Authenticating Photographs Taken from Social Media Sites

Author : Jeff Welty

Categories : Evidence, Uncategorized

Tagged as : authentication, Evidence, facebook, myspace, photographs, pictures, social media

Date : May 19, 2014

Suppose that the defendant is charged with a gang-related murder. The State seeks to establish that the defendant is a gang member by introducing a photograph that a detective found on the defendant's Facebook page. The photograph shows the defendant flashing gang signs. The defendant argues that the picture can't be authenticated, because digital photographs can easily be altered, and because the State does not have a witness who was present when the picture was taken and who can testify that the image is a fair and accurate representation. Is the picture admissible?

The usual ways of authenticating photographs won't work here. Photographs are usually introduced to illustrate a witness's testimony, based on the witness's recitation that the witness was present when the photographs were taken and that the photographs "fairly and accurately depict" what the witness saw. *See*, *e.g.*, *State v. Vick*, 341 N.C. 569 (1995). When such a witness is available, this foundation is sufficient for digital photographs just as it is for film photography. G. Michael Fenner, *The Admissibility of Web-Based Evidence*, 47 Creighton L. Rev. 63 (2013) ("A photograph from a Facebook page showing the criminal defendant half-dressed and fully-drunk at a party during the thirty-one days when she had not yet reported that her nearly-three-year-old daughter was missing, or during the five months between the time her daughter was reported missing and the little girl's body was found, can be authenticated by someone who was at the party, remembers when the party occurred, and can identify the defendant from the photo. It does not matter where the photo was found: on Facebook, on a camera's flash memory card, or in a shoebox. They are all just photos and can be authenticated in the ordinary, old-fashioned way. When it is irrelevant whether the Facebook page was the source of the photo, then just because it was found on the web does not make authentication any more complicated.") However, in our hypothetical, that method of authentication isn't available to the State.

Sometimes it is possible to authenticate photographs even when there is no witness who has first-hand knowledge of the accuracy of the images. An analogous issue often arises with video recordings, and there is a body of case law concerning when surveillance videos may be admitted as "silent witnesses" despite the lack of a human witness who can confirm the recordings' accuracy. In general, authentication requires testimony from someone familiar with the surveillance system about how it worked, how the camera was functioning at the time of the recording, and how the video was copied from the system and preserved unaltered for trial. *See generally Bowman v. Scion,* __ N.C. App. __, 737 S.E.2d 384 (2012). A similar foundation could authenticate a surveillance photograph, but in our hypothetical, the State doesn't know how the picture was taken, and so can't authenticate the picture in this way either.

But other methods of authentication may be possible. Under Rule 901(a), "[t]he requirement of authentication . . . is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." The Rule lists several methods of authentication, but they are "[b]y way of illustration only, and not by way of limitation." N.C. R. Evid. 901(b). In our hypothetical, there are a few avenues the State might pursue to authenticate the photograph.

The fact that the picture was posted to the defendant's account. With electronic communications like emails and text messages, the key to authentication is establishing who likely authored the communication, and it is powerful evidence of authorship when a communication comes from an account linked to a specific person. By contrast, with a photograph, it doesn't really matter who took the picture, and the fact that the picture was posted to the defendant's

account doesn't shed much light on who took it anyhow. But the State still has a reasonable argument that the fact that the picture was on the defendant's Facebook page tends to support its authenticity. Courts have noted that digital images can be altered. *People v. Lenihan*, 30 Misc.2d 289 (N.Y. Sup. 2010) (defendant properly was barred from cross-examining prosecution witnesses about "photographs that [the defendant's] mother downloaded from [MySpace]" suggesting that the witnesses were gang members; "[i]n light of the ability to 'photo shop', edit photographs on the computer, defendant could not authenticate the photographs"). However, the fact that the defendant chose to display the picture on his own page suggests that he didn't think the picture was misleading or falsified, and tends to support its genuineness.

The context in which the picture is placed. The relationship between the picture and the other content on the defendant's Facebook page is also relevant. If the page is devoted to the defendant's love of puppetry and ceramic unicorns, and the picture at issue is the only thing on the page suggestive of gang affiliation, it is more likely that the picture is satirical, misleading, or was planted on the page by a nefarious interloper. If the page is an unbroken string of drug and gang references, the picture is more likely to be genuine. *People v. Valdez*, 201 Cal. App. 4th 1429 (Cal. Ct. App. 4th Dist. 2011) (the prosecution adequately authenticated photographs printed from the defendant's MySpace page that showed him making gang signs; the overall content of the page, including the interests reflected there and responses by the defendant's friends and family, "suggested the page belonged to [the defendant] rather than someone else by the same name, who happened to look just like him"; and the photograph was in keeping with the gang-related theme of the page, which tended to support its authenticity).

Metadata. Finally, digital photographs often contain metadata – embedded information about when a picture was taken, where it was taken, and the camera with which it was taken. In some instances, metadata might be relevant to authentication. If a witness with the proper expertise were able to review the metadata and to testify that the metadata revealed that the picture had not been altered, that also would tend to support authentication. *Cf. People v. Buckley*, 185 Cal. App. 4th 509 (Cal. Ct. App. 2nd Dist. 2010) (prosecution was wrongly allowed to introduce a photograph, obtained from a witness's MySpace page, of the witness flashing gang signs; however, based on prior case law, the court suggested that the picture may have been admissible with "evidence of when and where the picture was taken" and testimony from "a photographic expert . . . that the picture was not a composite and had not been faked").

How high a hurdle is authentication? The hypothetical at the beginning of this post didn't include any information about metadata or the other contents of the defendant's Facebook page. Plus, the law isn't settled in this area, particularly in North Carolina. Therefore, I don't have a conclusive answer to my own question, but as a practical matter, the answer may hinge in part on how certain a court must be about authenticity before it will allow the evidence to be introduced. The black-letter law is that authentication is a relatively low hurdle. *State v. Mercer*, 89 N.C. App. 714 (1988) (noting approvingly that "federal courts have held that a *prima facie* showing, by direct or circumstantial evidence, such that a reasonable juror could find in favor of authenticity, is enough"). But courts around the country seem to be approaching digital evidence carefully, and perhaps requiring greater certainty about the nature of digital evidence before admitting it.