North Carolina Criminal Law
AT THE UNC SCHOOL OF GOVERNMENT

March 25, 2024

Surveillance Video- When It Comes In and When It Doesn't

Daniel Spiegel

Video evidence authentication has received a **fair amount of treatment** on this blog. The topic remains an area of practical significance given the prevalence of video evidence in criminal trials and how common it is for the prosecution's case to hinge on the admission of video. We are increasingly a **video-focused** society. Between home security cam, doorbell cam, body-worn cam, in-car cam, pole cam, and even **parking lot cam**, juries increasingly expect to see video, whether the incident in question occurred outside a home, near a business, or on the roadside.

In this post, I will focus on surveillance video. As discussed by my colleague Jeff Welty, a party generally authenticates surveillance video in one of **two ways**. The first method involves calling a witness who was present for the events captured on video and eliciting testimony that the video "fairly and accurately depicts" what happened. The video is then admitted for illustrative purposes. The second method, often referred to as the "silent witness foundation," involves eliciting testimony that the recording equipment was functioning properly and that the video introduced at trial shows the same footage as that captured by the recording. The video can then be admitted for substantive purposes. *See* G.S. 8-97; *also see* **this prior post** for a discussion of the (generally minimal) difference between illustrative and substantive purposes.

When the State seeks to admit surveillance video at trial, the first method generally relies on a civilian such as a store clerk or loss prevention officer who was present on scene and observed the incident. The second method usually requires a similar individual, or perhaps a store manager or third-party technician, who is familiar with the recording equipment and who retrieved the footage from the system.

Getting surveillance video into evidence is not always as simple as one might expect. Authenticating witnesses may be difficult to locate with multiple corporate layers to penetrate, or the ownership of the business may have changed hands while the case is pending. The witnesses may have left the area, or they may be uninterested or fearful when it comes time to assist the prosecution.

A recent Court of Appeals case, ***State v. Jones***, 288 N.C. App. 175 (2023), got my attention because the authenticating witness the State relied on was not one of the witnesses one would expect. Rather than calling one of the witnesses described above, the State relied exclusively on the testimony of the investigating officer, albeit with some reference to what a civilian saw.

The video authentication in *Jones.* The surveillance video at issue in *Jones* captured a prior breaking and entering incident that the State introduced as 404(b) evidence. The officer testified at trial that:

1. The video exhibit showed the same footage she had reviewed the night of the incident;

2. the surveillance system was working correctly "to her knowledge" (she presumably lacked familiarity with the recording device); and

3. the footage on the video matched what the homeowner described had occurred.

This third statement may set off some alarm bells as the homeowner was not present at trial and the officer's testimony as to what the homeowner said appears to be hearsay. However, the case serves as a good reminder of Rule 104(a), which provides that the rules of evidence do not apply when the court is determining "preliminary questions" concerning the "admissibility of evidence." Per Rule 104(a), it was permissible for the trial court to consider the hearsay statement, offered for the truth of what the homeowner saw, for the limited purpose of determining whether the video evidence was accurate and reliable.

Considering these three pieces of testimony together, the Court of Appeals concluded that the surveillance video was adequately authenticated by the State and the trial court did not err in admitting the exhibit.

Compare with *Moore.* Compare the *Jones* case with ***State v. Moore***, 254 N.C. App. 544 (2017), where the Court of Appeals determined that the trial court erred in

admitting surveillance video. In *Moore*, the officer went to a gas station/convenience store to retrieve surveillance video the day after an incident of fleeing to elude arrest. However, the manager lacked authority to make a copy of the video. The officer took out his cell phone and recorded the footage displayed on the store's equipment. He then downloaded that cell phone video and made a copy for trial. At trial, he testified that the video introduced accurately showed the footage he had reviewed in the store. Furthermore, the store clerk testified that the defendant visited the store on the day in question and that the defendant could be seen on the video introduced in court. However, the store clerk never testified that the video accurately depicted events he had observed, and no one testified to the condition of the store's recording equipment. The *Moore* court concluded that the State did not present an adequate foundation to reliably admit the cell phone video of the surveillance footage.

In *Jones*, the Court of Appeals distinguished *Moore* and determined that the officer's testimony that the video at trial showed the same footage as that he reviewed shortly after the incident, in combination with her testimony that the homeowner's description of events matched the video, passed a threshold of reliability and was properly admitted.

Part of a trend? The analysis in *Jones* may be part of a larger trend where appellate courts are becoming less strict when it comes to the authentication of video evidence. The State got by in *Jones* with an officer who had limited familiarity (if any) with the recording equipment, and the officer only testified to a general congruence between what the homeowner told her and what the video showed. The officer did, of course, testify that the footage she saw on the night in question matched the video introduced at trial, which is compelling evidence of authenticity. But that same piece of testimony was not enough for the State in *Moore* from 2017. And when one compares *Jones* with a case that well predates *Moore*, *State v. Mason*, 144 N.C. App. 20 (2001), the court's analysis appears to have evolved. The *Mason* court 1) seemed to require some expertise with the recording technology, not mere familiarity; 2) was unsatisfied with a witness who was present on scene and testified to the accuracy of a portion of the video but not another, "more significant," part; and 3) placed emphasis on the lack of a chain of custody in ultimately concluding that it was error to admit the video (note that the North Carolina Supreme Court has since held that a complete chain of custody is not necessary to authenticate video in *State v. Snead*, 368 N.C. 811 (2016)).

In this age when video is ubiquitous and routinely relied upon, one might think it proper for the court to give less scrutiny to the authenticity of surveillance video. Under Rule 901, surveillance video would seem to be admissible without the moving party having to meet a particularly high burden. Rule 901(b)(9) provides for authentication of evidence that derives from an automated process, and Rule 901(a) appears to set a relatively low bar; there must only be "evidence sufficient to support a finding that the matter in question is what its proponent claims." *See State v. Snead*, 368 N.C. 811 (2016); *see also State v. Ford*, 245 N.C. App. 510 (2016) (the "burden to authenticate under Rule 901 is not high – only a *prima facie* showing is required").

On the other hand, some might argue that courts should remain vigilant with this type of evidence given the rise of "**deep fakes**" and AI-altered video. Perhaps courts should exercise a stronger gatekeeping function as there is more reason to be concerned that a video may have been tampered with. *See* Matthew Ferraro and Brent Gurney, ***The Other Side Says Your Evidence Is A Deepfake. Now What?***, Law360 (Dec. 21, 2022). When weighing the admissibility of other types of digital evidence, however, courts sometimes seem to require that the party challenging the authenticity of digital evidence develop some facts to show a motive to fabricate or reason to believe that the evidence has been edited or manipulated. *See, e.g.*, *United States v. Farrad*, 895 F.3d 859 (6th Cir. 2018) (Facebook photos were properly admitted under Federal Rule 901 where no specific evidence was presented by the defense tending to show the images might have been photoshopped or altered, nor did defense counsel develop such arguments on cross-examination).

Surveillance video chart. In reviewing *Jones*, *Moore*, and several other North Carolina appellate cases, it is not a simple task to delineate the quantum of evidence sufficient to authenticate surveillance video. I prepared the chart below, which summarizes the video authentication details from several recent cases, in an effort to distill the key facts that determined whether the video was or was not properly admitted. Reviewing the chart, it is apparent that there is not one way to authenticate a video. Rather, the appellate courts consider the various pieces of foundational testimony in a cumulative manner and then decide whether the video evidence is sufficiently reliable to be admitted.

The chart can be found **here**.