Catholic University Journal of Law and Technology

Volume 26 | Issue 1 Article 3

2018

Mobile Instant Messaging Evidence in Criminal Trials

Youngjin Choi

MOBILE INSTANT MESSAGING EVIDENCE IN CRIMINAL TRIALS

Youngjin Choi[+]

Mobile instant messaging ("MIM") applications ("app(s)") like WhatsApp, WeChat, and Line allow mobile users to send real-time text messages, voice messages, picture messages, video messages, or files to individuals or groups of friends.[1] The evolution and rise of smartphone technologies, along with the

+ Assistant Public Defender, Cattaraugus County Office of the Public Defender. J.D. Northwestern University Pritzker School of Law; B.A. University of Southern California. I thank Director Juliet Sorensen, without whom this comment would not exist. I also thank the staff of the *Catholic University Journal of Law and Technology* for their excellent work on this Comment. I also thank Mr. Darryl Bloom, Mr. Shane Booth, Ms. Paula Bullers, Mr. Mark Cunningham, Ms. Gabi DiBella, Ms. Margaret Gilroy, Ms. Linda Lovell, Ms. Amy Minner, Ms. Kim Payne, Mr. Ben Smith, Ms. Karen Todd, Ms. Dawn Westfall, Mr. Mark Williams, and Mr. Philippe Yates at the Cattaraugus County Office of the Public Defender; Ms. Martina Avalos, Mr. Julian Benavidez, Mr. Steve Bremser, Mr. Mark Bruce, Mr. Geoff Canty, Mr. Alex Friedman, Mr. Albert Hsueh, Ms. Tawnya Hughes, Ms. Marlene Jobe, Mr. Kevin Lee, Mr. Jim Liu, Mr. Jerome Macht, Mr. Eric McBurney, Mr. Mike Mendoza, Mr. Dan Messner, Ms. Meshia Moss, Mr. Scott Seeley, Mr. Mark Shoup, Ms. Angela Stangle, Mr. Eric Teti, Mr. Lance Thompson, Mr. Andrew Wallin, Mr. Ward Wilson, and all others at the San Bernardino County Office of the Public Defender; Mr. Zamir Ben-Dan, Mr. Mark Berger, Ms. Kristin Bruan, Ms. Virginia Cora, Ms. Shannon Griffin, Ms. Nesta Johnson, Ms. Karen Kalikow, Ms. Vanity Muniz, Ms. Dorothy McDonald, Mr. Eric Scott and all others at the Legal Aid Society; Mr. Kulmeet Galhotra, Ms. Julie Koehler, Ms. Kathy Lisco, Ms. Gina Piemonte, and all others at the Cook County Office of the Public Defender; Mr. June Chung, Ms. Jessica Watts, and all others at the Orange County Office of the Public Defender; Director Pascale Bishop, Professor Jay Koehler, Dean Susie Roth, Director Katie Shelton, Professor Maureen Stratton, Professor Deborah Tuerkheimer, Professor Jeffrey Urdangen, Professor Cliff Zimmerman, and all others at Northwestern University Pritzker School of Law; Ms. Tawny Do; Ms. Jane Rosales; Ms. Dominique Williams; Mr. Sam Yee; Ms. Hojung Choi, Mr. Sungjin Choi, Dr. Yonghwan Choi, Professor Heewon Shin; and all my friends and colleagues for their support and encouragement.

[1] *See* Karen Church & Rodrigo de Oliveira, *What's Up with WhatsApp? Comparing Mobile Instant Messaging Behaviors with Traditional SMS*, TELEFONICA RESEARCH (Aug. 30, 2013), https://pdfs.semanticscholar.org/3ea1/9dcbe7c8fcde728f546d96543ae9e2aa8d07.pdf (describing new platforms such as WhatsApp, WeChat, and Line that allow users to send text, voice picture, video). *See generally* WHATSAPP, https://www.whatsapp.com/ (last

decreasing cost and convenience of mobile data plans and public Wi-Fi accessibility, has driven the popularity and explosion of MIM apps in recent years.[2] Estimates state that in the year 2014, MIM apps carried more than twice the volume of messages carried by the traditional "text message" short messaging service ("SMS") – 50 billion messages per day versus 21 billion messages per day.[3] In April 2016, Mark Zuckerberg, whose company Facebook owns two of the market-leading MIM apps, WhatsApp and Facebook Messenger, announced that the messaging volume on just Facebook Messenger and WhatsApp combined was now three times larger than the entire global volume of all SMS messages – 60 billion messages per day compared to 20 billion messages per day.[4] Researchers predict that the popularity of MIM apps is likely to continue to grow in the future and ultimately lead to significant decreases in the traditional SMS "text messaging" traffic.[5] A marketing research firm predicted that by the year 2019, more than 2.19 billion people will use MIM apps worldwide.[6]

This comment will examine the evidentiary issues surrounding the admissibility of the MIM evidence in criminal trials, with emphasis on the authentication of the evidence. This comment will first discuss the characteristics of the modern MIM app, especially in comparison with other forms of more traditional electronic communication platforms, including the e-mail, the SMS text messaging, and the computer-based instant messaging ("IM") program. This comment will then examine the preliminary foundational requirements regarding the admissibility of the MIM evidence and the current

---

visited Dec. 24, 2017) (advertising WhatsApp as one of the major MIM platforms); Alex Heath, *An app you've probably never heard of is the most important social network in China*, BUS. INSIDER (Nov. 1, 2015, 3:28 PM), http://www.businessinsider.com/what-is-wechat-2015-10 (explaining how WeChat is one of the superior MIM apps because of its versatility); LINE, https://line.me/en/ (last visited Dec. 24, 2017) (showcasing the various functionalities Line offers).

[2] Church & Oliveria, *supra* note 1.

[3] *Short Messaging Services Versus Instant Messaging: Value Versus Volume*, DELOITTE, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/technology-media-telecommunications/deloitte-au-tmt-short-messaging-services-versus-instant-messaging-011014.pdf (last visited Dec. 24, 2017); Sophie Curtis, *Instant messaging overtakes texting in the UK*, TELEGRAPH (Jan. 13, 2014, 1:08 PM), http://www.telegraph.co.uk/technology/news/10568395/Instant-messaging-overtakes-texting-in-the-UK.html.

[4] *See* Lauren Goode, *Messenger and WhatsApp process 60 billion messages a day, three times more than SMS*, VERGE (Apr. 12, 2016, 1:25 PM), http://www.theverge.com/2016/4/12/11415198/facebook-messenger-whatsapp-number-messages-vs-sms-f8-2016 (describing how Facebook and WhatsApp are overtaking SMS).

[5] Church & Oliveria, *supra* note 1; *Mobile Messaging to Reach 1.4 Billion Worldwide in 2015*, EMARKETER (Nov. 11, 2015), https://www.emarketer.com/Article/Mobile-Messaging-Reach-14-Billion-Worldwide-2015/1013215.

[6] *Mobile Messaging to Reach 1.4 Billion Worldwide in 2015*, *supra* note 5.

case law on these requirements. Finally, this comment will summarize the status of law regarding the admissibility of the MIM evidence in criminal trials.

NATURE OF MOBILE INSTANT MESSAGING

The modern MIM app can be seen as a hybrid between the traditional SMS text messaging and the traditional computer-based IM program.[7] Like the SMS, the MIM app is largely used on mobile devices, and messages are exchanged through the wireless network infrastructure that one or more of the mobile networks operators owns and operates.[8] On the other hand, like the IM service—and unlike the SMS—the MIM app allows its user to retain a single identity across multiple client devices by utilizing a user log-in system.[9] Also similar to the IM program but unlike the SMS, the modern MIM app often employs a proprietary protocol, making it impossible for users of different MIM apps to exchange messages with one another.[10] However, the modern MIM app is also much more than a hybridized SMS-IM. Many modern MIM apps support

---

[7] Tom Morgan, *Google updates Hangouts app with combined SMS and IM conversations*, EXPERTREVIEWS (Apr. 22, 2014), http://www.expertreviews.co.uk/mobile-phones/28045/google-updates-hangouts-app-with-combined-sms-and-im-conversations.

[8] *See generally What is an SMS Center/SMSC?*, DEVELOPER'S HOME, http://www.developershome.com/sms/sms_tutorial.asp?page=smsc (last visited Dec. 24, 2017) ("The main duty of an SMSC is to route SMS messages and regulate the process. If the recipient is unavailable (for example, when the mobile phone is switched off), the SMSC will store the SMS message. It will forward the SMS message when the recipient is available.").

[9] *See generally* Umesh Gupta, *An Overview on the Architecture of WhatsApp*, 7 INT'L J. OF COMPUTER SCI. & ENG. TECH. 335, 336-37 (2016), http://www.ijcset.com/docs/IJCSET16-07-07-015.pdf (describing WhatsApp's handling of user login information through the use of Mnesia Database Management System). *See also* Raymond B. Jennings III, Erich M. Nahum, David P. Olshefski, Debanjan Saha, Zon-Yin Shae & Chris Waters, *A Study of Internet Instant Messaging and Chat Protocols*, IEEE NETWORK 16, 18-19 (2006), http://www.cs.columbia.edu/~nahum/papers/ieee-network-instant-messaging.pdf (describing ability to use the same login information unilaterally).

[10] *Compare* GWENAËL LE BODIC, MOBILE MESSAGING TECHNOLOGIES AND SERVICES: SMS, EMS AND MMS 29 (2d ed. 2005) ("SMS, EMS, and MMS are three mobile messaging services for which underlying technologies have been subject to significant standardization activities.") *with* Jennings, *supra* note 9, at 16 ("The protocols [for the traditional IM services] are not standardized, many of them are proprietary, and they are even seen as a control point in this business by the companies involved.") *and* Li Zhang, Chao Xu, Parth H. Pathak & Prasant Mohapatra, *Characterizing Instant Messaging Apps on Smartphones*, UC DAVIS 83, 83 (2015) http://spirit.cs.ucdavis.edu/pubs/conf/li-pam15.pdf ("Most of the current [mobile] IM apps either implement their own protocol or modify existing standard such as XMPP to customize them.").

various functionalities, including built-in voice chat,[11] video chat,[12] internet telephony (VoIP),[13] file transfer,[14] social networking,[15] online gaming,[16] mobile payment processing,[17] and digital advertising.[18] There are many in-app features

---

[11] *See, e.g.*, VOXER, http://www.voxer.com/ (last visited Dec. 24, 2017) (advertising Voxer's voice chat functionality as a "Walkie Talkie" similar to that on a smart device). *See generally* Miguel Helft, *Google's Free Phone Manager Could Threaten a Variety of Services*, N.Y. TIMES, Mar. 12, 2009, at B9 (specifying the competition google is facing with their new voice-in chat application).

[12] Josh Constine, *Facebook Messenger Launches Free VOIP Video Calls Over Cellular And Wi-Fi*, TECHCRUNCH (Apr. 27, 2015), https://techcrunch.com/2015/04/27/facebook-messenger-video-chat/. *See generally* Mark Gurman & Sarah Frier, *Facebook Is Working on a Video Chat Device*, BLOOMBERG (Aug. 1, 2017, 2:49 PM), https://www.bloomberg.com/news/articles/2017-08-01/facebook-is-said-to-work-on-video-chat-device-in-hardware-push (illustrating the innovative technological video chat device Facebook is working on).

[13] Britta O'Boyle, *5 apps that give you free voice calling*, POCKET-LINT (Apr. 1, 2015), http://www.pocket-lint.com/news/133404-5-apps-that-give-you-free-voice-calling. *See generally* Bryn Glover, *VoIP phones and providers*, STARTUPS (Oct 11, 2017), https://startups.co.uk/voip-phones-and-providers/ (listing the new upcoming technology regarding internet telephony).

[14] Sandy Stachowiak, *Viber now lets you attach files, delete messages and more*, APPADVICE (Nov. 24, 2015), http://appadvice.com/appnn/2015/11/viber-now-lets-you-attach-files-delete-messages-and-more. *See generally* Aimée McLaughlin, *WeTransfer launches new app to "make sharing simple"*, DESIGNWEEK (Oct. 12, 2017, 3:48 PM), https://www.designweek.co.uk/issues/9-15-october-2017/wetransfer-launches-new-app-to-make-sharing-simple/ (clarifying the big transition from file sharing through computers to now transferring files through mobile devices).

[15] Josh Constine, *Snapchat Makes Adding People Way Easier With Profile URLs*, TECHCRUNCH (Jan. 28, 2016), https://techcrunch.com/2016/01/28/snapchat-share-username/. *See generally China's Best Social Media and Internet Stocks*, FORBES (Oct. 17, 2017, 6:58 PM), https://www.forbes.com/sites/moneyshow/2017/10/17/chinas-best-social-media-and-internet-stocks/#32193070623c (highlighting China's dominance in combining social media functionality with global advertising).

[16] Kaylene Hong, *Chinese messaging app WeChat takes its games across the world in a bid to become a social platform*, NEXT WEB (Jan. 13, 2014), http://thenextweb.com/apps/2014/01/13/chinese-messaging-app-wechat-takes-its-games-across-the-world-in-a-bid-to-become-a-social-platform/. *See generally* Josh Constine, *Discord steals gamers from Skype with video chat and screensharing*, TECHCRUNCH (Aug. 10, 2017), https://techcrunch.com/2017/08/10/discord-video/ (emphasizing the competition between Skype and Discord on online gaming).

[17] *Instant Messaging as a new platform for mobile payments*, BBVA (Jan. 26, 2015), http://www.centrodeinnovacionbbva.com/en/news/instant-messaging-new-platform-mobile-payments. *See generally* Tom Krazit, *Why Stripe co-founder John Collison thinks his company is the Amazon Web Services of payments*, GEEKWIRE (Oct. 13, 2017, 2:00 PM), https://www.geekwire.com/2017/stripe-co-founder-john-collison-thinks-company-amazon-web-services-payments/ (inferring that mobile payment processing could take over the debit card swipe).

[18] *See* Rachel Gee, *How the BBC and Just Eat are using WhatsApp*, MARKETING WEEK (June 9, 2016, 10:48 AM), https://www.marketingweek.com/2016/06/09/how-vice-the-bbc-and-just-eat-are-using-whatsapp/ (describing how digital advertising is being used

such as booking doctor's appointments, paying utility bills, booking passport appointments, booking driver's license appointments, obtaining traffic camera feeds, booking transportation tickets, buying movie tickets, air quality monitoring, paying traffic fines, and police incident reporting.[19] Therefore, it is proper to say that "major [mobile instant] messaging apps are becoming something even greater [than mere messaging services]: they are becoming platforms, portals, and in some ways, even operating systems" due to these apps' heightened utility.[20]

The unique nature of the modern MIM app can be better understood by comparing it with other forms of popular electronic communications. In an e-mail communication, the parties who exchange e-mails know each other personally or the server administrators know their identities.[21] Server Administrators preserve parties' logs, IP addresses, and even copies of e-mails, sometimes indefinitely.[22] Therefore, the parties to the conversation may be able to identify e-mail evidence or be able to produce the logs and IP addresses of the parties from the server.[23] In a phone conversation, identifying the voices of a conversation typically authenticates the evidence.[24] There is also a presumption that the party who picks up the phone is the one who is listed on the phone directory as the owner of the phone line connected to the phone number.[25] For SMS text messages, the wireless carriers keep the logs of when certain messages were exchanged between certain phone numbers.[26] Depending on the wireless carrier, the metadata attached to each exchanged message may also include the

---

by companies on WhatsApp). *See generally* Mike Shields, *Google Wants to Own the Future of TV Ad Infrastructure*, BUS. INSIDER (Oct. 16, 2017, 10:59 PM), http://www.businessinsider.com/google-is-looking-to-wedge-into-tv-advertising-by-displacing-comcast-2017-10 (explaining the competition Google faces in digital advertising and innovative strategies are being implemented).

[19] Tudor Stanciu, *Why WeChat City Services Is A Game-Changing Move For Smartphone Adoption*, TECHCRUNCH (Apr. 24, 2015), https://techcrunch.com/2015/04/24/why-wechat-city-services-is-a-game-changing-move-for-smartphone-adoption/.

[20] Elad Natanson, *Messaging Platforms, Bots and the Future of Mobile*, FORBES (Apr. 8, 2016, 12:24 PM), https://www.forbes.com/sites/eladnatanson/2016/04/08/messaging-platforms-bots-and-the-future-of-mobile/#4353e8151039.

[21] *How Does Email Work? A Simple (Illustrated) Explanation*, VISION DESIGN GROUP, https://www.visiondesign.com/how-does-email-work-a-simple-illustrated-explanation/ (last visited Dec. 24, 2017).

[22] Marshall Brain & Tim Crosby, *How E-Mail Works*, HOW STUFF WORKS, https://computer.howstuffworks.com/e-mail-messaging/email.htm (last visited Dec. 24, 2017).

[23] Ryan Malkin, *Introducing Email Evidence at Trial*, 14 CRIM. LITIG. 6, 6 (2013).

[24] *Evidence - Admissibility of Phone Conversations - Identification of Calling Party*, 26 WASH. U.L. REV. 433, 433 (1941).

[25] *Id.*

[26] Chloe Albanesius, *How Long Does Your Wireless Carrier Retain Texts, Call Logs?*, PC MAG. (Sept. 30, 2011, 10:01 AM), https://www.pcmag.com/article2/0,2817,2393887,00.asp.

location of the cell tower used to send the message.[27] Like the regular phone conversation, there is a presumption that the listed owner of the mobile phone from which the text message was sent is the one who actually sent the message from the phone.[28] In computer-based IM programs, parties identify themselves using "handles".[29] It would be difficult to prove the identity of the "handle" – except based on circumstantial evidence – because there is no physical billing address attached to them.[30] However, most IM service providers keep a log of user logins, including user IP addresses from which the client was logged in, which may be used to track down the user.[31] Some IM service providers also keep the log of the actual message contents as well, which could be easily produced upon request.[32]

For MIM apps, parties identify themselves by their user names.[33] The sign-up process often requires either or both a valid e-mail address and a working cell phone number.[34] However, there are many web services that offer disposable e-mail and SMS-only numbers for verification purposes.[35] Although some MIM service providers may keep certain log-in information, millions of phones share mobile IP addresses which change constantly depending on the cell tower used.[36] Therefore, a foreign traveler visiting a popular tourist destination for vacation

---

[27] *Id.*

[28] Commonwealth v. Purdy, 945 N.E.2d 372, 381(Mass. 2011).

[29] *See generally Handle*, TECHTERMS (Apr. 17, 2008), https://techterms.com/definition/handle ("In the online world, a handle is another word for a username."); *Why Usernames Are Important and How to Choose Good Ones*, LEAPFROG (June 4, 2017), https://leapfrogservices.com/why-usernames-are-important-and-how-to-choose-good-ones/.

[30] Beth S. Rose, *Authentication Of Social Media Evidence: 2 Cases To Know*, LAW360 (Mar. 3, 2018, 1:19 PM), https://www.law360.com/articles/897947/authentication-of-social-media-evidence-2-cases-to-know.

[31] In a survey conducted in 2008, all eight major IM service operators except for Microsoft (Windows Live Messenger) responded that they keep logs of user logins. Declan McCullagh, *How safe is instant messaging? A security and privacy survey*, CNET (June 9, 2008, 11:37 AM), https://www.cnet.com/news/how-safe-is-instant-messaging-a-security-and-privacy-survey/.

[32] *See id.* (stating that Facebook, Google, and Yahoo indicated that the actual contents of the messages may be saved in one way or another).

[33] Sergio Caro-Alvaro, Eva Garcia-Lopez, Antonio Garcia-Cabot, Luis de-Marcos & Jose-Maria Gutierrez-Martinez, *A Systematic Evaluation of Mobile Applications for Instant Messaging on iOS Devices*, 2017 UNIV. OF ALCALA 1, 6 (2017).

[34] *Id.*

[35] Gabe Carey & Tyler Lacoma, *Reluctant to Give Your Email Address Away? Create A Disposable with One of These Services*, DIGITAL TRENDS (Apr. 28, 2017, 10:03 AM), https://www.digitaltrends.com/computing/best-sites-for-creating-a-disposable-email-address/.

[36] Lincoln Spector, *Your mobile IP address: Its safety is one thing, its privacy is another*, PCWORLD (Aug. 21, 2015, 7:35 AM), https://www.pcworld.com/article/2955112/phones/your-mobile-ip-address-its-safety-is-one-thing-its-privacy-is-another.html.

could theoretically be using the same mobile IP address that a child pornographer was using just seconds ago.[37] However, if a user logs in from a particular IP address repeatedly, that may be an indication that the IP address in question is associated with that user.[38] This is most likely to happen if the user frequently uses MIM app through Wi-Fi hotspots at home or at work.[39] Most MIM service providers do not log the actual contents of messages themselves.[40] Many MIM apps also employ advanced encryption protocols, which make it impossible even for the service providers themselves to verify the actual contents of the messages in question.[41] On the other hand, many modern MIM apps feature some sort of semi-permanent social-networking profile feature.[42] This is particularly true for such MIM services as Twitter Direct Message or Facebook Messenger, which originally started out as the private messaging components for pre-existing traditional computer-based social networking services, and are now provided as integral parts of the comprehensive social media platforms operated by their parent companies.[43] Such social-networking features of the modern MIM app may actually make it easier to identify the real-life person behind a particular user id than it would be for us to identify the real-life person behind a particular handle in a traditional computer-based IM service.[44] With the exceptions of WhatsApp and Facebook Messenger, both of which are owned by Facebook, eight of the top ten popular MIM apps are owned

---

[37] *Id.*

[38] Chris Allard, *Could Somebody Track My Location Using My Cell Phone's IP Address?*, NORTHAMPTON COMPUTER REPAIR (Oct. 24, 2013), http://www.northamptoncomputerrepair.com/ask-a-techie/bid/321978/could-somebody-track-my-location-using-my-cell-phone-s-ip-address.

[39] *Id.*

[40] McCullagh, *supra* note 31.

[41] *Id.*

[42] Josh Constine, *Why Snapchat's Only Non-Ephemeral Content, The Profile GIF, Is A Big Deal*, TECHCRUNCH (Sept. 29, 2015), https://techcrunch.com/2015/09/29/profile-gif/; Danielle Corcione, *Snapchat for Business: Everything You Need to Know*, BUS. NEWS DAILY (Apr. 5, 2017, 1:52 PM), http://www.businessnewsdaily.com/9860-snapchat-for-business.html; Aatif Sulleyman, *Facebook Trials New Feature Linking Accounts to Instagram, LinkedIn and Snapchat Profiles*, INDEPENDENT (Feb. 20, 2017, 11:08 AM), http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-latest-news-feature-user-profiles-social-media-linkedin-snapchat-youtube-twitter-pinterest-a7589376.html.

[43] *About Direct Messages*, TWITTER, https://support.twitter.com/articles/14606 (last visited Dec. 24, 2017); Louis Boval, *Sign Up for Messenger, Without a Facebook Account*, FACEBOOK NEWSROOM (June 24, 2015), https://newsroom.fb.com/news/2015/06/sign-up-for-messenger-without-a-facebook-account/.

[44] *See, e.g.*, Sublet v. State, 113 A.3d 695, 720 (Md. 2015) (holding that the twitter direct message evidence was properly authenticated by utilizing the social networking features connected with the user id used to send and receive the direct message evidence in question, such as the profile picture for the user id and the public tweets sent out under the user's identification). *But see* Griffin v. State, 19 A.3d 415, 423-24 (Md. 2011) (holding that a social media page which identifies the birthdate, location, and picture of an individual is not enough to allow for authentication of an individual's threatening messages).

by foreign companies with servers in foreign jurisdictions.[45] This would make it difficult for U.S. courts or government agencies to compel the production of any information that these companies may possess connected to a particular user id.[46]

MOBILE INSTANT MESSAGING EVIDENCE IN CRIMINAL TRIALS

To admit MIM evidence in a criminal trial, five preliminary foundational requirements must be met.[47] First, the evidence must be relevant.[48] Second, if relevant, the evidence must be authentic.[49] Third, if the evidence is offered for its substantive truth, it must either not be hearsay, or be covered by an applicable hearsay exception.[50] Fourth, the evidence must be either an original or a duplicate under the best evidence rule, or if not, must be an admissible secondary evidence to prove its content.[51] Fifth, its probative value must not be substantially outweighed by the danger of UNFAIR PREJUDICE or other concerns of fairness.[52]

A. Relevance

MIM evidence must be relevant to be admissible at a criminal trial.[53] Evidence is relevant if (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action.[54]

---

[45] *See Most Popular Mobile Messaging Apps Worldwide as of January 2017, Based on Number of Monthly Active Users (in Millions)*, STATISTA, https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (last visited Dec. 24, 2017). Skype is developed and operated by Skype Communications SARL, a wholly owned subsidiary of Microsoft Corporation. Even though Microsoft is an American company, Skype Communications was incorporated and is registered and headquartered in Luxembourg. *See About Skype*, SKYPE, https://www.skype.com/en/about/ (last visited Dec. 24, 2017).

[46] *See In re* Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 222 (2d Cir. 2016) (holding that the Federal Store Communications Act's warrant provision is not meant to apply extraterritorially and therefore cannot be used to compel Microsoft, an American company, to produce to the government the contents of a customer's e-mail account stored exclusively in Ireland).

[47] *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007) (providing a general framework for working out the evidentiary issues surrounding the admissibility of electronically stored information).

[48] *Id.*; Fed. R. Evid. 401.

[49] *Lorraine*, 241 F.R.D. at 538; Fed. R. Evid. 901.

[50] *Lorraine*, 241 F.R.D. at 538; Fed. R. Evid. 801-807.

[51] *Lorraine*, 241 F.R.D. at 538; Fed. R. Evid. 1001-1008.

[52] *Lorraine*, 241 F.R.D. at 538; Fed. R. Evid. 403.

[53] *Lorraine*, 241 F.R.D. at 540; Fed. R. Evid. 401-402.

[54] Fed. R. Evid. 401.

MIM evidence that is far too attenuated from the fact in question to have any probative value may not be admissible as irrelevant.[55] For example, in a criminal possession of a weapon case, a New York appellate court held that the trial court erred by allowing the prosecution to introduce two Facebook messages the defendant sent three months after the crime.[56] In those messages, the defendant bragged about possessing and discharging firearms that were of larger caliber than those his adversaries used.[57] In that case, the prosecution conceded the defendant was not referring to the charged crime in those messages, but rather, to an entirely different incident that occurred months later.[58] The Court ruled the Facebook messages were far too attenuated to have any probative value as to the defendant's knowledge of the gun found in the car or his intent to use that weapon on the day of the incident.[59]

MIM evidence that is not connected to any genuine issue at trial may be inadmissible as irrelevant.[60] For example, in a manslaughter case arising from a drug deal gone awry, the defendant-drug-dealer was charged with killing one of his customers with a shotgun during a struggle that ensued when two customers exited their car and attacked him in the middle of a drug deal.[61] The defendant contended that the trial court erred by excluding from evidence the Facebook messages exchanged between one of his attackers and a female witness who was also present at the scene of incident.[62] There was evidence presented at trial that the female witness and the defendant were romantically involved in the past, and the female witness was upset because the defendant would not have sexual intercourse with her anymore and declared that the defendant was "going to get robbed."[63] According to the defendant, the excluded Facebook conversation was material to his defense because it supported his theory that the attacker and the female witness had a motive to attack him and they conspired together to attack him on the day of the incident.[64] The South Dakota Supreme Court ruled that the trial court properly precluded the Facebook messaging evidence as irrelevant.[65] The Court observed, "the content of the Facebook messages was not contradicted at trial."[66] The Court stated:

> [t]he Facebook messages merely bolstered the otherwise truthful testimony of [the attacker], and therefore served no purpose of impeachment. Furthermore, the primary issue at trial was whether the defendant was justified in using deadly force

---

55 People v. Singleton, 139 A.D.3d 208, 214-15 (N.Y. App. Div. 2016).
56 *Id.* at 214.
57 *Id.*
58 *Id.* at 214-15.
59 *Id.* at 215.
60 State v. Birdshead, 871 N.W.2d 62, 64, 76 (S.D. 2015).
61 *Id.* at 67-68.
62 *Id.* at 75.
63 *Id.*
64 *Id.*
65 *Id.* at 76.
66 *Id.*

> to defend himself against [the attackers.] The Facebook messages did not shed light on whether [the defendant]'s use of deadly force was reasonable as it had nothing to do with his intent or state of mind.[67]

These cases show that MIM evidence must be connected to a genuine issue at trial to be considered relevant and thus admissible.

B. Authentication

Relevant MIM evidence must be authenticated or identified before the trial court may admit it into evidence.[68] To satisfy the requirement of authenticating or identifying an item of evidence, the proponent of the MIM evidence must produce evidence sufficient to support a finding that the item is what the proponent claims it is.[69]

User identification is the key to authenticating MIM evidence.[70] There are varying practices MIM service providers use to keep track of its users' identities.[71] Most MIM apps require a valid e-mail address for its users to sign up for its service.[72] Many also require giving a valid phone number and signing up for its service.[73] However, using disposable e-mail addresses or phone numbers makes it possible to circumvent these restrictions.[74]

In the mobile context, IP addresses are not as meaningful as its traditional counterparts. They are fluid and constantly changing.[75] The same IP address is shared between many different devices.[76] Therefore, using IP addresses to track

---

[67] *Id.*

[68] *See* Jonathan Sablone & Steven M. Richard, *Instant Messages as Evidence: Questions of Authenticity and Admissibility Addressed in Massachusetts Appeals Court Ruling*, NIXON PEABODY (Oct. 3, 2014), https://www.nixonpeabody.com/en/ideas/articles/2014/10/03/instant-messages-as-evidence-questions-of-authenticity-and-admissibility-addressed-in-m ("[A]ll forms of evidence, electronic communications – such as IM or text messages – must be properly authenticated in order to be admitted.").

[69] Fed. R. Evid. 901(a).

[70] *See generally* Alan Pendleton, *Admissibility of Electronic Evidence: A New Evidentiary Frontier*, BENCH & BAR (Oct. 14, 2013), http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/ (discussing how authorship or identity of the poster is one of the challenges to authenticating e-evidence).

[71] *How to Instant Message*, WIKIHOW, https://www.wikihow.com/Instant-Message (last visited Dec. 24, 2017) (explaining how to sign up for different instant messaging apps and what they require to create an account).

[72] *Id.*

[73] *Id.*

[74] *See generally* Andy Greenberg, *How to Anonymize Everything You Do Online*, WIRED (June 17, 2014, 6:30 AM), https://www.wired.com/2014/06/be-anonymous-online/ (discussing ways to anonymize yourself by using disposable emails and other software).

[75] Spector, *supra* note 36.

[76] *See* Chris Hoffman, *How and Why All Devices in Your Home Share One IP Address*, HOW-TO GEEK (Apr. 15, 2013), https://www.howtogeek.com/148664/how-and-

down the identity of the user may not be a viable option in establishing the identity of a user.[77] Because the applications are usually always turned on at all times while the mobile device is turned on, a phone that was originally logged on from one location can be used to receive messages at a location and time far removed from the time and location of the original log in.[78] This may make it harder to pin down the user identity based solely on the log-in information.[79]

However, a pattern of repeated log-ins from particular IP addresses for a username signals to a court that those particular IP addresses are connected to the username.[80] This is most likely to happen when the mobile devices used to access the MIM apps are connected to the internet through a Wi-Fi hotspot at home or at work.[81] For example, in a child pornography case, the Federal Bureau of Investigation served administrative subpoenas on KIK Interactive Inc. ("KIK"), the owner and operator of the MIM app KIK, seeking account information for the username "lookingforyounggirls."[82] KIK advised the FBI "that the user of 'lookingforyounggirls' was associated with the user of 'Suppix.Records@gmail.com,' and provided three login IP addresses associated with the account."[83] Based on this advice, "administrative subpoenas were issued to the internet service providers for these IP addresses; two resolved back to residences associated with [the defendant], . . . and the third to his employer's business address."[84] Administrative subpoenas were used to obtain the

---

why-all-devices-in-your-home-share-one-ip-address/ (explaining how Public and Private IP addresses work and how one router is assigned one public address and is shared among devices).

[77] *See generally* Kashmir Hill, *How to Bait and Catch the Anonymous Person Harassing You on the Internet*, FORBES (Sept. 28, 2012, 12:08 PM), https://www.forbes.com/sites/kashmirhill/2012/09/28/how-to-bait-and-catch-the-anonymous-person-harassing-you-on-the-internet/#e0af42a7e1a0 (showing how to use an IP address to find a user, should the user be on a static IP address).

[78] *See generally The Problem with Mobile Phones*, SURVEILLANCE SELF-DEF., https://ssd.eff.org/en/module/problem-mobile-phones (last visited Dec. 24, 2017) (discussing in depth how mobile monitoring works and how to protect yourself from unwanted tracking).

[79] *Id.*

[80] *See generally* Jessica Rich, *Keeping up with the Online Advertising Industry*, FED. TRADE COMM'N (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry (arguing that IP Addresses and other persistent identifiers are personally identifiable).

[81] *See generally* Amadou Diallo, *Want Privacy on the Internet? Then You Need a VPN*, FORBES (Mar. 7 2014, 11:15 AM), https://www.forbes.com/sites/amadoudiallo/2014/03/07/want-privacy-on-the-internet-then-you-need-a-vpn/#42d925502d57.

[82] United States v. Pinchot, No. CR 16-20006, 2016 WL 2956265, at *1 (E.D. Mich. Apr. 28, 2016).

[83] *Id.* at *2.

[84] *Id.*

information the government used during the investigation and they were also presented at trial as evidence.[85]

In this case, KIK, a Canadian company,[86] voluntarily provided the requested user information to an administrative subpoena the United States government issued.[87] However, this is highly unlikely to happen with many other popular non-U.S. based MIM services. For example, China's Tencent owns and operates QQ Mobile and WeChat, the third and the fourth most popular MIM apps in the world, respectively.[88] Luxemburg's Skype Communications operates Skype, the fifth most popular MIM app in the world.[89] Although Skype Communications is a wholly owned subsidiary of the Microsoft Corporation of the U.S.,[90] Microsoft has shown its willingness to fight the U.S. government's attempt to obtain its user data saved and maintained in a data center foreign subsidiaries own and operate, especially in criminal cases, and have recently obtained a positive result in doing so.[91] Telegram, the ninth most popular MIM app in the world, heavily markets its security and encryption as its selling point and is registered as a network of shell companies around the world, which disguises the application's true ownership and is said to be "intended to deter subpoenas and other requests from government."[92] It would be highly unrealistic to expect a Chinese company, such as Tencent, or a multinational shell company that was designed so for the purpose of deterring governmental requests, such as Telegram, to voluntarily hand over user information upon a request made by a U.S. court or government agency.

In most traditional computer-based IM programs, one must manually choose to save each chat history and log before ending each session to preserve the

---

[85] *Id.*

[86] *See Reach Out to Us*, KIK, https://www.kik.com/contact/ (last visited Dec. 24, 2017); *see also Learn Our Company Story*, KIK, https://www.kik.com/about/ (last visited Dec. 24, 2017).

[87] *Pinchot*, 2016 WL 2956265, at *2.

[88] *See Most Popular Mobile Messaging Apps Worldwide as of January 2017, Based on Number of Monthly Active Users (in Millions)*, *supra* note 45. *See also Social Networks*, TENCENT, https://www.tencent.com/en-us/system.html (last visited Dec. 24, 2017).

[89] *About Skype*, *supra* note 45.

[90] *About Skype*, *supra* note 45.

[91] *In re* Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 222 (2d Cir. 2016) (holding that the Federal Store Communications Act's warrant provision is not meant to apply extraterritorially and therefore cannot be used to compel Microsoft, an American company, to produce to the government the contents of a customer's e-mail account stored exclusively in Ireland).

[92] Caitlin Dewey, *The Secret American Origins of Telegram, the Encrypted Messaging App Favored by the Islamic State*, WASH. POST (Nov. 23, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/11/23/the-secret-american-origins-of-telegram-the-encrypted-messaging-app-favored-by-the-islamic-state/. *See also Telegram FAQ*, TELEGRAM, https://telegram.org/faq (last visited Dec. 24, 2017).

contents of the chat for later access.[93] In contrast, in most modern MIM apps, chat history is usually automatically saved on the device semi-permanently, which one can load and access at any later time.[94] This may make it easier to authenticate user identity based on past chat history.[95]

Courts have generally held that to authenticate MIM evidence, the trial judge must determine that there is proof that a reasonable juror could find that the evidence is what the proponent claims it to be.[96] Circumstantial evidence, including the testimony of a witness, has generally been held to be adequate to identify MIM evidence for courts.[97] In a recent case, the Kentucky Court of Appeals held that trial testimony by either one of the parties involved in the conversation—even when the other party of the conversation denies its authenticity—is enough to identify Facebook Messenger and Viber evidence for preliminary authentication purposes.[98] In doing so, the Court noted,

> while [the defendant] attempts to impart a mystical, magical quality to electronic messages, we disagree . . . they are not so different from photos . . . A trial court may admit a piece of evidence solely on the basis of testimony from a knowledgeable person that the item is what it purports to be and its condition has been substantially unchanged.[99]

In another case, a New York court ruled that the testimony of a witness who is not a direct participant in the conversation could authenticate Facebook Messenger evidence.[100] In that case, the Court ruled that all of the circumstantial

---

[93] *See* People v. Pierre, 838 N.Y.S.2d 546, 548 (N.Y. App. Div. 2007) ("The court properly received, as an admission, an Internet instant message in which defendant told the victim's cousin that he did not want the victim's baby. Although the witness did not save or print the message, and there was no Internet service provider evidence or other technical evidence in this regard, the instant message was properly authenticated, through circumstantial evidence, as emanating from defendant.").

[94] Mike Musgrove, *Instant Messaging, Lingering Paper Trail*, WASH. POST (Oct. 6, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/10/05/AR2006100501594.html.

[95] *Id.*

[96] *See, e.g.*, Sublet v. State, 113 A.3d 695, 722 (Md. 2015) (applying the reasonable juror standard to twitter private messages and Facebook messages); State v. Smith, 192 So.3d 836, 842 (La. Ct. App. 2016) (applying the reasonable juror standard to Instagram "text messages").

[97] *See, e.g.*, Campbell v. State, 382 S.W.3d 545, 551 (Tex. App. 2012) (holding that Facebook messages were properly authenticated because the messages contained internal characteristics that tended to connect the defendant as the author).

[98] Kays v. Commonwealth, 505 S.W.3d 260, 269 (Ky. Ct. App. 2016).

[99] *Id.*

[100] People v. Moye, No. 2138/2014, 2016 WL 1708504, at *8 (N.Y. Sup. Ct. Mar. 31, 2016) (holding that where a witness is deemed to be physically unavailable testify, as they were an underage victim of domestic abuse and refuse to testify following their former partner's breach of restraining order, the court may introduce statements made to an attorney, family member and/or 911 operator). *See also* Jeffrey Bellin, *The Case for eHearsay*, 83 FORDHAM L. REV. 1317, 1319 (2014) (proposing that text messages which can be considered a recorded communication, are from a known sender, and go to prove the truth of the matter asserted should be admissible under the Federal Rules of Evidence Rule

evidence together, including the mother's testimony that her daughter, the complaining witness, logged into her own Facebook account using her mother's phone and showed her mother the message from the account registered as "Preme Low" were sufficient to establish a reasonable likelihood that the writing came from the defendant. This was sufficient authentication of the Facebook message evidence introduced at trial.[101] The Court observed that no particular type of evidence is required for the authentication of these Facebook messages, only that the circumstantial evidence is sufficient to support a finding that there is a reasonable likelihood the matter in question is what its proponent claims it is.[102] The Court also noted it is not necessary to know exactly who typed the message, by eyewitnesses or other evidence, for the purpose of admission.[103] According to the court, the exact authorship of the Facebook messages in question was an evidentiary issue the fact finder should have weighed and decided, similar to the issue of forgery of traditional written documents that someone is able to forge or type on someone else's computer or typewriter.[104] The Court also rejected the contention "that the complainant [was] the only witness qualified to testify about her own Facebook account."[105] These cases show that circumstantial evidence, including the testimony of a witness who is neither the author nor the recipient of the proffered MIM evidence, may authenticate or identify MIM evidence for the court in a criminal trial.

The Maryland Court of Appeals went a step even further, and held that a witness who was not only a non-party to the conversation, but also had never seen the actual contents of the conversation beforehand, could still authenticate

804(b)(5) "Recorded Statement of Recent Perception" when the party is unavailable to testify as they have been murdered and the other party is a suspect in the alleged crime).

[101] *Moye*, 2016 WL 1708504, at *2. *But see* State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct. 2011) (holding that where a defendant was charged with assault with a deadly weapon and introduces Facebook messages in their defense, authentication requires more than just knowing that an individual was the owner of an account as there is no proof that they were the only individual who had accessed it).

[102] *Moye*, 2016 WL 1708504, at *7. *See also* Paul W. Grimm, Lisa Yurwit Bergstrom, & Melissa M. O'Toole-Loureiro, *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 459 (2013) (arguing that a court should find that when a proponent shows plausible evidence of authentication the threshold has been met).

[103] *Moye*, 2016 WL 1708504, at *7.

[104] *Moye*, 2016 WL 1708504, at *8. *See also* Tienda v. State, 358 S.W.3d 633, 641-42 (Tex. Crim. App. 2012) (noting that social media messages and other electronic communications require more authentication than just looking at the alleged source as hacking can occur or an individual may identify themselves as someone else).

[105] *Moye*, 2016 WL 1708504, at *7. *See generally* People v. Pierre, 838 N.Y.S.2d 546, 548 (N.Y. App. Div. 2007) (holding that in the interest of justice, if there is enough circumstantial evidence to support finding that a message does not need authentication by the original party, it may still be admitted through the authentication of others).

MIM evidence for the court.[106] In that case, the prosecution sought to authenticate the Twitter direct messages the defendant exchanged with his friend, Foulke, which, if admitted, would have implicated the defendant in the crimes charged.[107] The prosecution sought to authenticate the messages through the testimony of a mutual friend of both the defendant and Foulke, who testified at trial that the two Twitter accounts used to exchange messages belonged to the defendant and Foulke, respectively.[108] The Court ruled the direct messages were properly authenticated and admitted.[109] The Court agreed with the prosecution that not only did the prosecution's witness identify the Twitter account as belonging to the defendant, but also the photographs accompanying the Twitter account were those of the defendant.[110] The Court also noted the timeline of the direct messages suggested "someone with knowledge of and involvement in the situation" wrote the messages that gave rise to the crimes in which the defendant was charged, "which involved only a small pool of individuals," one of whom was the defendant.[111] Considering these facts, the Court ruled that there was enough evidence to allow the trial judge to determine that "a reasonable juror would have found that the 'direct messages' were authentic."[112] This case shows that the "reasonable juror" requirement for the authentication of MIM evidence is a rather easy standard to satisfy.

This does not mean, however, that any MIM evidence is automatically admissible. The Third Circuit has held that MIM evidence is not in and of itself

---

[106] Sublet v. State, 113 A.3d 695, 721 (Md. 2015) (finding that where a message is authenticated, concurrent direct messages were also considered admissible, as they were deemed authenticated by the original messages).

[107] *Id.* at 705.

[108] *Id. See also* Dan Grice & Bryan Schwartz, *Social Incrimination: How North American Courts Are Embracing Social Network Evidence in Criminal and Civil Trials*, 36 MAN. L.J. 221, 236-37 (2012) (discussing how a brother's identification of a suspect's account was one factor which allowed for authentication of messages in addition to forensic software results and personal details which were noted and would have only been known to the parties involved in the case).

[109] *Sublet*, 113 A.3d at 720-21.

[110] *Id.* at 720 (noting, in the subcase Harris v. State, that because of the timing of the messages and the link between a participant and a twitter handle, a tweet could be authenticated by someone with knowledge of the issue, which in this instance was a government agent). *But see* Griffin v. State, 19 A.3d 415, 423-24 (Md. 2011) (holding that a social media page which identifies the birthdate, location, and picture of an individual is not enough to allow for authentication of an individual's threatening messages).

[111] *Sublet*, 113 A.3d at 720. *See also* Kristen L. Mix, *Discovery of Social Media*, 5 FED. CTS. L. REV. 119, 134 (2011) (noting that a social media page which has not been authenticated by a person with first-hand knowledge of its authorship may not be admissible as evidence as it may instead be considered hearsay).

[112] *Sublet*, 113 A.3d at 720. *See generally* Grimm et al., *supra* note 102, at 456 (stating that if there is enough evidence to allow a juror to believe that there may be enough for authentication, a reasonable juror should be able to find in favor of either party).

self-authenticating.[113] In that case, the prosecution argued that a set of Facebook chat log the Facebook Company produced in response to a search warrant, which was executed by its records custodian and was accompanied with a certificate of authenticity that tracked the language of Rule 803(6) of Federal Rules of Evidence, was properly self-authenticating pursuant to Rule 902(11) of the Federal Rules of Evidence as records of regularly conducted business activity.[114] The Court rejected the prosecution's argument.[115] The Court noted that although the "relevance of the Facebook records hinged on the fact of authorship", here, the record custodian could not attest to whether the defendant and the victims actually authored the Facebook messages at issue, but could only confirm that "the communications took place as alleged between the named Facebook accounts."[116] According to the Court, "[t]his [wa]s no more sufficient to confirm the accuracy or reliability of the contents of the Facebook chats than a postal receipt would be to attest to the accuracy or reliability of the contents of the enclosed mailed letter."[117] This case shows that even when coming directly from the service provider itself, MIM evidence is not automatically self-authenticating by the virtue of its mere existence, and it must be independently authenticated or identified through the testimony of a knowledgeable witness or other accepted means before it can be properly admitted.

Courts may also refuse to admit MIM evidence, despite a supporting testimony by a knowledgeable witness, because the proponent of the evidence failed its burden to satisfy the "reasonable juror" standard.[118] In *State v. Smith*,

---

[113] United States v. Browne, 834 F.3d 403, 409 (3d Cir. 2016) (arguing that just because a message may be deemed to be authentic, it may not be deemed admissible if it is not relevant). *See generally* United States v. Reilly, 33 F.3d 1396, 1404 (3d Cir. 1994) (stating that where not all documents are considered authenticated, it may be because not all are relevant, and relevance is a condition that must be met before a document can be authenticated under the Federal Rules of Evidence).

[114] *Browne*, 834 F.3d at 408-09.

[115] *Id.* at 410 (finding that the government's argument could not be accepted as to do so would imply that social media would not have to be deemed relevant to be admissible and the government inaccurately interpreted the business record rule as the communications were not made in the regular course of business).

[116] *Id. See also* People v. Kent, 81 N.E.3d 578, 591-92 (2017) (noting that when a social media profile or posting is being admitted into evidence, it must be shown to be relevant under the Federal Rules of Evidence before it can be authenticated).

[117] *Browne*, 834 F.3d at 411. *See also* Campbell v. State, 382 S.W.3d 545, 550 (Tex. App. 2012) (finding that Facebook accounts are difficult to self-authenticate for two reasons: first, because the profile could be created by another user and there is no way of knowing if it is legitimate and second, another person could potentially access the user's Facebook page without their authorization and post content which may not be authorized by the profile owner).

[118] *See e.g.*, State v. Smith, 192 So.3d 836, 840-41 (La. Ct. App. 2016). *See also* Brendan W. Hogan, *Griffin v. State: Setting the Bar too High for Authenticating Social Media Evidence*, 71 MD. L. REV. 61, 80 (noting that the dissent in Griffin v. State found that under the "reasonable juror" standard evidence of a social media posting should have been

the Louisiana Court of Appeal held the Instagram "text messages"[119] the State sought to introduce were not properly authenticated because the State did not offer "sufficient facts from which the jury could reasonably find the evidence authentic."[120] The State's witness:

> was unable to identify from which social media platform the messages were allegedly sent. Further, no evidence or testimony was offered as to whether [the defendant] created the account and/or profile on the social media platform or whether he had ever accessed the platform. Likewise, there [was] no evidence of whether, assuming he created the online account, [the defendant] allowed others access using his password or any unique qualities regarding the messages themselves from which one may assert [that it was the defendant who] sent the messages.[121]

These cases indicate that although the bar for the authentication of MIM evidence is pretty low, trial courts still want to see at least some extrinsic and independent evidence of authenticity for the proffered evidence that would satisfy the "reasonable juror" standard.[122]

C. Hearsay Issues

---

admitted because name, birthdate, and picture was enough to allow a reasonable juror to conclude that the Myspace page belonged to Barber); George Parker Young, Layne Keele & Josh Borsellino, *"A Rough Sense of Justice" or "Practical Politics"? Recent Texas Supreme Court Opinions and Causation*, 46 ADVOC. (TEX.) 30, 34 (2009) (explaining that the "reasonable juror" standard is one where evidence may be admitted (pending other considerations) where a reasonable juror could believe it to be true, but also noting that the problem with this standard is that reasonable jurors may believe different things); 6A MD. EVIDENCE, STATE & FED. § 901:5 (2017) (explaining that under the "reasonable juror" standard a social media page may be authenticated by circumstantial evidence but also noting that following Sublet v. State, the threshold was raised to a high standard which allowed the trial judge to establish the bar for authentication).

[119] *See Smith*, 192 So.3d at 837-38 n.1 (referring to the instant messaging conversation in question, and noting that "[a]lthough [the police officer] referred to [the defendant's] alleged communication with the victim as 'text messages,' … [evidence] reveals that the virtual correspondence occurred over an unidentified social media platform, rather than mobile text messaging."); *id.* at 838 (deducing that the "text messages" in question were private Instagram messages exchanged between the defendant and the complaining witness and noting that the Officer could not speak to the origin of the "text messages" and photos or "from what social media service the messages were allegedly sent.").

[120] *Id.* at 842.

[121] *Id.*

[122] *See* Grimm et al., *supra* note 102, at 456 (recognizing that all a proponent is required to do "to authenticate social media evidence [is] introduce sufficient facts - generally by any of the methods identified by Rule 901(b) . . . to persuade a reasonable juror that the evidence was created by the person who the proponent alleged created the evidence."). *See also* John G. Browning, *Introducing Social Media Evidence*, 74 ADVOC. (TEX.) 110, 114 (2016) ("Like relevance, authentication has a very low threshold. Simply put, under Rule 901, the proponent must come forward with evidence 'sufficient to support a finding that the item is what the proponent claims it is.'").

Relevant and authentic MIM evidence nonetheless will not be admitted into evidence if it is a hearsay statement—unless it falls under one or more of the hearsay exceptions.[123] A hearsay statement is a statement that "a party offers in evidence to prove the truth of the matter asserted in the statement," and one the declarant did not make while testifying at the instant trial or hearing.[124] A declarant-witness's prior statement or an opposing party's statement is considered a non-hearsay statement.[125]

One of the most commonly litigated hearsay issues in the context of MIM evidence is whether the proffered MIM evidence constitutes the statement of a party opponent.[126] This hearsay issue is deeply intertwined with the issue of authenticating MIM evidence.[127] Let us imagine a situation where a party offers MIM evidence, claiming it to be a message written and sent by the party-opponent, but does not properly authenticate the evidence as being such. This MIM evidence is now inadmissible not only because it has not been properly authenticated, but also because it is an inadmissible hearsay statement if offered for the truth of the matter asserted.[128] Therefore, in such a case, the determination of the hearsay issue would necessarily depend on whether the evidence was properly authenticated.

---

123 *See* FED. R. EVID. 802 ("Hearsay is not admissible unless any of the following provides otherwise: a federal statute; these rules; or other rules prescribed by the Supreme Court."). *See also* Daniel J. Capra, *Electronically Stored Information and the Ancient Documents Exception to the Hearsay Rule: Fix It Before People Find out about It*, 17 YALE J.L. & TECH. 1, 6 (2015) (explaining the "ancient documents rule" as containing two rules that the document be over 20 years old, that it is in a place that it would likely be, its placement does not arouse suspicion, and a showing sufficient to establish the reasonable person standard that the document is what the proponent says it is).

124 FED. R. EVID. 801(c).

125 FED. R. EVID. 801(d)(1)-(2).

126 *See, e.g.*, United States v. Brinson, 772 F.3d 1314, 1320–21 (10th Cir. 2014) (acknowledging that in order for the court to admit instant messages as statements of the defendant into evidence, the government had to establish that the defendant authored the messages under a "fake name" by a preponderance of the evidence); People v. Bell, No. 307564, 2013 WL 1748603, at *2 (Mich. Ct. App. Apr. 23, 2013) (challenging the effectiveness of defendant's counsel for stipulating to the admission of text messages).

127 *See* Mix, *supra* note 111 (identifying that the "five evidentiary hurdles" to using electronically stored information, include relevance, authenticity, prohibition on hearsay, requirement of an original writing, and the probative value must outweigh the danger of unfair prejudice). *See also* Agnieszka A. McPeak, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, 48 WAKE FOREST L. REV. 887, 940-41 (2013) (recommending that courts be mindful to distinguish social media account activity when the content is posted either by the individual themselves or the individual is "tagged or referenced" when evaluating prejudice and importance to a case).

128 *See* Mix, *supra* note 111 (illustrating the point that information from social media sites are not "self-authenticating," because anyone can purchase an internet address and so corroboration by an independent party or other evidence is necessary).

For example, in a child trafficking and prostitution case, the 10th Circuit held that even though the defendant "presented evidence that other individuals had access to the Facebook account and had posted messages through it[,] the district court could reasonably find by a preponderance of the evidence that [the defendant] had authored the [Facebook] messages" in question, and thus "the district court properly admitted the Facebook messages as statements of a party opponent."[129] This case illustrates the importance of a proper authentication of MIM evidence in determining hearsay issues surrounding it.

A trial court may admit MIM evidence, which the court would ordinarily consider to be an inadmissible hearsay statement if it falls under one of the hearsay exceptions.[130] The North Dakota Supreme Court ruled that a Facebook message the murder victim sent to her sister would be accepted into evidence, despite the defendant's hearsay objection, because it fell under the state-of-the-mind hearsay exception.[131] The Georgia Supreme Court ruled that the Facebook messages the defendant exchanged with his murdered wife, who was pretending to be someone else, were properly accepted into evidence despite the defendant's hearsay challenges, because they fell under the "residual hearsay exception."[132] These cases show some of many possible ways by which the proponent of MIM evidence may move to admit the evidence despite its hearsay nature.

D. Requirement of the Original Document (Best Evidence Doctrine)

Article X of the Federal Rules of Evidence codifies the requirement of the original document, commonly known as the best evidence doctrine, under the title "Contents of Writings, Recordings, and Photographs."[133] This doctrine, "expresses a preference for original writings and recording over lesser evidence of the contents of those writings and recordings, such as testimony."[134]

---

[129] *Brinson*, 772 F.3d at 1321 (holding that the lower court reasonably concluded authorship of the Facebook messages through a preponderance of the evidence).

[130] *See e.g.*, FED. R. EVID. 803; FED. R. EVID. 804. *See also* Andrew M. Grossman, *No, Don't IM Me-Instant Messaging, Authentication, and the Best Evidence Rule*, 13 GEO. MASON L. REV. 1309, 1320 (2006) (describing the business-records exception that allows for emails with a business' domain name to be self-authenticating, an exception to the hearsay rule).

[131] State v. Kalmio, 846 N.W.2d 752, 760-62 (N.D. 2014). *See also* FED. R. EVID. 803(3) (providing an exception to the rule against hearsay for then-existing state of mind evidence).

[132] *See* Smart v. State, 788 S.E.2d 442, 448-50 (Ga. 2016) (explaining that the Facebook messages in question did not lack the "exceptional guarantees of trustworthiness" required to be admissible under the residual hearsay exception, nor were their admission in plain error).

[133] *See* FED. R. EVID. 1002 ("An original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise.").

[134] Grossman, *supra* note 130, at 1321. *See also* Dale A. Nance, *The Best Evidence Principle*, 73 IOWA L. REV. 227, 227 (1988) ("[T]here exists, even today, a principle of

Therefore, this issue only arises when a party is seeking to prove the contents of a writing, recording, or photograph.[135] To prove the content of a writing, recording, or photograph, an original is required unless a statutory exception applies.[136] A party in a criminal trial will typically seek to prove the contents of a writing, recording, or photograph in one of two situations: (1) when the writing, recording, or photograph is by itself an element or defense of a crime that the party seeks to prove, or (2) when the contents of the writing, recording, or photograph, if proven, will bolster an assertion made by the party.[137]

MIM evidence can fall under either of the two categories mentioned above.[138] For example, in a child solicitation case, the contents of the MIM conversation itself would be the key evidence that would directly prove many of the elements of the case, and thus fall under the first category.[139] In most other instances, MIM evidence would fall under the second category, in that it aids its proponent to prove a fact, which in turn would help its proponent to prove an element or a defense to the charged offense.[140]

Courts have generally held that "screenshots" of the IM conversation are admissible to prove the contents of the messages.[141] But is there any sort of minimum quality requirement for such screenshot evidence? There appears to be no current case law answering that question directly for us.[142] However, there are some cases that may be able to give us some useful guidance regarding the issue.

In a recent shaken baby syndrome case, the Arkansas Court of Appeals was faced with the issue of whether the court properly admitted a black-and-white

---

evidence law that a party should present to the tribunal the best evidence reasonably available on a litigated factual issue.").

135 Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 56 (2009).

136 FED. R. EVID. 1002.

137 Goode, *supra* note 135.

138 Goode, *supra* note 135, at 57-58.

139 *See generally* United States v. Jackson, 488 F. Supp.2d 866, 869-73 (D. Neb. 2007); United States v. Lundy, 676 F.3d 444, 446-47, 451 (5th Cir. 2012).

140 *See*, *e.g.*, Kays v. Commonwealth, 505 S.W.3d 260, 269-70 (Ky. Ct. App. 2016) (discussing whether Facebook Messenger and Viber messaging evidence should be used to show the nature of a relationship between the defendant, a high school teacher and volleyball coach, and the victim, one of the volleyball players in his team, in a rape and sodomy case).

141 *See*, *e.g.*, State v. Frank, 192 So.3d 888, 894-95 (La. App. Ct. 2016) (holding that the screenshots of Kick messaging are admitted into evidence); Sublet v. State, 113 A.3d 695, 698 (Md. Ct. App. 2015) (holding that screenshots of Facebook messages and screenshots of Twitter direct messages are admitted into evidence).

142 *See* FED. R. EVID. 901 (presenting no test measuring quality, the only concern seems to be independently determining the authenticity of the screenshot by adhering to FRE 901, there are no additional requirements at this time).

copy of the CT scan of the baby's brain into evidence.[143] The court noted that there was some concern about the quality of the evidence, because "[t]he image (a poorly reproduced paper copy at that) is not readily identifiable as being one of [the baby]'s brain because there is no name, birth date, or some other specific personal identifier on the reproduced image that links it to [the baby]."[144] The majority in this case ultimately punted on the question, noting that

> [w]e need not decide if the CT scan was properly authenticated because even if it was not, its admission would be a harmless error given the whole of Dr. Laken's testimony and the multiple sources of medical information she relied on when giving her opinion—including the X-ray of [the baby]'s leg that the doctor used to show that he had a fracture consistent with having experienced severe physical abuse.[145]

In her concurrence to the majority opinion, Judge Gruber expressed her belief that the CT scan of the baby's brain was properly authenticated, because "[t]he printout of the CT scan introduced by the trial court and authenticated by a witness with knowledge, Dr. Laken, falls within the definition of an 'original' under subsection three of Arkansas Rule of Evidence 1001."[146] In support of her assertion, Judge Gruber relied on *Donley v. Donley*,[147] where the Arkansas Supreme Court "held that 'screenshots' of comments on a Facebook photograph were properly authenticated when a witness testified that the comments were made using her Facebook account."[148] The Court's decision and Judge Gruber's concurrence here tell us that even a screenshot evidence of a particularly poor image quality may still be admissible when buttressed by the supporting testimony of a knowledgeable witness.

However, in a recent case involving Instagram messages, the Louisiana Court of Appeal ruled that the black-and-white printouts of the screenshots of the Instagram messages were not properly authenticated and therefore the trial court abused its discretion in ruling the evidence admissible.[149] The Court noted that "there [was] no testimony as to how the images on the phone shown to Officer Harvey were copied or reproduced onto paper"[150] and the State did "not have color copies, nor [did] they have copies that [were] clearer or less blurry."[151] The

---

143 *See generally* Washington v. State, 2016 Ark. App. 565, 2 (App. Div. 2016).

144 *Id.* at 6.

145 *Id.*

146 *Id.* at 10 (Gruber, J., concurring).

147 *Id.* (citing Donley v. Donley, 493 S.W. 3d 762, 770 (Ark. 2016)) (noting that Arkansas Rule of Evidence 901 properly authenticates circumstantial evidence when it ties one of the parties to the screenshot).

148 *Id.* (citing Donley v. Donley, 493 S.W. 3d 762, 770 (Ark. 2016)) (summarizing the holding of *Donley* in which the court relies on to conclude how screenshots are best authenticated).

149 State v. Smith, 192 So.3d 836, 845 (La. Ct. App. 2016) (leaving to question the exact nature of the evidence at question such as whether it deals with Instagram public posts or Instagram private messages).

150 *Id.* at 838.

151 *Id.* at 845 n.3.

Court also quoted and discussed a part of the State's direct examination of the Officer who testified in support of the evidence, which highlighted the poor quality of the black-and-white printout of the screenshot:

> Q. So whatever form of communication that is, whether it's Instagram or text messages—
>
> A. uh-huh.
>
> Q—next to the words written by the defendant, is there a picture?
>
> A. The picture—I can't see, I can't see—it's kind of fuzzy, so I don't know...
>
> Q. Do you recognize the document I gave you?[152]

Upon further questioning, "Officer Harvey further testified that she could not make out any other portions of the social media post. The officer stated: 'Not on this paper, no, ma'am, I cannot see; it's very, it's very faint . . . You can see certain things but not whole statements.'"[153] This case indicates that even though the poor quality of the screenshot printout of MIM evidence would not necessarily make the evidence inadmissible based on the best evidence doctrine alone, it could still become a problem in authenticating the evidence and thus render the evidence inadmissible nonetheless.[154]

Furthermore, it is conceivable that at certain point, the court will draw the line at the poor quality of the screenshot printouts, and rule that admitting an evidence of such a poor quality would be unfair to the opponent of the evidence.[155] Therefore, such evidence will have to be adequately supported by the testimony of a knowledgeable witness so that the trial judge could rule that a reasonable juror would find the evidence to be what the proponent claims it to be.[156]

E. Exclusion of Relevant MIM Evidence

---

[152] *Id.* at 838.

[153] *Id.* at 839.

[154] *See In re* Gonzales, 355 B.R. 644, 648 (Bankr. N.D. Ohio 2006) ([T]he copy of the check presented to the Court for comparison is of sub-par quality. Although not fatal to its admissibility, the poor quality of the check makes this Court reluctant to use it for comparison purposes.").

[155] *See* FED. R. EVID. 1003; *cf.* United States v. Rogozinski, 339 Fed.Appx 963, 967-68 (11th Cir. 2009) ("Rogozinski argued that the district court should not have excluded the check under Federal Rule of Evidence 1003 because it was a duplicate that 'wasn't the same color' and 'was barely legible.' Rogozinski commented that 'even the jury laughed when they saw it[.]' . . . [W]e disagree. . . . Although the copy of the check is blurred slightly, it is not of such poor quality that it was unfair to admit into evidence.").

[156] *See* Commonwealth v. Wright, 323 A.2d 349, 354 (Pa. Super. Ct. 1974) (Hoffman, J., dissenting) (illustrating how in this particular case he did not believe that the complainant was able to provide the support necessary to cure the "poor quality" of the evidence at hand).

An otherwise admissible MIM evidence may nonetheless be inadmissible "if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence."[157] This issue is especially likely to appear when the MIM evidence in question deals with a party's other acts that are not subjects of the trial.[158] Moreover, "[e]vidence of a crime, wrong, or other act is not admissible to prove a person's character in order to show that on a particular occasion the person acted in accordance with the character."[159] Although such evidence may be admissible for another purpose, such as proving motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident,[160] the criminal law's presumption against propensity evidence is so strong that its danger of unfair prejudice may easily outweigh what probative value it may have.[161]

A Massachusetts appellate court held Facebook messaging evidence of other bad acts is admissible in an underage rape case because

> [t]he conversations illustrate how the defendant cultivated the victim's feelings toward him, educated her about various forms of sexual interaction, and manipulated her insecurities to cause her to fear the loss of his affections. . . Though the lurid nature of the conversations undoubtedly caused prejudice to the defendant, the prejudice flowed directly from their properly probative effect to illustrate the development of the relationship between the defendant and the victim, its increasingly sexually charged character, and their shared reflection on several sexual encounters. The prejudice, in other words, was not unfair.[162]

On the other hand, a New York appellate court held in a gun possession case that the trial court erred in admitting Facebook messages the defendant sent

---

157 FED. R. EVID. 403.

158 *See* FED. R. EVID. 404(b)(1) (stating that other bad acts as evidence is not admissible to prove a person's character in order to show that on the occasion in question the person acted in accordance with this character trait).

159 FED. R. EVID. 404(b)(1).

160 FED. R. EVID. 404(b)(2).

161 *E.g.*, Michelson v. United States, 335 U.S. 469, 475–76 (1948). The Court explained that:

> Courts that follow the common-law tradition almost unanimously have come to disallow resort by the prosecution to any kind of evidence of a defendant's evil character to establish a probability of his guilt. Not that the law invests the defendant with a presumption of good character, but it simply closes the whole matter of character, disposition and reputation on the prosecution's case-in-chief. The State may not show defendant's prior trouble with the law, specific criminal acts, or ill name among his neighbors, even though such facts might logically be persuasive that he is by propensity a probable perpetrator of the crime. The inquiry is not rejected because character is irrelevant; on the contrary, it is said to weigh too much with the jury and to so overpersuade [sic] them as to prejudge one with a bad general record and deny him a fair opportunity to defend against a particular charge. The overriding policy of excluding such evidence, despite its admitted probative value, is the practical experience that its disallowance tends to prevent confusion of issues, unfair surprise and undue prejudice.

Id.

162 Commonwealth v. Gilman, 54 N.E.3d 1120, 1126 (Mass. App. Ct. 2016).

because "the prejudice in admitting them far outweighed any probative value. Allowing the jury to hear [the defendant] boasting about a shootout involving several different types of firearms, months after the crime on trial, could have led the jury to convict him based solely on his propensity for gun violence."[163] These cases illustrate that otherwise relevant and admissible MIM evidence may nonetheless be deemed inadmissible if the trial court determines that its probative value is substantially outweighed by a danger of unfair prejudice or other concerns of fairness.

CONCLUSION

To be admissible into evidence, MIM evidence must (1) be relevant, (2) be authentic, (3) be non-hearsay (or fall under a hearsay exception), (4) satisfy the best evidence doctrine, and (5) not have its probative value substantially outweighed by the danger of unfair prejudice or other concerns of fairness.[164]

To be relevant, MIM evidence must connect to a genuine issue at trial without being too attenuated from the issue.[165] Courts generally employ the "reasonable juror" standard in authenticating MIM evidence; this requires the proponent of the MIM evidence to provide proof that a reasonable juror could find the evidence is what the proponent claims it to be.[166] The bar is pretty low, and courts have held circumstantial evidence, including the testimony of a knowledgeable witness, to be adequate for such purposes.[167]

This does not mean that any MIM evidence would be automatically admissible by the virtue of its existence.[168] At least one federal circuit court has rejected the Government's attempt to admit certain MIM evidence as self-authenticating.[169] Separately, a Louisiana appellate court has also held a corroborating witness's extremely poor performance failed to meet the

---

[163] People v. Singleton, 139 A.D.3d 208, 215 (N.Y. App. Div. 2016).

[164] FED. R. EVID. 403; FED R. EVID. 404(b); FED. R. EVID. 801(d).

[165] *See* State v. Birdshead, 871 N.W.2d 62, 81 (S.D. 2015) (stating that the circuit court is required to conduct a two-part balancing test, the first part being that the court needs to determine whether the other-act evidence is relevant to some material issue in the case other than character).

[166] *See* Sublet v. State, 113 A.3d 695, 722 (Md. 2015) (applying the reasonable juror standard to Twitter private messages and Facebook messages).

[167] *See* Campbell v. State, 382 S.W.3d 545, 551 (Tex. App. 2012) (holding that Facebook messages were properly authenticated because when combined with other circumstantial evidence, the record may support a finding by a rational jury that the messages were authored and sent by the defendant).

[168] *See* State v. Smith, 192 So.3d 836, 845 (La. Ct. App. 2016) (holding that since the evidence of social media posts were not properly authenticated and the State did not carry its burden, the evidence should not be admitted).

[169] *See* United States v. Browne, 834 F.3d 403, 409 (3d Cir. 2016) (concluding that Facebook chat logs do not qualify as self-authentication).

"reasonable juror" standard in authenticating the MIM evidence.[170] Authenticating MIM evidence is also crucial for determining whether the court deems the MIM evidence as a statement of a party opponent, and therefore, an admissible non-hearsay statement when the proponent of the evidence offers it for the truth of the matter it asserts.[171]

As to the issue of what satisfies the "best evidence" doctrine, courts generally consider the printout of the screenshot of MIM evidence to be an admissible duplicate of the original evidence satisfying the requirements.[172] Extremely poor quality of the printout, however, can negatively affect the authentication of the evidence, rendering it inadmissible.[173] Furthermore, extremely poor quality of the printout evidence may also cause the court to deny its admission because its probative value would be substantially outweighed by concerns of fairness.[174]

Although otherwise admissible, MIM evidence may still be inadmissible "if its probative value is substantially outweighed by a danger of . . . unfair prejudice" or other concerns of fairness.[175] This issue is especially important to consider when dealing with MIM evidence that deals with other bad acts of a criminal defendant that are not the subjects of the trial itself.

---

[170] *See Smith*, 192 So.3d at 842-43 (stating that because the State did not attempt to bring someone in to corroborate the social media post that a reasonable jury would not be able to authenticate it).

[171] FED. R. EVID. 801(d)(2); *see* Dylan Charles Edwards, *Admissions Online: Statements of a Party Opponent in the Internet Age*, 65 OKLA. L. REV. 533, 540 (2013) (explaining that Rule 801(d)(2) is only implicated if the statement is offered in evidence to prove the truth of the matter asserted).

[172] Josh Gilliland, *The Admissibility of Social Media Evidence*, 39 LITIG. J. 20, 21 (2013).

[173] *See In re* Gonzales, 355 B.R. 644, 648 (Bankr. N.D. Ohio 2006) ("The copy of the check presented to the Court for comparison is of sub-par quality. Although not fatal to its admissibility, the poor quality of the check makes this Court reluctant to use it for comparison purposes.").

[174] *See* United States v. Rogozinski, 339 F. App'x 963, 967-68 (11th Cir. 2009) (stating that Rogozinski commented that "even the jury laughed when they saw [the poor quality]" . . . [W]e disagree. . . . Although the copy of the check is blurred slightly, it is not of such poor quality that it was unfair to admit into evidence."). *See generally* Ann K. Wooster, Annotation*, Criminal Defendant's Tattoos, Scars, or Injuries as Factor in Determination of Whether Circumstances of Witness's Identification of Defendant in Photographic Array Shown by Police to Witness Were Impermissibly Suggestive as Matter of Federal Constitutional Law*, 21 A.L.R. 7TH 6 (2017).

[175] FED. R. EVID. 403.