LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
MONDAY, NOVEMBER 21, 2022

PERSPECTIVE

GUEST COLUMN

Mobile messaging and e-discovery

By Daniel B. Garrie and Gail A. Andler

There are two obvious parties to every text message conversation: you, and the recipient. Under certain circumstances, typically not anticipated at the time of the conversation, there may be other recipients, such as the court or an adverse party, when the texts are sought as evidence in litigation.

There is also a certain paradox to mobile messaging: it is the most discreet and most recorded form of communication. Many people assume that text messages are private, but recent momentous events have shown otherwise. From investigating the Capitol siege in the Jan. 6th hearings to high-profile court cases such as *Depp v. Heard, Commonwealth v. Carter,* and *United States of America v. Anthony Weiner*, mobile messaging is playing a pivotal role in the courtroom.

The constantly evolving nature of mobile messaging has become foundational in the realm of electronic discovery (e-discovery): the process of identifying, collecting, and producing electronically stored information (ESI) for legal purposes by electronic means. Analogous to social media posts and other forms of digital communication, mobile messages can be used as evidence in court and can be instrumental in the outcome of criminal and civil cases. However, while laws concerning e-discovery are front and center, their application to mobile communications, which merges oral and data communications, presents a new frontier that raises a litany of unique issues regarding privacy, data retention, and production. This article examines those issues.

Mobile messaging, or text messaging, refers to the ability to send and receive text-based messages via mobile phones using Short Message Services (SMS), a protocol used for sending short messages over wireless networks. The convenience and simplicity of SMS, combined with the evolution of pricing models have contributed to significant growth of the SMS market in Asia and North America over the past few years. According to a 2021 Statista report, there were 2.2 trillion text messages exchanged in 2020, an increase of 102 billion messages since 2019. (Statista. 2021. Total number of SMS and MMS messages sent in the United States from 2005 to 2020).

When considering specific demographics, a 2020 Statista report shows that 83% of teens ages 13-17 used text messages to keep in touch with friends and family during the COVID-19 pandemic, followed by phone calls (72%), social media (66%) and video calling (66%). (Statista. 2021. Technologies used by teens in the United States to stay connected to friends and family they no longer see in-person during the coronavirus pandemic in April 2020). And of course, with new technologies come new legal proceedings. So, just like social media posts and other forms of digital communication, text messages can be used in court as evidence and can be instrumental in deciding criminal and civil cases.

With the advent of the personal computer revolution in the late 1970s and early 1980s, courts grappled with the integration of e-discovery's highly variable cost structure into the Federal Rules' traditional discovery principles. In 1995, Magistrate Judge Peck issued an opinion and order regarding the discovery of "data processing files" that famously pronounced that "today it is black letter law that computerized data is discoverable if relevant." See, *e.g., Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 at 1 (S.D.N.Y. 1995) (holding order compelling production of documents, including data compilations).Yet, the early 2000s saw federal courts struggle to align e-discovery with technological advances, notably in *McPeek v. Ashcroft*, 202 F.R.D. 3, 35 (2001) (holding that the DOJ will have to search in the restored emails for any document responsive to any of plaintiff's requests for production of documents, and then file a sworn statement to the expense and time used for the search); *Rowe Entm't, Inc. v. The William Morris Agency*, 205 F.R.D. 421, 433 (S.D.N.Y. 2001) (holding that "plaintiffs shall designate one or more experts who shall be responsible for isolating each defendant's emails and preparing them for review. The defendants shall have the opportunity to object to any expert so designated"); and *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (holding that because the cost-shifting analysis is so fact-intensive, it is necessary to determine what data may be found on the inaccessible media. Requiring the responding party to restore and produce responsive documents from a small sample of the requested backup tapes is a sensible approach in most cases). In such cases, corporations had been ordered to produce, oftentimes at considerable expense, computerized information such as e-mail

Daniel B. Garrie, Esq. *is the founder of Law & Forensics, a global legal engineering company, and a Nationwide neutral who specializes in discovery, business, forensics, cybersecurity, privacy, class actions, and cryptocurrency, and* **Gail A. Andler** *is a retired Orange County Superior Court judge and Southern California-based neutral who specializes in business, employment, class actions, and mass torts.*

messages, support systems, software, voicemail systems, computer storage media, backup tapes, and telephone records. *Id.*; see also *McPeek*, supra note 20 & *Rowe*, supra note 21.

Considering the variety of forms electronic information may take, it was unclear which forms met the definition of discoverable "documents" under Federal Rule of Civil Procedure Rule 34. See Hon. Shira A. Scheindlin & Jeffery Rabkin, Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?, 41 B.C. L. REV. 327, 347 (2000) (discussing that deleted ESI, "embedded data" (i.e. application metadata), and log-on and network data (i.e. system metadata) may be relevant discoverable information, but does not fit neatly within the definition of documents in the prior version of Rule 34). In attempts to mitigate this problem, the Federal Rules were broadly amended in December 2006 to provide clearer guidance regarding the production of ESI in litigation. These new rules coined the term Electronically Stored Information (ESI), which is data "stored in any medium from which information can be obtained directly or, if necessary, after translation by the responding party into a reasonably usable form," including data received or transmitted by mobile devices, and set out several requirements for ESI identification and production. Fed. R. Civ. P. 34(a).

Courts have responded to these new rules by actively requiring all relevant parties in litigation to preserve, identify, disclose and produce any relevant information on an electronic device. See, *e.g., Arista Records LLC v. Usenet.com, Inc.*, 608 F. Supp.2d 409, 440 (2009) (imposing attorneys fees, costs, and adverse inference sanction for defendant's failure to preserve usage data and digital music files from its servers); see also *Fox v. Riverdeep, Inc.*, No. 07 Civ. 13622, 2008 U.S. Dist. LEXIS 101633 (E.D. Mich. Dec. 16, 2008) (awarding sanctions where defendant failed to preserve evidence, including emails, once it received cease and desist letter); *Gordon Partners, et. al. v. Blumenthal*, 244 F.R.D. 179, 200-201 (S.D.N.Y. 2007) (imposing adverse inference spoliation sanction in securities fraud action because defendant corporation had the practical ability to obtain documents it needed from a non-party corporation and defendant corporation's failure to preserve emails relevant to plaintiffs' claims was grossly negligent); see also *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614, 636 (D. Co. 2007) (imposing monetary sanctions and requiring defendant to bear the cost of a second review of its computer files and website for relevant ESI). Failure to comply in "good faith" could result in sanctions from the court. Fed. R. Civ. P 37(e): The good faith requirement of Rule 37(e) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. Nonetheless, it is not explicit, but allows for the inability of production of discoverable evidence when the supplying party is unable to do so because of honest unforeseeable circumstances that are unrelated to the litigation or through no fault of their own are unable to produce such information. However, among the 2006 amendments was also the creation of a "safe harbor provision" that protected individuals against sanctions from ESI lost as a result of the "routine, good faith operation of an electronic information system." *Id.* At large, the provision sought to limit the disclosure of trade secrets, and inadvertent release of discoverable information and address age-old privacy concerns. However, the 2015 amendments to the Federal Rules withdrew such protection and made this significant statement: if ESI that should have been preserved in anticipation of litigation is lost because a party failed to take "reasonable steps" towards its preservation, it cannot be restored or replaced through other discovery, the court can enter Rule 37 sanctions, even without a finding of prejudice. *Id.* Such amendments were concerning to many litigators, especially with the increasingly complex and expansive nature of most mobile messaging.

Subsequent court cases spotlight the heightened challenges mobile messaging presents in litigation as a result of rapidly advancing technological features. For example, in *Fast v. GoDaddy*, the court contemplated whether Facebook Messenger's "unsend" feature prevented reasonable disclosure of evidence and concluded that the action warranted the issuance of an adverse inference instruction at trial. See *Fast v. GoDaddy.com LLC*, No. CV-20-01448-PHX-DGC, 2022 WL 901380 (D. Ariz. Mar. 28, 2022). Similarly, in *Paisley Park Enters., Inc. v. Boxill* and *Nuvasive, Inc. v. Absolute Med*, the courts found that by enabling the iOS automated deletion feature, a user-enabled automated deletion feature on their Apple iPhones, Plaintiffs demonstrated intent to eliminate relevant evidence and failure to preserve relevant text messages. See *Paisley Park Enters., Inc. v. Boxill*, 330 F.R.D. 226 (D. Minn. 2019); *Nuvasive, Inc. v. Absolute Med., LLC*, No. 6:17-CV-2206-CEM-GJK, 2021 WL 3008153 (M.D. Fla. May 4, 2021).

Given the burgeoning of new technologies, courts need to recognize that identifying, preserving, and producing mobile messages imposes significant costs on both parties of litigation. Considering the costs of third-party involvement from telecommunication service providers, the intricacy of mobile messaging features, and greater protections traditionally provided to private, non-business communications, it is imperative that courts carefully evaluate the necessity and scope of mobile discovery requests and institute a mobile-specific discovery rule that balances cost versus rationality. This includes assessing the need for the requested discovery in comparison to the corresponding financial burdens and policy concerns. Mobile data continues to be on an upward trajectory in our everyday lives and shows no signs of abating. Since messaging on mobile devices has become an ordinary practice in our daily lives, it is easy to overlook the wealth of potentially relevant information in everyone's hands. However, with the unique characteristics and increasing prevalence of mobile messaging, laws need to develop in accordance with the evolution of extracting evidence.