19 A.3d 415
Maryland Court of Appeals

Griffin v. State

2011

BATTAGLIA, J.

In this case, we are tasked with determining the appropriate way to authenticate, for evidential purposes, electronically stored information printed from a social networking website, in particular, MySpace.

* * *

Griffin was charged in numerous counts with the shooting death, on April 24, 2005, of Darvell Guest at Ferrari's Bar in Perryville, in Cecil County. During his trial, the State sought to introduce Griffin's girlfriend's, Jessica Barber's, MySpace profile to demonstrate that, prior to trial, Ms. Barber had allegedly threatened another witness called by the State. The printed pages contained a MySpace profile in the name of "Sistasouljah," describing a 23 year-old female from Port Deposit, listing her birthday as "10/02/1983" and containing a photograph of an embracing couple. The printed pages also contained the following blurb:

> FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!

* * *

The potential for fabricating or tampering with electronically stored information on a social networking site, thus poses significant challenges from the standpoint of authentication of printouts of the site, as in the present case. Authentication, nevertheless, is generally governed by Maryland Rule 5-901, which provides:

> (a) General provision. The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

Potential methods of authentication are illustrated in Rule 5-901(b). The most germane to the present inquiry are Rules 5-901(b)(1) and 5-901(b)(4), which state:

> (b) Illustrations. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this Rule:
>
> (1) Testimony of witness with knowledge. Testimony of a witness with knowledge that the offered evidence is what it is claimed to be.
>
> * * *
>
> (4) Circumstantial evidence. Circumstantial evidence, such as appearance, contents, substance, internal patterns, location, or other distinctive characteristics, that the offered evidence is what it is claimed to be.

We and our colleagues on the Court of Special Appeals have had the opportunity to apply the tenets of Rule 5-901(b)(4) to a toxicology report, *State v. Bryant*, 361 Md. 420, 761 A.2d 925 (2000), to recordings from 911 emergency calls, *Clark v. State*, 188 Md.App. 119, 981 A.2d 666 (2009), and to text messages received on the victim's cellular phone, *Dickens v. State*, 175 Md. App. 231, 927 A.2d 32 (2007), but neither we nor our appellate brethren heretofore has considered the Rule's application to authenticate pages printed from a social networking site.

Rather, we turn for assistance to the discussion in *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D.Md. 2007), wherein Maryland's own Magistrate Judge Paul W. Grimm, a recognized authority on evidentiary issues concerning electronic evidence, outlined issues regarding authentication of electronically stored information, in e-mail, websites, digital photographs, computer-generated documents, and internet postings, etc. with respect to Rule 901 of the Federal Rules of Evidence:

> (a) GENERAL PROVISION. The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.
>
> (b) ILLUSTRATIONS. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:
>
> (1) *Testimony of Witness With Knowledge.* Testimony that a matter is what it is claimed to be.
>
> * * *
>
> (4) *Distinctive Characteristics and the Like.* Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

Regarding Rule 901(a), Judge Grimm iterated in *Lorraine* that the "requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims," to insure trustworthiness. *Id.* at 541-42. Judge Grimm recognized that authenticating electronically stored information presents a myriad of concerns because "technology changes so rapidly" and is "often new to many judges." *Id.* at 544. Moreover, the "complexity" or "novelty" of electronically stored information, with its potential for manipulation, requires greater scrutiny of "the foundational requirements" than letters or other paper records, to bolster reliability. *Id.* at 543-44, quoting Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 900.06[3] (Joseph M. McLaughlin ed., Matthew Bender 2d ed.1997).

In the present case, Griffin argues that the State did not appropriately, for evidentiary purposes, authenticate the pages allegedly printed from Jessica Barber's MySpace profile, because the State failed to offer any extrinsic evidence describing MySpace, as well as indicating how Sergeant Cook obtained the pages in question and adequately linking both the profile and the "snitches get stitches" posting to Ms. Barber. The State counters that the photograph, personal information, and references to freeing "Boozy" were sufficient to enable the finder of fact to believe that the pages printed from MySpace were indeed Ms. Barber's.

We agree with Griffin and disagree with the State regarding whether the trial judge abused his discretion in admitting the MySpace profile as appropriately authenticated, with Jessica Barber as its creator and user, as well as the author of the "snitches get stitches" posting, based upon the inadequate foundation laid. We differ from our colleagues on the Court of Special Appeals, who gave short shrift to the concern that "someone other than the alleged author may have accessed the account and posted the message in question." *Griffin*, 192 Md.App. at 542, 995 A.2d at 805. While the intermediate appellate court determined that the pages allegedly printed from Ms. Barber's MySpace profile contained sufficient indicia of reliability, because the printout "featured a photograph of Ms. Barber and [Petitioner] in an embrace," and also contained the "user's birth date and identified her boyfriend as `Boozy,'" the court failed to acknowledge the possibility or likelihood that another user could have created the profile in issue or authored the "snitches get stitches" posting. *Id.* at 543, 995 A.2d at 806.

We agree with Griffin that the trial judge abused his discretion in admitting the MySpace evidence pursuant to Rule 5-901(b)(4), because the picture of Ms. Barber, coupled with her birth date and location, were not sufficient "distinctive characteristics" on a MySpace profile to authenticate its printout, given the prospect that someone other than Ms. Barber could have not only created the site, but also posted the "snitches get stitches" comment. The potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that Ms. Barber was its creator and the author of the "snitches get stitches" language.

* * *

The State refers us . . . to *In the Interest of F.P.*, 878 A.2d 91 (Pa.Super.Ct.2005), in which the Pennsylvania intermediate appellate court considered whether instant messages were properly authenticated pursuant to Pennsylvania Rule of Evidence 901(b)(4), providing that a document may be authenticated by distinctive characteristics or circumstantial evidence. In the case, involving an assault, the victim, Z.G., testified that the defendant had attacked him because he believed that Z.G. had stolen a DVD from him. The hearing judge, over defendant's objection, admitted instant messages from a user with the screen name "Icp4Life30" to and between "WHITEBOY Z 404." *Id.* at 94. Z.G. testified that his screen name was "WHITEBOY Z 404" and that he had printed the instant messages from his computer. In the transcript of the instant messages, moreover, Z.G. asked "who is this," and the defendant replied, using his first name. Throughout the transcripts, the defendant threatened Z.G. with physical violence because Z.G. "stole off [him]." *Id.* On appeal, the court determined that the instant messages were properly authenticated through the testimony of Z.G. and also because "Icp4Life30" had referred to himself by first name, repeatedly accused Z.G. of stealing from him, and referenced the fact that Z.G. had told high school administrators about the threats, such that the instant messages contained distinctive characteristics and content linking them to the defendant. *In the Interest of F.P.* is unpersuasive in the context of a social networking site, because the authentication of instant messages by the recipient who identifies his own "distinctive characteristics" and his having received the messages, is distinguishable from the authentication of a profile and posting printed from MySpace, by one who is neither a creator nor user of the specific profile.

. . . [W]e should not be heard to suggest that printouts from social networking sites should never be admitted. Possible avenues to explore to properly authenticate a profile or posting printed from a social networking site, will, in all probability, continue to develop as the efforts to evidentially utilize information from the sites increases. *See, e.g.*, Katherine Minotti, Comment, *The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, 60 S.C.L.Rev. 1057 (2009). A number of authentication opportunities come to mind, however.

The first, and perhaps most obvious method would be to ask the purported creator if she indeed created the profile and also if she added the posting in question, i.e. "[t]estimony of a witness with knowledge that the offered evidence is what it is claimed to be." Rule 5-901(b)(1). The second option may be to search the computer of the person who allegedly created the profile and posting and examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question. One commentator, who serves as Managing Director and Deputy General Counsel of Stroz Friedberg, a computer forensics firm, notes that, "[s]ince a user unwittingly leaves an evidentiary trail on her computer simply by using it, her computer will provide evidence of her web usage." Seth P. Berman, et al., *Web 2.0: What's Evidence Between "Friends"?*, Boston Bar J., Jan.-Feb.2009, at 5, 7.

A third method may be to obtain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it. This method was apparently successfully employed to authenticate a MySpace site in *People v. Clevenstine*, 68 A.D.3d 1448, 891 N.Y.S.2d 511 (2009). In the case, Richard Clevenstine was convicted of raping two teenage girls and challenged his convictions by asserting that the computer disk admitted into evidence, containing instant messages between him and the victims, sent via MySpace, was not properly authenticated. Specifically, Clevenstine argued that "someone else accessed his MySpace account and sent messages under his user-name." *Id.* at 514. The Supreme Court of New York, Appellate Division, agreed with the trial judge that the MySpace messages were properly authenticated, because both victims testified that they had engaged in instant messaging conversations about sexual activities with Clevenstine through MySpace. In addition, an investigator from the computer crime unit of the State Police testified that "he had retrieved such conversations from the hard drive of the computer used by the victims." *Id.* Finally, the prosecution was able to attribute the messages to Clevenstine, because a legal compliance officer for MySpace explained at trial that "the messages on the computer disk had been exchanged by users of accounts created by [Clevenstine] and the victims." *Id.* The court concluded that such testimony provided ample authentication linking the MySpace messages in question to Clevenstine himself.