos, Too*, NY TIMES [Mar. 4, 2018], available at https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html [last accessed Feb. 10, 2026]). The exemplars of realistic videos manipulated by this technology are too numerous to recite here (*see, e.g.*, Kartik Hosanagar, *Deepfake Technology Is Now a Threat to Everyone. What Do We Do?*, WALL STREET JOURNAL [Dec. 7, 2021], available at https://www.wsj.com/tech/ai/deepfake-technology-is-now-a-threat-to-everyone-what-

2022, when law enforcement first took possession of the videos in this case, technological innovations "enabled users to convincingly alter or substitute the appearance of people in videos of actual events" (Singas, J., dissenting op at 4 [emphasis omitted]).

The facts relied on by Family Court do not alleviate the reliability concerns raised by the unusual origin and uncertain chain of custody of these videos. First, Family Court credited the expertise and testimony of Agent Baranski in determining the videos were not altered. Agent Baranski was concededly familiar with child pornography through his experience, but the County never sought to qualify him as an expert (or establish his experience) in video authentication, which is the point. Broad familiarity with a subject does not make someone learned in detecting evidence of tampering or fabrication.[6] Yet Agent Baranski did not testify as to any training or experience in identifying signs of tampering or video alteration that could establish his ability to authenticate as a lay witness. He was not asked whether he examined the videos to look for tampering; whether he used any forensic tool to detect tampering; or even whether he was able to offer a learned affirmative opinion that the video was not tampered with, as *Patterson* mandates. Instead, the question he was asked about tampering was: "[D]id you make any observations that led

---

do-we-do-11638887121?msockid=0b493934559e68d519052f1254876973 [last accessed Feb. 10, 2026] [accompanying video showing multiple exemplars]).

[6] *See* Andrew Lewis et al., *Deepfake detection with and without content warnings* (Royal Soc'y Open Science) (Nov. 2023), available at https://pmc.ncbi.nlm.nih.gov/articles/PMC10679876/ (last accessed Feb. 10, 2026) (finding that familiarity with an actor depicted in a fake video did not improve odds of detecting deepfake of that actor).

you to believe that the video footage had been tampered with or altered in any way?" to which he answered, "No" without elaboration. Agent Baranski himself may have possessed the experience or training necessary to authenticate the videos, but we will never know because he was not asked the important foundational questions.

Investigator Mahoney's testimony that the videos matched his personal observations of the layout of the living room and items he observed there are similarly insufficient and are not meaningfully different from what we rejected in *Patterson*. There, an officer who had visited the store where the robbery occurred testified that the video was an accurate depiction of the store's "actual physical layout" (*Patterson*, 242 AD2d at 741).[7] The fact that much of the video apparently accurately depicted the home is not sufficient—as it was not in *Patterson*—to authenticate the video. If such testimony was insufficient then, the increasing prevalence of "deepfake" videos has only rendered the method of matching circumstantial details in a video to personal observations a more suspect form of authentication; most fabricated videos "leverage" real details from real photos and videos of real places and people, then alter the pieces the person wishes to alter to create a realistic, but manipulated, video (*see* Amicus Br. of Center for Integrity in Forensic Sciences at 7-8). In the authentication context, what matters most is whether the events depicted are as real as the proponent claims them to be, not whether there are some identifying features of

[7] Puzzlingly, one dissent credits the fact that in *Patterson*, the Appellate Division relied on the fact a police officer testified as to the "physical layout" of the store (Troutman, J., dissenting op at 6-7). But the mode by which that video was authenticated was one this Court deemed insufficient (*Patterson*, 242 AD2d at 741).

the video that can be corroborated in real life. Contrary to the dissents' characterization (Troutman, J., dissenting op at 5-6; Singas, J., dissenting op at 6-8), that the circumstantial evidence offered here is insufficient does not mean that circumstantial evidence is never relevant to authentication. We see nothing "shortsighted" (Troutman, J., dissenting op at 10) or "troubling" (Singas, J., dissenting op at 12) in continuing to rely on *Patterson*'s proven framework in light of changing technological circumstances (*Patterson*, 93 NY2d at 84 ["the obligation and need for responsible accuracy and careful reliability should not be sacrificed to some of the whims and weaknesses of fast moving and rapidly changing technology"]). Without saying so, our dissenting colleagues would like to overrule *Patterson*. No party has asked us to do so, and *Patterson* is particularly prescient in the factors it identified as insufficient to establish the authenticity of a video, especially given the far greater ability to manipulate video images now as compared to 1999, when we decided *Patterson*.

Erie County's reliance on *People v Goldman* (35 NY3d 582 [2020]) is entirely misplaced. In *Goldman*, we affirmed a trial court's authentication of a video posted on YouTube. The defendant, charged with a drive-by gang-related homicide, objected to authentication of a rap video (appearing to show him boasting about the crime) solely on the ground that the People could not prove when it was made (*id.* at 588). The cooperating witness, a friend of the defendant who was the driver of the car during the shooting, testified that the evening after the shooting, the defendant invited him to come to the filming of a rap video the next morning and told him what the name of the video would be (which corresponded to its name on YouTube) (*id.*). The cooperating witness also testified

that he viewed the video on YouTube, shortly after defendant posted it, identified in the video the defendant and the two rear-seat passengers, who were well-known to him; and identified the social media handle used by defendant and his crew, which appeared on the video (*id.*). He further testified that the video introduced in court accurately represented the video he had previously watched on YouTube (*id.*). Those facts provided a far more robust basis for authentication than is present here.

The rules of evidence apply in Family Court just as much as they apply in any other court. The proponent of evidence bears the burden of demonstrating its authenticity.[8] *Patterson* is on all fours with this case and, as explained herein, the evidence establishing the authenticity of the store video in *Patterson* was stronger than that present here, yet we held that the store video was not properly authenticated. The failure to authenticate evidence sufficiently does not mean the evidence was false, but only that it was not properly authenticated according to the rules of evidence. Our dissenting colleagues' abundant use of colorful adjectives and adverbs neither establishes the authenticity of this evidence nor persuades as to the occurrence of the predicted catastrophes. We do not mean to suggest that the videos here could not have been authenticated, or that child victims must testify, or that B.W., Agent Baranski, or some other person could not have offered adequate authentication testimony. But the evidence of authentication proffered here was legally

[8] Our dissenting colleagues' characterization of the issue as weight of the evidence is misplaced (*see* Troutman, J., dissenting op at 6-7; Singas, J., dissenting op at 7). Authentication and other rules of evidentiary admissibility determine what is to be weighed, not how much weight to give.

insufficient. What that means for the next case is that in Family Court, as in all our courts, evidence must be properly authenticated.

***

Accordingly, the orders of the Appellate Division should be reversed, without costs, and the petitions dismissed.

TROUTMAN, J. (dissenting):

The majority holds that videos depicting the mother's live-in boyfriend sexually abusing her 14-year-old daughter were not properly authenticated, and therefore should not have been admitted into evidence by Family Court. The majority expresses concern about

the rise of "deepfake" videos.[1] Yet no one uttered the word "deepfake" during the Family Court proceedings below, nor was there any evidence presented that the portions of the videos depicting sexual abuse were fabricated. In addressing a concern that was never raised below, the majority creates new and perhaps insurmountable hurdles for future authentication of video evidence. As a result, children will be harmed and abusers will escape accountability. I dissent.

I.

The majority's recitation of the facts is incomplete. It is true that while being interviewed at the Child Advocacy Center, the daughter denied that she had been sexually abused by the mother's boyfriend. But Family Court did not find those denials convincing, and explained why:

> "The digital recording of the interview was moved into evidence as Respondents' Exhibit A and viewed by the Court. Respondents' counsel argue that the video shows the child denying any sexual abuse at least eight different times during the video. While it is certain that the child made no disclosures during the video, it is not persuasive evidence that the child was not abused. [The daughter] cried throughout the video and sat in silence for uncomfortable periods of time after questions were asked. When she did respond, she provided whispered, one-word answers. She stated that she was 'conflicted' and 'confused' by the allegations and description of the video. She described her relationship with her mother as 'distant' and said that she has a better relationship with [the mother's boyfriend], whom she calls 'dad.' At the end of the interview, [the daughter] was asked a series of questions about whether anyone had ever touched her, with or without her consent. [The

[1] A "deepfake" video is, essentially, a "genuine-looking video that makes real people appear to do and say things they never did or said" (Riana Pfefferkorn, *"Deepfakes" in the Courtroom*, 29 BU Pub Int LJ 245, 245 [2020]).

> daughter] did not make a clear and convincing denial. Instead, she uttered a whispered 'no,' given through tears. She did not present as a happy, confident young woman of seventeen, but rather as a much younger child who was defeated and frightened. Nothing about this interview supported the argument that [the daughter] honestly denied being abused. On the contrary, she presented as an abused child who was afraid to speak honestly."

This Court has repeatedly recognized the validity of Child Sexual Abuse Accommodation Syndrome (CSAAS), which explains that children who have been sexually abused might not only delay disclosure; they may also deny that they were sexually abused at all (*see People v Nicholson*, 26 NY3d 813, 828 [2016], citing *People v Spicola*, 16 NY3d 441, 453-454 [2011]).

The majority further states that during a search of the family's home, "police officers took several pictures of the living room which appeared to match details shown in the videos" (majority op at 3). That description belies the level of detail regarding the home that was confirmed by police to match what was depicted in the videos. As Family Court explained:

> "[I]t is clear that the room shown in the video is the same room photographed by [the investigator] during his investigation of [the boyfriend's] home. The same couch, painting, afghan, end table and lamp are all visible. Photographs taken during the execution of a search warrant further establish the reliability of the video. These photographs . . . show objects recovered in the home. Those objects can also been seen in the video. Specifically, [one photograph] shows the foot massager/scraper that [the daughter] was using on [the boyfriend's] feet in the video. [Another photo] shows the vibrators and dildos recovered from the drawer in the bedroom shared by the Respondents. And in [other photos], [the daughter's] room is decorated with the same type of stuffed

> animal she was holding in the video in which [the boyfriend sexually abused her]."

These factual findings were affirmed by the Appellate Division (229 AD3d 1040, 1042-1043 [4th Dept 2024]).

Finally, the majority states that the mother joined the boyfriend's objection to admission of the videos (majority op at 4). The specific objection made by the boyfriend's counsel was that given the period of time between when the videos were recorded and when they were recovered by the FBI, the chain of custody was lacking, and that the Department of Social Services (DSS) would be unable to show "that it wasn't altered unreasonably in any way." The mother's counsel agreed with that objection and stated that the video may have been "heavily altered." No one used the word "deepfake," or argued that the videos accurately depicted the family's home and the individuals who lived there (which the mother now does not dispute) but that the portions of the videos showing sexual abuse were fabricated, which is the mother's current position.

II.

Generally, video evidence "may be authenticated by the testimony of a witness to the recorded events or of an operator or installer or maintainer of the equipment that the videotape accurately represents the subject matter depicted" (*People v Patterson*, 93 NY2d 80, 84 [1999]). "Testimony, expert or otherwise, may also establish that a videotape truly and accurately represents what was before the camera" (*id.* [internal quotation marks omitted]). " 'Any person having requisite knowledge of the facts' " may provide the necessary foundation for authentication (*People v Rodriguez*, 38 NY3d 151, 155 [2022],

quoting *People v Price*, 29 NY3d 472, 477 [2017]). "The decision to admit or exclude videotape evidence generally rests . . . within a trial court's founded discretion," and the trial court's ruling "may disturbed by this Court only when no legal foundation has been proffered or when an abuse of discretion as a matter of law is demonstrated" (*Patterson*, 93 NY2d at 84).

Circumstantial evidence is also a permissible method of authentication. In *Patterson*, we recognized that "reasonable inferential linkages can ordinarily supply foundational prerequisites" (*id.* at 85). And in *People v Goldman* (35 NY3d 582 [2020]), we held that "distinctive identifying characteristics" in the video at issue there demonstrated that the video "accurately represented the subject matter depicted" (*id.* at 595 [internal quotation marks and alteration omitted]). The Guide to New York Evidence published on the New York Courts website recognizes circumstantial evidence as a permissible method of authentication, observing that the "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances," may be sufficient for authentication (*see* Guide to NY Evid rule 9.05 [6], Methods of Authentication and Identification, https://nycourts.gov/judges/evidence/9-AUTHENTICITY/9.05_METHODS.pdf [last accessed Feb. 6, 2026]).

Here, circumstantial evidence amply demonstrates that the videos accurately represented the subject matter depicted, such that Family Court did not abuse its discretion in admitting them. First, the mother affirmatively identified her boyfriend and her daughter from screenshots taken from the videos. Second, video cameras that the police found in the living room were in position to capture the sexual abuse as depicted in the videos.

Third, the living room's appearance and furnishings were as they appeared in the video upon a search of the home. And finally, items indistinguishable from those shown in the videos *during the instances of sexual abuse* were found in the home.

This circumstantial evidence was sufficient for Family Court to conclude that a sufficient foundation was laid to authenticate the videos and admit them into evidence. Although the majority relies heavily upon the length of time that passed between when the videos were recorded and when they were recovered by the FBI, that factor goes to weight, not admissibility, given that FBI Agent Baranski adequately explained the circumstances leading to the recovery of the videos.

In addition to the circumstantial evidence of authenticity, DSS presented the testimony of Agent Baranksi, who testified about the circumstances leading to the recovery of the videos from B.W. Baranski further testified that that he did not observe anything in the videos that led him to believe that they had been tampered with or altered. Baranski worked exclusively on crimes against children, primarily investigated child pornography and human trafficking, and "perform[ed] digital forensic work and online undercover work." Baranski's testimony that the videos were not altered implicitly relied upon his training and experience.

Patterson does not require a different result. *Patterson* was reversed on other grounds regarding the admission of a police officer's testimony regarding the victim's earlier lineup identification of the defendant (*see* 93 NY2d at 82). The Court merely noted, that because further proceedings would occur, "the present state of the record provides an inadequate basis for admissibility" of the surveillance video (*id.* at 85). Furthermore, the

Appellate Division decision noted that a police officer had confirmed that the surveillance video "accurately depicted the actual physical layout of the grocery store" (*see People v Patterson*, 242 AD2d 740, 741 [2d Dept 1997], *revd* 93 NY2d 80).

Patterson is readily distinguishable, because here, the evidence that the videos accurately depicted events occurring in the family's home was far more robust than merely corroboration of the home's "physical layout." There is no dispute on appeal that the innocuous portions of the videos accurately depicted the members of the family and their home, as confirmed by the mother's identifications, the nearly identical appearance of the living room when the police searched it, and cameras placed at the angle that would have captured the sexual abuse. Furthermore, as explained, similar items to those seen in the videos during the portions depicting the boyfriend sexually abusing the daughter were also found in the home. The majority claims to be puzzled by my comparison of the stronger evidence of authentication presented here than that presented in *Patterson* (majority op at 12 n 7), yet nowhere in its opinion does it purport to contend with these differences.

In sum, the circumstantial evidence of authenticity, coupled with Agent Baranski's testimony, was sufficient for Family Court to conclude that the videos were admissible. The remaining issues raised by the mother were relevant to the weight afforded to the videos, not their admissibility. Neither the mother nor the boyfriend testified during the proceedings that the videos were not accurate.

III.

The majority's and the mother's theory that the videos could have been "deepfakes," although not explained in any detail, appears to be as follows: B.W. did in fact hack into

the family's living room camera and viewed the individuals who lived in the home interacting with each other and going about their days, but he then used that accumulated video footage and some unspecified software program to fabricate the portions of the video depicting the mother's boyfriend sexually abusing the daughter. And he fabricated those portions of the videos depicting sexual abuse but made sure to include in those fabrications inanimate objects that were later found in the family's home. This outlandish theory was never raised by the mother or her boyfriend before Family Court. The mother raised this ridiculous proposition for the first time on appeal.

Moreover, the majority's speculation that the videos might have been deepfakes relies upon suppositions and inferences that were never presented to Family Court. For example, the majority states that B.W.'s "ability to hack into computers and cameras of far-away people, with whom he had no connection, suggests he possessed the technical savvy to manipulate video images" (majority op at 9 n 4). No evidence was presented of B.W.'s technical expertise, nor was any evidence presented regarding the software programs for creating deepfakes that were available in 2019 (*see* majority op at 10 n 5).

In addition, the majority asserts that "[t]raders of child pornography splice and edit videos to enhance their appeal," based on assertions made in an amicus brief (*see* majority op at 9 n 4). No evidence was presented to Family Court regarding the behavior of those who trade in child pornography, nor was any evidence whatsoever presented that B.W. traded these videos or edited them in any way beyond simply saving certain portions of them to his computer, as Agent Baranski testified.

The majority states that "the increasing prevalence of 'deepfake' videos has only rendered the method of matching circumstantial details in a video to personal observations a more suspect form of authentication" (majority op at 12). It seems that in the future, a party opposing the introduction of video evidence need only posit, with no evidentiary support whatsoever, that the video might be a deepfake. The party introducing the video then must disprove that unfounded accusation. How is the party seeking admission to do so, if circumstantial evidence is not a permissible method of authentication?

The majority rightfully does not suggest that the daughter should have been required to view the video of her sexual abuse and testify that it accurately depicted the horrors she suffered. Imposing such trauma upon a survivor of child sexual abuse by revictimizing them cannot be a necessary method of authentication, and Family Court Act § 1046 (a) (vi) specifies that children are not required to testify in such proceedings. The majority notes, however, that the boyfriend, who created the videos, did not testify to authenticate them (majority op at 8). It is hardly surprising that DSS could not authenticate videos of child sexual abuse through the perpetrator of that abuse, who would be admitting to various felonies by testimony that the videos were accurate.

That leaves, ostensibly, expert testimony. According to the majority, Agent Baranski's testimony did not suffice. For the reasons explained, I disagree. But the majority's conclusion is problematic for other reasons that will have ramifications far beyond this particular case. Given that the speculation that the videos were deepfakes was raised for the first time on appeal, there is nothing in the record to suggest that DSS will be able to find, secure, and compensate an expert in identifying deepfake videos in the future.

Do such experts exist? Are there sufficient numbers of them such that they will be available to testify in every criminal or Family Court proceeding where video evidence of child abuse is offered and the perpetrator contends it is a deepfake?[2] The majority does not say, and lower courts and those tasked with protecting children from abuse will be left to sort through the havoc the majority's opinion will wreak.[3]

The majority's decision unfortunately will make it exponentially more difficult not only to authenticate video evidence but also to protect victims of child abuse and hold perpetrators accountable. This decision is shortsighted.

[2] A 2020 law review article on the subject asserted that "[a]t present, there are likely only a handful" of expert witnesses who are qualified to assess allegedly deepfake videos, and their numbers "will not grow quickly" (*see* Pfefferkorn, 29 BU Pub Int LJ at 265). This is because "[t]he necessary forensic expertise to detect deepfakes requires a specialized background in a field with complex barriers to entry, meaning the few who have it can command top dollar for their services" (*id.*). Paying "top dollar" for such an expert witness is likely beyond the financial resources of most local child protective agencies.

[3] Like the majority (*see* majority op at 6), I will not address the remaining issues raised by the mother on this appeal, except to note that I would affirm the Appellate Division order in all other respects.

SINGAS, J. (dissenting):

I fully agree with Judge Troutman's dissent. I am compelled to write separately to emphasize that the majority's superficial and simplistic analysis of "deepfake" technology raises serious legal questions to which the majority supplies no answer, and defies the

critical approach taken by the federal courts and other jurisdictions. More importantly here, it will harm abused and neglected children. I cannot countenance this result.

Make no mistake: in a Family Court child-protective proceeding, the majority rejects the sole evidence of the boyfriend's serial sexual abuse of the mother's 14-year-old daughter due to its concern about deepfakes and similar forgery, absent any meaningful connection whatsoever between such technology and the facts of this case.

The majority contorts the record. It misleadingly describes the videos at issue as "appear[ing] to show" the boyfriend committing sexual abuse (*see* majority op at 3). In reality, after viewing the videos, Family Court found that they depict the boyfriend "touch[ing] and kiss[ing]" the daughter "in a sexual manner," "kiss[ing] her neck and fondl[ing] her breasts," and "us[ing] an inanimate object and his fingers to penetrate her vaginally." The majority's claim that the daughter "denied" being abused (majority op at 3) is equally dishonest by omission (*see* Troutman, J., dissenting op at 2-3 [revealing what the record actually reflects]). Nor does the majority acknowledge that the mother denied the boyfriend's sexual abuse despite refusing to even watch these videos, or that the mother never argued the videos are fake. Indeed, the mother declined to testify at all, despite being warned that Family Court would draw the strongest permissible adverse inference against her if she chose to remain silent.

It is vital to understand what the majority nonetheless posits may have occurred here. The majority proposes that in or before January 2022, B.W., a voyeur child pornographer, after hacking into this family's living-room security camera and gathering innocuous footage of the boyfriend, mother, daughter, and son, (1) somehow also gathered

innocuous footage of specific sex toys owned by the boyfriend, which police found stored in the boyfriend's fingerprint-locked bedroom (where there were no cameras); (2) manipulated the innocuous footage to conjure multiple, wholly forged videos of the boyfriend repeatedly vaginally penetrating the daughter in the living room, with hyper-realistic depictions of the boyfriend and daughter's faces and bodies; (3) in doing so, fabricated the boyfriend penetrating the daughter with the exact sex toys later found in the boyfriend's personal possession; (4) also added hyper-realistic audio to the fabricated videos, including conversations between the boyfriend and the daughter speaking in their actual voices, and the daughter loudly crying out while being sexually abused; and (5) during one such conversation, had the daughter rub her arm, and the boyfriend respond by asking if that was where the daughter "got her shot"—during a video that, petitioner later proved, was date-stamped shortly after the daughter, in actual fact, received two vaccinations at a doctor's office. According to the majority, B.W. would have done all this so convincingly that, upon watching the videos, an FBI agent specializing in child pornography, Family Court, and two Appellate Division panels saw no indication that any portion of the videos was altered, let alone fabricated wholesale (*see* 229 AD3d 1040, 1043 [4th Dept 2024] ["(Family Court) determined that the 'actions, dialog( ), and behavior shown in the videos show no indication of any tampering' "]; *Matter of G.H. (D.K.)*, 229 AD3d 1048, 1051 [4th Dept 2024] [stating, in the boyfriend's separate appeal in these proceedings, that "(the boyfriend), the mother, and the children were all easily identifiable in the videos, and we agree with (Family Court's) determination that the 'actions, dialog,

and behavior shown in the videos show no indication of any tampering.' There were no visible cuts or edits, or jumps in the time stamps on the videos"]).

The majority fails to account for the fundamental question of whether, at the time relevant to this case, video-faking technology was even capable of the wholesale fabrication that the majority imagines. The majority instead misdirects by waving this question away (*see* majority op at 10 & n 5). But to restate the majority's position is to dismantle it. Given the significance that the majority attaches to its conclusion that petitioner insufficiently disproved the possibility these videos were forged (*see* majority op at 8-13 & nn 4-7), how could the fact that such forgery was impossible be "abstract" and "not germane" to the majority's analysis (majority op at 10 & n 5)?

To be clear, the level of fakery required here was not possible, let alone readily available, when these events were captured on video in 2019 or recovered by police in 2022 (*see generally e.g.* Thanh Thi Nguyen et al., *Deep learning for deepfakes creation and detection: A survey*, 223 Comput Vision & Image Understanding, art 103525 [Oct. 2022] [as of 2022, deepfake video technology merely enabled users to convincingly alter or substitute the appearance of people *in videos of actual events*]; Yisroel Mirsky & Wenke Lee, *The Creation and Detection of Deepfakes: A Survey*, 54 ACM Computing Surveys, art 7 [No. 1, Dec. 2020] [same, as of 2020]). Insofar as such videos could be generated at all at the relevant time, the videos at issue here certainly could not be falsified convincingly (*see generally e.g.* Nuha Aldausari et al., *Video Generative Adversarial Networks: A Review*, 55 ACM Computing Surveys, art 30 [No. 2, Jan. 2022] [as of 2022, "(t)he current state of the art for (deepfake videos) suffers from low quality frames or low number of

frames or both"]; Jonathan Ho et al., *Video Diffusion Models*, NIPS'22: Proceedings of the 36th International Conference on Neural Information Processing Systems 8633-8646 [2022] [as of 2022, state-of-the-art deepfake video technology could generate videos not exceeding 128x128-pixel resolution]; *see United States v Schram*, 128 F4th 922, 926 [8th Cir 2025], quoting David Thiel et al., Generative ML and CSAM: Implications and Mitigations 2 [2023] [as of 2023, even "highly photorealistic" deepfake child pornography—a category that comprised "less than one percent of child sexual abuse material" in circulation—"could still be 'visually distinguished as being (computer) generated' "]). I invite the reader to research the state of the technology in and before 2022, including by reading the three nontechnical lay articles cited by the majority, which only further support my position (*see* majority op at 10 n 5), and to reach their own informed conclusion.

The majority is therefore deeply out of touch. Deepfake and other emerging technologies raise thorny evidentiary challenges that our courts will need to grapple with, thoughtfully and with nuance, in cases where they are actually presented. The majority's naïve analysis—essentially, saying the word "deepfake," throwing up its hands without critical thought, and returning an abused child to an abuser's care—cannot be the way forward.[1]

This marks only the beginning of the majority's parade of legal and factual errors. After accepting the impossible premise of fakery, the majority substantively ignores the

[1] Like Judge Troutman, I would affirm the Appellate Division order in all respects.

most powerful indicia of the videos' reliability: the compelling circumstantial evidence of authenticity that petitioner put forth, much of which Judge Troutman's dissent describes (*see* Troutman, J., dissenting op at 3-4). Above all, the Appellate Division affirmed Family Court's factual finding that *the very instrumentalities of the sexual abuse seen on the videos* were recovered by police from the boyfriend's locked bedroom inside the home, which did not have a camera in it (*see* 229 AD3d at 1043). Even assuming, as the majority does, that B.W. somehow saw the boyfriend's specific sex toys in innocent use while accessing the family's living-room camera feed, why would B.W., when later generating videos of fabricated sexual abuse involving total strangers, depict that abuse being committed with specific objects in the boyfriend's personal possession? More to the point, why must the videos' proponent disprove that made-up proposition as a precondition to the threshold step of admitting the videos into evidence in the hearing court's discretion—after which the mother could then challenge the videos' evidentiary weight? After all, parties argue all the time that evidentiary exhibits are not what they purport to be. The majority's novel burden flips the authentication standard on its head, requiring the proponent to disprove unsupported theories of fakery as a prerequisite to mere admissibility.

The circumstantial evidence substantively ignored by the majority does not end there. As revealed by FBI Agent Baranski's testimony, it was the police, not B.W., who ultimately identified the boyfriend, mother, and children as the people seen on the videos. The police made these identifications based on their extensive investigatory work, including an apparent IP address and an email address associated with the security camera's owner that, police discovered, comprised the boyfriend's first initial and last name and the

name of his employer. And, as the majority again fails to acknowledge, petitioner also established an unbroken chain of custody from when the videos were recovered, and "gaps in the chain of custody may be excused when circumstances provide reasonable assurances of the identity and unchanged condition of the evidence. Such gaps go to the weight of the evidence, not its admissibility" (*People v Baez*, 42 NY3d 124, 128 [2024] [alterations omitted], quoting *People v Hawkins*, 11 NY3d 484, 494 [2008]). That too is precisely the case here.

These facts, all the more in combination, render *People v Patterson* (93 NY2d 80 [1999]) fundamentally inapposite (*see* Troutman, J., dissenting op at 6-7), notwithstanding the majority's superficial comparison to that case. Certainly, the circumstantial evidence here, especially the evidence involving the specific instrumentalities of the boyfriend's serial abuse, was absent in *Patterson* and is more than sufficient to refute the majority's bald speculation that these videos depict fictional events. The majority also ignores our observation in *Patterson* itself that "reasonable inferential linkages can ordinarily supply foundational prerequisites" for evidentiary authentication (93 NY2d at 85). So too, in conclusory fashion, the majority purports to distinguish *People v Goldman* (35 NY3d 582 [2020]) after merely reciting its facts (*see* majority op at 13-14). The majority never actually explains its nonsensical assertion that the markedly weaker circumstantial evidence in *Goldman*—which this Court deemed adequate for authentication in a criminal case (*see* 35 NY3d at 595-596)—was somehow more probative than the highly compelling constellation of circumstantial evidence before Family Court here.

Given the majority's conclusion, it is hard to imagine what circumstantial evidence could ever suffice to authenticate a video. The majority papers over this important question by tersely claiming that circumstantial evidence may be "relevant to authentication," yet it fails to explain why this circumstantial evidence was insufficient or what other forms of circumstantial evidence could possibly suffice (*see* majority op at 13). If, as it appears, the majority is effectively holding that circumstantial evidence can never be enough, the majority is unaccountably sweeping aside well settled law recognizing circumstantial evidence as a valid method of authentication (*see* Troutman, J., dissenting op at 5-6).

The majority is not just wrong on the facts and on the law. Its errors will harm child victims. The majority claims not to be requiring "that child victims must testify" in cases like this one (majority op at 14), but that is the predictable effect of its misguided approach. Surely, a child abuser will not testify to the accuracy of a video showing them committing sexual abuse. Nor will a voyeur who happens upon, watches, and saves such child pornography, as B.W. allegedly did here, admit on the witness stand to committing those crimes. Without a cooperation agreement, no competent attorney would allow their client to give such testimony. Unlike the majority, I reject the proposition that Family Court's ability to protect abused children should hinge upon abusers and child pornographers agreeing to cooperate in child-protective proceedings (*see* majority op at 9 n 3).

Recognizing that such testimony was never going to happen, petitioner also properly relied, in part, on Baranski's testimony as an FBI Special Agent who "primarily investigate[s] child pornography related matters" and "perform[s] digital forensic work." Agent Baranski's testimony makes plain that he is indeed a child-pornography expert, not

a mere layperson, but that is how the majority treats him in discounting his testimony as a matter of law (*see* majority op at 8-9, 11-12). And the majority's further assertion that Agent Baranski somehow never opined on the videos' authenticity is incoherent. The majority itself acknowledges Baranski's testimony detailing the circumstances whereby the FBI obtained the videos, and his testimony that he saw nothing "that led [him] to believe that the video footage had been tampered with or altered in any way" (majority op at 12). Yet in the next breath, the majority claims that Agent Baranski did not testify to "whether he examined the videos to look for tampering" or whether he could "offer a learned affirmative opinion that the video was not tampered with" (majority op at 11). The majority's own quotation of his testimony refutes its self-serving account. To state the obvious, it is unsurprising that Agent Baranski did not expressly testify to the absence of wholesale forgery in these videos (*see* majority op at 12), because—to reiterate—the technology that the majority fears *did not then exist*. Again, Agent Baranski's testimony was surely enough to support Family Court's discretionary determination that the videos were adequately authenticated.

With circumstantial evidence of the videos' authenticity and testimony by a child-pornography expert out of the picture, all that remains is testimony by the child victim of the abuse. As Judge Troutman explains (*see* Troutman, J., dissenting op at 9), we cannot—must not—force the choice of either revictimizing child victims by requiring them to testify, or returning these victims to their abusers' care. Tragically, the majority fails to see that its holding will impose this profound harm.

The majority also fails to apprehend the broader consequences of its ruling. Taken to its logical conclusion, the majority's holding radically alters the authentication landscape, with unknown effects of which the majority appears entirely unaware. Precisely what type of expert testimony would the majority now require whenever a litigant cries "deepfake," regardless of whether that incantation has any evidentiary support? The majority's novel requirement of such testimony to rebut even this patently baseless deepfake defense—which must be given by "an expert . . . in video authentication" (majority op at 11)—is unreasoned, in no way supported by *Patterson* (*contra* majority op at 14), and cannot be squared with black letter law recognizing other valid methods of evidentiary authentication.

The majority's holding also marks a significant departure from other jurisdictions' thoughtful approach. The federal Advisory Committee on Evidence Rules (Advisory Committee), for one, has prepared a working draft of a new Federal Rule of Evidence 901 (c) addressing authentication and deepfakes, requiring the exhibit's opponent to put forth evidence sufficient to find that such forgery occurred:

> "(c) Potentially Fabricated Evidence Created by Artificial Intelligence.
>
> > "(1) *Showing Required Before an Inquiry into Fabrication.* A party challenging the authenticity of an item of evidence on the ground that it has been fabricated, in whole or in part, by generative artificial intelligence must present evidence sufficient to support a finding of such fabrication to warrant an inquiry by the court.
> >
> > "(2) *Showing Required by the Proponent.* If the opponent meets the requirement of (1), the item of

> evidence will be admissible only if the proponent demonstrates to the court that it is more likely than not authentic" (Advisory Committee on Evidence Rules, Agenda Book 167 [Nov. 5, 2025], available at https://www.uscourts.gov/sites/default/files/document/2025-11_evidence_rules_commitee_agenda_book_final.pdf).

The draft rule thus "sets out a two-step process for regulating claims of deepfakes" under which "the opponent must set forth enough information for a reasonable person to find that the item has been fabricated in whole or part by the use of generative artificial intelligence" (*id.* at 168 [draft Committee Note accompanying the rule]). This eminently logical proposal recognizes that "a broad claim of 'deepfake' is not enough to put the court and the proponent to the time and expense of showing that the item has not been manipulated" (*id.*; *see also id.* [admonishing that a deepfake "argument that is made without foundation in the evidence" "is subject to the court's inherent authority"]). Sister states and federal courts have likewise held, deepfake technology notwithstanding, that an exhibit's proponent "need not rule out all possibilities that are inconsistent with authenticity, or prove beyond any doubt that the evidence is what it purports to be" (*Mooney v State*, 487 Md 701, 734-735, 321 A3d 91, 111 [2024] [brackets omitted] [specifically discussing deepfakes]; *see e.g. Schram*, 128 F4th at 926 ["(T)he government need not produce evidence to negate a speculative assertion that a child in an image is virtual. . . . On the nearly empty record here, (the defendant's) concern that images shown to the jury depicted virtual children is just speculation unsupported by any concrete facts"]; *People v Gonzales*, 2019 COA 30, ¶ 29, 474 P3d 124, 130 [Colo App 2019] ["the fact that

the falsification of electronic recordings is always possible does not, in our view, justify restrictive rules of authentication that must be applied in every case when there is no colorable claim of alteration" (citing *People v Sangster*, 2014 IL App [1st] 113457, ¶ 51, 8 NE3d 1116, 1127 [2014])], *affd* 2020 CO 71, 471 P3d 1059 [Colo 2020]). As the Reporter to the Advisory Committee has observed, "a contention such as 'it might be a deepfake' or 'deepfakes are easy to do' has to be a nonevent" (Daniel J. Capra, *Deepfakes Reach the Advisory Committee on Evidence Rules*, 92 Fordham L Rev 2491, 2506 [2024]). Yet the majority rests its holding on sheer surmise that because B.W. had some "technical savvy," he might have created a deepfake (majority op at 9 n 4). The majority identifies no legal authority supporting its reactionary approach.

Chaos will ensue. For example, must every proponent of surveillance footage now introduce expert forensic testimony to authenticate it, in any proceeding in any of our courts? What about a criminal defendant offering a video establishing an alibi, if the People cry "deepfake" in response? Must the defendant either find and pay for an authentication expert, or take the stand to testify to their personal knowledge of the video's accuracy—and waive their Fifth Amendment privilege in the process? Are videos such as traffic cameras, video doorbell cameras, and the like now subject to the majority's presumption of deepfake forgery? More broadly still, what about every other medium susceptible to fakery, such as writings, signatures, and still images? The majority purports to address videos, but I am unable to discern any principled reason why its holding does not equally apply to every other form of evidentiary exhibit. The majority's ho-hum approach blithely raises all of these questions and more.

The majority opinion is therefore more than shortsighted. It is troubling, and its consequences will be grave. In practicality, in child-protective proceedings, the majority places the onus on child victims to authenticate videos that their abusers and pornographers create. Above all, the majority returns a child victim to an abuser's care by holding for the first time—in a case predating the possibility of wholesale deepfake video forgery—that sheer speculation of such forgery renders sex-abuse videos inadmissible absent testimony by an observer, a participant, or an expert. In the wake of the majority's reckless holding, Family Court, criminal, and civil litigants alike will surely raise a deepfake defense, however baseless, when faced with unfavorable evidentiary exhibits of all kinds, and the most vulnerable among us will suffer the consequences.

I dissent.

Orders reversed, without costs, and petitions dismissed. Opinion by Chief Judge Wilson. Judges Rivera, Cannataro and Halligan concur. Judge Troutman dissents in an opinion in which Judges Garcia and Singas concur, Judge Singas in a separate dissenting opinion in which Judge Garcia concurs.

Decided February 17, 2026