FEATURE
CRIMINAL LAW

THE JUSTICE SYSTEM NEEDS AN UPDATE
AUTHENTICATION AND ADMISSIBILITY IN THE WAKE OF APPLE'S RECENT REVISIONS TO ITS MESSAGING APPLICATION

BY ERIC NEMECEK

Apple recently announced that it has added three major features to its messaging application, iMessages, *to wit*: if the message is an iMessage, not an SMS text, then users will be able to edit messages, recall messages sent by mistake, and snooze texts so users can handle them later. *See* Kif Leswing, *et al.*, *Here's everything Apple just announced: New MacBook Air, MacBook Pro, M2 chip, iPhone software and more*, CNBC (Jun. 6, 2022, 6:26 PM), https://www.cnbc.com/2022/06/06/apple-wwdc-live-updates-ios-16.html.

The announcement was accompanied by a short video demonstrating how these new features function. Assuming these features operate as represented by Apple and depicted in the video, users will now be able to alter — and even erase — text message communications in real time. While these updates may be a welcome change for Apple's customers, they raise serious concerns within the context of the judicial system, particularly as it relates to the reliability and admissibility of the electronic messages.

Overview of Authentication, the Best Evidence Rule, and Admissibility

Electronic communications are subject to the same admissibility requirements as other forms of evidence — namely, the proffered evidence must first be determined to be relevant. *See, e.g.,* Fed. R. Evid. 401; Ohio Evid.R. 401. Once the evidence is determined to be relevant, both federal and state rules of evidence require that the proponent establish that the proffered item is authentic – in other words, that the item is what the proponent claims it to be. *See, e.g.,* Fed. R. Evid. 901(a); Ohio Evid.R. 901(A); *see also* Weissenberger, *Ohio Evidence Treatise,* § 901.1 (2010) ("[T]he function of authentication or identification is to establish ... a connection between the evidence offered and the relevant facts of the case"). This nexus is a necessary precondition to admissibility as the object or item is of no relevance if it cannot be attributed to or otherwise connected with a particular person, place, or issue in a case. *Id.*

The Rules impose additional admissibility requirements when the evidence sought to be introduced is a writing, recording, or photograph, particularly where the document is a duplicate copy — either printed or manufactured — of the original.[1] In such instances, apart from identifying the authenticity of the evidence, the writing must also be shown to be a true and accurate copy of the original.[2]

Thus, there are two (2) interrelated components to the admissibility of writings, recordings or photographs, both of which serve to ensure that the evidence is properly vetted before being introduced for the trier of fact's consideration: first, the proponent must prove the identity of the individual who authored the writing; second, the proponent must establish that the writing is a true and accurate copy of the original.

Establishing the author's identity is particularly important within the context of electronic communications "such as a Facebook message, an e-mail or cell phone text message, [which] could be generated by someone other than the named sender." *State v. Eleck*, 23 A.3d 818, 822 (Conn. App. Ct. 2011). "This is true even with respect to accounts requiring a unique user name and password, given that account holders frequently remain logged in to their accounts while leaving their computers and cell phones unattended." *Id.*

Similarly, the purpose underlying the Best Evidence Rule "is to promote accurate fact-finding[,] by reducing the risk of 1) 'mistransmission of critical facts;' 2) fraud; and 3) incompleteness." *United States v. Condry*, 2021 WL 5756385, *1 (N.D. Okla. Dec. 3, 2021), *citing United States v. Chavez*, 976 F.3d 1178, 1194 (10th Cir. 2020). Under this exception, courts have held that a duplicate is inadmissible when the proponent offers a document that fails to reproduce important or critical parts of an original, and the opponent establishes that the remainder is needed for some purpose such as cross-examination. *See, e.g.,* Fed. R. Evid. 1003 Advisory Committee's Note; *Amoco Prod. Co. v. United States*, 619 F.2d 1383, 1391 (10th Cir. 1980).

Neither the Rules nor precedent case law establish a clear test for determining when the opponent of a duplicate raises a genuine question as to the authenticity of the original under the Best Evidence Rule. Thus, despite the important interests served by the Rule, evidentiary hurdles are minimal with respect to authenticating printouts as accurate copies — a witness who has seen the email, text message or instant message need only testify that a printout offered is an accurate reproduction.

Electronic Communications

Electronic messages can be authenticated by the testimony of a witness with knowledge or by distinctive characteristics of the item, including circumstantial evidence such as the author's screen name or monikers, customary use of emoji or emoticons, the author's known phone number, the reference to facts that are specific to the author, or reference to facts that only the author and a small number of other individuals may know.

Although "[t]estimony that a person received a text or email from another is not sufficient, by itself, to authenticate the identity of the sender," *see* Charles W. Ehrhardt, 1 *West's Fla. Practice Series* § 901.1a (2020), other factors can circumstantially authenticate the text. *See, e.g., United States v. Siddiqui*, 235 F. 3d 1318, 1322 (11th Cir. 2000); *Pavlovich v. State*, 6 N.E. 3d 969, 978-79 (Ind. Ct. App. 2014) (text messages authenticated by witness who testified that they recognized the defendant's voice on the outgoing voicemail and that the messages from the phone number in question indicated familiarity with the witness's escort business, the prior meeting between the witness and defendant and their prior discussion); *compare Commonwealth v. Koch*, 39 A. 3d 996, 1005 (Pa. Super. Ct. 2011) (text messages not properly authenticated where there was no testimony from the persons who sent or received the text messages and no contextual clues).

Jurisdictional Approach to Admissibility of Electronic Communications

Historically, cases involving "complaints that a duplicate was admitted over an objection asserting the existence of a genuine question of authenticity reject the claim." Olin Guy Wellborn III, *The "Best Evidence" Article of the Texas Rules of Evidence*, 18 St. Mary's L.J. 99, 114 (1986). While the majority of courts continue to apply a relatively low burden for admitting duplicate writings or recordings, some judges have taken a more stringent approach with respect to electronic evidence. For instance, the Superior Court of Pennsylvania recently held that screen shots of Facebook posts are insufficient to authenticate authorship and/or introduce as evidence. *See Commonwealth v. Mangel*, 2018 PA Super. 57. Likewise, courts in Georgia, Washington, and Massachusetts have imposed more stringent requirements for authenticating content derived from social media accounts. *See, e.g., Brown v. State*, 796 SE 2d 283 (Ga. 2017) (State failed to properly authenticate cropped screenshot of a YouTube Video, incriminating Facebook posts, and a photograph downloaded from Twitter); *State v. Kolanowski*, 197 Wash. App. 1054 (2017) (affirming exclusion of Facebook screenshot due to improper foundation and lack of authentication); *Commonwealth v. Purdy*, 459 Mass. 442 (2011) ("Evidence that the defendant's name is written as the author of an email or that the electronic communication originates from an email or a social networking Web site such as Facebook ... that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant").

The Prosecution of Danny Kay

The prosecution of Danny Kay serves as a prime example of what can happen when courts apply lax standards of admissibility to electronic evidence. *See Danny Steven Kay v. Regina* [2017] EWCA Crim 2214. Kay was accused of raping a 16-year-old female[3] on the sofa of his living room in Derby, England. Kay and the young woman had exchanged messages on Facebook, which she provided to the police. *Id.* Kay knew the messages were incomplete, but he was unable to find the messages in his Facebook account, and his attempts to retrieve them directly from Facebook proved fruitless. He was found guilty of the offense and sentenced to 4 ½ years in prison. *Id.*

Nearly three years later, Kay's attorney was able to recover all the messages from an archived folder in Kay's Facebook account, which confirmed that the accuser had selectively deleted messages from her Facebook account that showed the sexual activity had been consensual. *Id.* The appellate court unanimously quashed Kay's conviction, noting: "[w]e have come to the conclusion that, in a case of one word against another, the full Facebook message exchange provides very cogent evidence both in relation to the truthfulness and reliability of A, who, in any event, gave a series of contradictory accounts about other relevant matters, and the reliability of the applicant's account and his truthfulness." *Id.*

Ethical Considerations

Apple's recent modifications may also implicate certain ethical obligations imposed on counsel. Specifically, lawyers must render competent representation, which necessarily requires attorneys to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." Model Rules of Prof'l Conduct r. 1.1, cmt. 8 (Am. Bar Ass'n 1983).[4] Ignorance of technological developments such as the recent changes to various functions on Apple's iPhone can conceivably constitute grounds for ineffective assistance of counsel. *See, e.g., Cannedy v. Adams*, 706 F.3d 1148 (9th Cir. 2013) (defense attorney's failure to investigate AOL Instant Messages sent by victim constituted ineffective assistance of counsel).

In addition to contesting the authenticity or admissibility of electronic evidence, counsel may also need to undertake efforts to try and establish that the proposed evidence is incomplete or otherwise objectionable, which can be accomplished by retaining an expert to conduct an independent forensic examination of the electronic device(s) and/or attempting to recover deleted messages from iCloud or iTunes (if the iPhone was previously backed up through those platforms) or with the assistance of reputable third-party software.

Likewise, lawyers must instruct clients to not alter, destroy, or otherwise tamper with messages that may be relevant to the pending — or impending — litigation. *See, e.g., Allied Concrete Co. v. Lester*, 736 S.E.2d 699 (Va. 2013) (court imposed $722,000.00 in sanctions and suspended plaintiff's attorney for 5 years where plaintiff's paralegal instructed plaintiff to delete 16 Facebook photos during pendency of wrongful death lawsuit).

Conclusion

The recent updates announced by Apple present similar concerns to those that materialized in the prosecution of Danny Kay. The ease with which a person can unilaterally alter or delete messages undoubtedly raises genuine issues as to the authenticity or reliability of a particular writing. Accordingly, counsel must educate courts and practitioners on these recent technological developments in order to competently and effectively object to the admissibility of said evidence at trial. Additionally, counsel should consider the efficacy of attempting to retrieve deleted messages, either with the assistance of third-party software or by retaining an expert to conduct an independent forensic examination of the particular device — or devices — that purportedly sent or received the messages at issue.

[1] Every state has either adopted a counterpart to Federal Rule 1003 or some version of the similar Uniform Photographic Copies of Business and Public Records as Evidence Act. *See* Jeffrey S. Kinsler & Anne R. Keyes MacIver, *Demystifying Spoliation of Evidence*, 34 Tort & Ins. L.J. 761, 779–82 (1999).

[2] This Rule, commonly referred to as the "Best Evidence Rule," has been adopted, verbatim or in substance, by every jurisdiction that has promulgated or enacted the Rules with the exception of Maine, which still adheres to the common law principle of requiring an original document, writing, recording or photograph. *See* 2 Joseph & Saltzburg, *Evidence in America* (1987 & Supp. 1994).

[3] Sixteen is the age of consent in England. *See* Sexual Offences (Amendment) Act of 2000 (c. 44), https://www.legislation.gov.uk/ukpga/2000/44/contents.

[4] As of September 2017, 28 States had expressly recognized and formally adopted this Comment regarding ethical competence as extending to technology, including social media. Even jurisdictions not formally adopting the Comment have issued advisory opinions and guidelines expressly noting social media ethics requirements. *See, e.g.,* New Hampshire Op. 2012-13/04; California Op. 2015-193.

Eric Nemecek is Partner at Friedman and Nemecek, L.L.C., a criminal defense law firm. He has handled an array of complex criminal matters in both state and federal courts throughout the U.S. and internationally. Many of these cases fall within the ambit of "cyber crimes," including violations of the Computer Fraud and Abuse Act as well as other computer and technology-based offenses. He is actively involved in the American Bar Association, serving as a co-chair of the Cybercrime Committee for the American Bar Association since 2011 and previously as a Delegate for the Young Lawyer's Division. Mr. Nemecek is also the Past Chair of the CMBA's Criminal Law Section. He has been a CMBA member since 2010. He can be reached at (216) 928-7700 or ecn@fanlegal.com.