JONES DAY | One Firm Worldwide℠

WHITE PAPER

June 2019

Current Trends: Discovery of Electronically Stored Information on Mobile Devices and Social Media

The rise of mobile technology and the pervasiveness of social media have introduced new questions regarding a corporation's preservation responsibilities pertaining to electronically stored information ("ESI") and to its potential discoverability.

This Jones Day *White Paper* provides an overview of recommendations for identifying and preserving ESI, and examines how discovery rules apply to mobile devices and social media. Particular attention is given to preservation requirements and the possible sanctions imposed for data loss.

TABLE OF CONTENTS

The evolution of mobile technology and social media continues to raise new questions about the preservation and discoverability of electronically stored information ("ESI"). Technological growth is constantly changing the scope of discoverable ESI and the type of ESI subject to preservation obligations. Practically speaking, these issues can heavily impact businesses that rely on mobile technology and social media to communicate. In turn, the courts have grappled with the application of these ever-evolving business platforms to the more traditional discovery parameters set by the Federal Rules of Civil Procedure. Concerns regarding the permissibility and scope of obtaining these types of ESI have left corporations questioning the extent to which there is a duty to preserve and what information is discoverable.

This *White Paper* provides an overview of how courts have applied the Federal Rules to the discovery of mobile devices and social media, giving insight to navigating this new age of e-discovery.[1]

IS MOBILE-DEVICE AND SOCIAL-MEDIA ESI DISCOVERABLE?

Text Messages and Social Media

Some courts have held that text messages are discoverable if the requesting party can show that the messages are relevant and in the possession and control of the responding party.[2] Some courts have also ordered the production of social-media ESI, including Facebook messages or posts. Production of social-media posts may be ordered when the information sought directly references the opposing party or is relevant to the issues raised in the complaint. However, courts have been careful not to order over-inclusive production of social-media data, likening such "unfettered access" to inviting the requesting party to "rummage through the desk drawers and closet in plaintiff's home."[3]

Personal-Behavior Data, Mobile Applications, and Images

Physical activity and application usage recorded on mobile devices have also been held to be discoverable if relevant and in the custody, possession, or control of the responding party. For example, the Eastern District of Texas ordered a plaintiff to produce her Fitbit data, phone fitness applications, and other phone application usage where the defendant claimed such information was relevant to his rebuttal of the plaintiff's injury claims.[4] There, the plaintiff was required to produce browser histories, event logs, and other activity logs, but was not required to provide the actual content of the applications used because it was the use of the devices, not the information contained within, that was relevant to the defendant's rebuttal.[5] The court noted that the defendant's request to review all of the plaintiff's electronic devices posed a significant intrusion into her privacy, which would be appropriate only where the plaintiff had failed to comply with her discovery obligations.[6]

Information exchanged using end-to-end encrypted phone applications such as WhatsApp and iMessage present unique production challenges. When these applications are used, service providers cannot view the exchanged information and the information cannot be extracted from the devices without decryption.[7] Further complicating matters are "ephemeral" applications such as Snapchat and Wickr, where images and messages transferred remain on the recipient's mobile device for a limited period of time before expiring. Once the information is deleted, it is impossible to obtain.[8] How courts deal with these issues is discussed below, along with the methods employed by the courts to rectify prejudice resulting from the use of these applications.

DISCOVERY RULES AS APPLIED TO MOBILE DEVICES, SOCIAL MEDIA, AND OTHER MOBILE DATA

The most significant recent developments in the case law concerning discoverability of ESI on mobile devices and social media include: (i) developing the meaning of possession/custody and relevancy of ESI stored on mobile devices; (ii) resolving questions of burden; and (iii) applying curative measures or sanctions where appropriate. The following sections provide an overview of how courts have resolved these issues.

When is ESI that is Stored on Employees' Mobile Devices Within the Responding Party's Custody, Possession, or Control?

Parties are limited to obtaining discovery that is within the responding party's "possession, custody, or control."[9] While the definition of "control" varies by jurisdiction, it is often defined

as the "legal right to obtain the documents requested" or the "practical ability" to obtain the requested information.[10] The question of who maintains control of a business's data is subject to a fact-specific analysis that considers both ownership and usage of the device at issue.

- **Company Ownership**. Data stored on employer-owned devices is usually considered to be under the employer's control; thus, company-owned mobile devices used by employees are regularly subject to discovery when the company is faced with litigation if the discovery sought is also relevant and proportional to the needs of the case.[11]

- **Employee Ownership**. Some courts have found that a company "controls" data for purposes of discovery even when the employee owns the device at issue if the company has directed employees to use their own devices for work.[12] In some cases, companies will reimburse employees for mobile-device usage fees, but courts have yet to address the impact of such practices on the question of "control." Relatedly, there is a gray area where an employer has not affirmatively instructed or permitted employees to use their personal devices for work purposes. In order for discovery to be allowed in such situations, it is likely that a requesting party must, at a minimum, show that employees used their personal devices for business purposes and there is potentially relevant data on them.[13]

The Technological Challenges of Applying Proportionality and Burden Principles to Mobile-Device and Social-Media ESI Discovery

Collecting ESI from mobile devices and social media is expensive and time-consuming.[14] Parties who object to discovery requests must show why the requests are disproportionate to the needs of the case or overbroad.[15] Specifically, the objecting party must provide details regarding the time, cost, and resources required to obtain the information in order to show the court that the discovery is unduly burdensome[16] and that the burden or expense outweighs the benefit of the information[17]—unsupported assertions are likely not enough.

While some mobile-device data can be easily duplicated, more complicated data extraction usually requires professional assistance and additional expenses. For example, data-collection service providers may need to bypass security or retrieve deleted data.[18] If there are no in-house experts who can provide specifics regarding cost and effort to retrieve data, a party may have to consult outside experts, generating additional litigation expenses.

Data Preseveration and the Risk of Self-Destructing Messaging Applications

Once the duty to preserve has been triggered, reasonable steps should be taken to preserve data.[19] Generally, the duty to preserve is triggered when litigation is foreseeable, such as when a government investigation is initiated or a demand letter is received. Once on notice, parties should institute a litigation hold for all relevant custodians and data-storage systems for relevant ESI to prevent the loss of relevant data.

Loss of relevant data, or "spoliation," is defined as the "destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation."[20] Perfection is not required, but courts will consider a party's sophistication, resources, and costs in its reasonableness evaluation. To confirm that preservation methods were reasonable, the courts may request that parties provide information on their preservation efforts and resources.[21] For parties with fewer resources, such as individual litigants, less expensive and less comprehensive efforts may be reasonable. On the other hand, parties with extensive litigation resources and experience in preserving data may be held to a higher standard.

Generally, the use of self-deleting applications or programs to conduct business should be avoided. Recent sanctions against Uber illustrate the peril of using such applications. In a case between Uber and Waymo, information exchanged on Wickr became the subject of discovery. Wickr is an instant-messenger application where only the sender and recipient can read the exchanged messages and the messages are permanently deleted within a set period of time after being read. Uber instructed its employees to use Wickr to exchange instant messages. Later, discovery of the instant messages was impossible. To sanction Uber, the court permitted Waymo to present evidence of Uber's use of Wickr to explain missing information in Waymo's proof that Uber had misappropriated trade secrets.[22] Whether Uber's use of Wickr was *intended* to shield the exchanged information from discovery was immaterial to the court's decision to allow Waymo to present this evidence.

PLANNING AHEAD

Corporate Policies for Use of Mobile Devices

Companies should decide whether to issue company-owned mobile devices or to require employees to use their own devices. A related decision is when and to what extent (if at all) employers permit their employees to use mobile devices for work-related purposes. If mobile devices are necessary to conduct business, companies should consider writing and implementing clear mobile device policies for employees to follow that address these issues. Whatever the content of such policies, employers and employees should be aware that once litigation is reasonably anticipated, relevant data on employee mobile devices can be subject to preservation obligations—even in situations where the employee owns the device at issue.[23] Further, to avoid the outcome in *Waymo*, companies can adopt policies barring the use of self-deleting applications for work purposes. Companies can also consider mobile-data back-up systems, such as cloud applications, to avoid the inadvertent loss of data. As always, each decision on policies and practices will vary, depending on individual company circumstances.

Preservation Action Plans

Long before litigation is a concern, consider putting into place an action plan for handling litigation-related preservation issues that can be implemented immediately if litigation becomes reasonably foreseeable. Processes that the plan could cover include:

- Determining the scope of the preservation obligations;
- Drafting the litigation hold notice;
- Identifying individuals who may have relevant documents and should receive the legal hold;
- Creating the distribution list for the litigation hold notice;
- Identifying the information technology ("IT") personnel who are available to suspend normal-course deletion functions and other hold issues that may arise;
- Monitoring and tracking compliance with the litigation hold, such as discussing the litigation hold with key employees and periodically following up to confirm execution.

To help reduce errors in the preservation process, counsel should be involved when a company is developing or updating its mobile-device/social-media use policies and action plans. Ideally, the company should utilize in-house or outside counsel familiar with drafting comprehensive policies, as well as with the legal landscape of preservation obligations and the company's mobile information systems and other electronic data sources. As technology evolves rapidly, so does this area of law.

An action plan can provide the necessary information to identify relevant company-owned mobile devices along with personal devices that are being used for business purposes, including a plan for preserving that information. Among the strategies for preserving mobile-device/social-media information are: (i) mirror imaging of devices; (ii) collection and storage of company-issued devices; and (iii) printing of screenshots, photos, text messages, social-media chats, or blog posts (including the preservation of associate metadata when it is reasonable to do so, particularly when the process relies on the individual custodian's compliance, which creates risk). In addition, while Facebook and Twitter provide users the ability to download their own information, the metadata, timestamps, and link content may not be available in the downloaded form. To the extent this information is necessary, counsel may need assistance from the third-party platform provider to retrieve such data.

In creating any type of data-preservation plan for mobile devices or social media, consulting with a forensic collection vendor, in conjunction with knowledgeable counsel, can help ensure that the plan is as comprehensive as possible. When hiring an outside vendor to assist with data back-up or preservation, companies should discuss storage issues with the vendor, including: (i) holding periods; (ii) data access (to ensure that the data is secure); and (iii) data ownership. Entrusting internal company data to an outside vendor can simplify in-house operations, but it can also limit the company's control of the access and use of the data, if not negotiated prior to executing the contract. Reviewing the action plans to update and revise them on a regular basis can ensure compliance with the current laws.

The Litigation Hold Has Been Triggered—Now What?

Once litigation is reasonably foreseeable, counsel (either in-house or outside) should be engaged to provide guidance and advice while the action plan is implemented. Counsel can be valuable in limiting preservation to only necessary information (thus reducing preservation costs), as well as minimizing the risk of failing to preserve potentially discoverable data. This is particularly important in the mobile-device/social-media

space, as this area of law is rapidly evolving. Knowledgeable counsel will be able to quickly and efficiently ensure that the action plan is tailored to the law at the time the obligation to preserve is triggered.

Counsel's advice can substantially and positively impact the costs associated with preservation. If the efforts to preserve mobile data are unreasonable, counsel (with the help of the company) may be able to identify other, less costly sources of the same information. For example, if largely duplicate information exists on multiple platforms (a company biography page and LinkedIn), counsel can analyze the risks associated with preserving only the more accessible platform.

Overall, it is ideal to involve counsel early and often to maintain and implement the action plan. Because IT is critical to the success of the action plan, some companies have designated specific IT personnel as responsible for engaging with counsel on preservation issues. The designated IT personnel should be able to provide information about the company's systems and applications, which is critical to complying with preservation obligations and responding to discovery requests. In the event that mobile-device or social-media data is requested (and prior to agreeing or objecting to those discovery requests), data-collection vendors can be helpful in evaluating the extent of the time, costs, and resources required to obtain the data.

Frequent updates to counsel on the implementation of the action plan will place counsel in the best position to advise the company and defend its practices later on. For example, if a company ultimately wants to take the position that the cost of producing certain data outweighs the perceived benefit, counsel's involvement throughout the action plan implementation will provide important insight into the costs and time required to produce the data that is critical to successfully avoiding production.

WHEN ARE SANCTIONS IMPOSED AND HOW CAN COMPANIES AVOID THEM?

Failing to preserve relevant data can result in serious sanctions, especially where an intent to deprive can be shown.[24] Here, we provide a quick overview of how that framework applies to ESI stored on portable devices and social media.

In the event of spoliation, courts analyze whether: (i) the ESI *should* have been preserved; (ii) the lost ESI is a result of the party's failure to employ *reasonable* efforts to preserve it; and (iii) the data cannot be restored or replaced through other means to determine if and to what extent sanctions should be imposed.[25] If the answer to each inquiry is yes, then the ESI is truly lost, and sanctions may be appropriate. Federal courts can also impose sanctions against bad-faith actors, even if ESI is not actually lost.[26]

Sanctions come in all shapes and sizes. To determine the severity of the sanctions, courts typically first analyze whether the non-offending party has been prejudiced and whether the offending party had an intent to deprive.[27] Courts determine the existence and extent of prejudice by evaluating whether the lost information was relevant[28] and if so, whether reasonable steps were taken to preserve the data.[29] The intent to deprive is defined as "intend[ing] to impair the ability of the other side to effectively litigate its case."[30] If prejudice and/or intent to deprive is found, numerous sanctions are open to the court, including ordering the offending party to pay for sanction motion costs, instructing the jury that it may or must presume that the lost information was unfavorable to the offending party (also known as an adverse inference instruction), and even in the most extreme situations case dismissals and default judgments.[31]

Though the degree of culpability in the intent-to-deprive analysis is not always perfectly clear, there have been some cases where the loss of ESI on mobile devices and social media has resulted in sanctions. At least one court has found an intent to deprive where a defendant used his personal iPhone and iPad for business purposes (including using his iPad to take screenshots of hundreds of corporate emails) and subsequently "lost" the devices, finding that the defendant "knew or should have known" he was required to preserve the data.[32] In another case, the Southern District of New York imposed an adverse inference instruction sanction against a defendant for intentionally depriving the plaintiff of relevant text messages, even though a contracted nonparty was responsible for replacing his mobile device and not backing up the text messages in question.[33]

In the most egregious and willful instances of ESI destruction and intent to deprive, default judgments have been imposed. The Fifth Circuit held that a default judgment was appropriate

after a defendant failed to produce text messages despite having been ordered to do so by the district court.[34] The Ninth Circuit similarly held that the district court did not abuse its discretion when it entered a default judgment against a defendant because he willfully deleted data from his laptop, despite explicit court orders to preserve "all data" on his electronic devices.[35] While the degrees of culpability that can rise to the level of intent to deprive may vary, the willful defiance of a court order to preserve data has been cited by several courts as a ground for leveling the most severe sanctions.

CONCLUSION

Although navigating the discovery of ESI from mobile devices and social media is complicated, companies can, with the assistance of counsel, avoid common pitfalls by: (i) having a comprehensive understanding of the mobile-device and social-media data used within their companies; (ii) maintaining and properly implementing mobile-device and social-media usage and preservation policies to avoid data loss and sanctions; (iii) developing an action plan to preserve mobile-device and/or social media data to implement when the party reasonably anticipates litigation; and (iv) involving counsel in the drafting and implementation of the action plan. Proper steps to ensure that litigation holds extend to mobile devices and social media, when necessary, can enhance a company's comprehensive data preservation strategy.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus.

Jennifer Del Medico
New York
+1.212.326.3658
jdelmedico@jonesday.com

Tiffany D. Lipscomb-Jackson
Columbus
+1.614.281.3876
tdlipscombjackson@jonesday.com

Jennifer Jiang
Washington
+1.202.879.3820
jjiang@jonesday.com

ENDNOTES

1 This *White Paper* addresses discovery only under the Federal Rules of Civil Procedure.

2 *See, e.g.*, *Lawrence v. Rocktenn CP LLC*, No. 16-821, 2017 WL 2951624, at *1 (W.D. La. Apr. 19, 2017) (concluding that text messages were relevant and granting motion to compel); *Dennis v. Red River Entm't of Shreveport, LLC*, No. 14-cv-2495, 2016 WL 8729956, *1–2 (W.D. La. Jan. 8, 2016) (ordering production of text messages from the time period that was relevant to the case or the plaintiff's damages); *see also Walker v. Carter*, No. 12-cv-05384, 2017 WL 3668585, at *2 (S.D.N.Y. July 12, 2017) (confirming that the magistrate judge properly ordered the plaintiff to produce text messages).

3 *See Ogden v. All–Star Career Sch.*, 2014 WL 1646934, at *4 (W.D. Pa. April 23, 2014); *see also Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc.*, No. 2:06–cv–00788–JCM-GWF, 2007 WL 119149, at *7 (D. Nev. Jan. 9, 2007) (finding that the defendants failed to show a relevant basis for production of the plaintiff's Myspace.com private email messages). *See also Smith v. Hillshire Brands*, No. 13-2605-CM, 2014 WL 2804188, at *4 (D. Kan. June 20, 2014) (ordering production of "social networking documents that directly reference or mention defendant or matters raised in plaintiff's complaint," but finding the plaintiff's social-media activity to be irrelevant).

4 *Cory v. George Carden Int'l Circus*, 2016 WL 3460781, at *2–3 (E.D. Tex. Feb. 5, 2016) (finding that "a mobile app that indicates Plaintiff performs strenuous activities may be relevant to claims of injury or disability").

5 *Id.*

6 *Id.* at *1–3 (noting that agreeing to the defendant's request would allow a "stranger unlimited access to Plaintiff's emails (both personal and professional), private records, and exercise habits").

7 *See* Robert D. Keeling, *The Challenge of Collecting Data from Mobile Devices in eDiscovery*, 18 Sedona Conf. J. 177, 182–83 (2017).

8 Paresh Dave & Heather Somerville, *Uber's Use of Encrypted Messaging May Set Legal Precedents*, Reuters, Nov. 29, 2017.

9 Fed. R. Civ. P. 34(a)(1).

10 *Benisek v. Lamone*, 320 F.R.D. 32, 34 (D. Md. 2017); *see, e.g.*, *Searock v. Stripling*, 736 F.2d 650, 653 (11th Cir. 1984) (stating that "[c]ontrol is defined not only as possession, but as the legal right to obtain the documents requested upon demand"); *see also Ronnie Van Zant, Inc. v. Pyle*, 270 F. Supp. 3d 656, 669 (S.D.N.Y. 2017) (finding that the text messages of a nonparty contractor were nonetheless under the defendant's control).

11 *See Lalumiere v. Willow Springs Care, Inc.*, No. 1:16-CV-3133-RMP, 2017 WL 6943148, at *2 (E.D. Wash. Sept. 18, 2017) (noting that a "company controls the text messages of its employees on work phones"); *see also Stinson v. City of N.Y.*, No. 10 Civ. 4228, 2016 WL 54684, at *5 (S.D.N.Y. Jan. 5, 2016) (concluding that cell phones issued by a police department "were within the possession, custody, or control of the City, and were subject to the same preservation obligation as the City's other ESI").

12 *See H.J. Heinz Co. v. Starr Surplus Lines Ins. Co.*, No. 2:15-cv-00631-AJS, 2015 WL 12791338, at *4 (W.D. Pa. July 28, 2015) (stating that "with regard to Heinz data present on employee-owned personal mobile devices under its [Bring Your Own Device] program, Heinz has custody and control of Heinz's data" and that when employees' personal phones were used for work, discovery was permitted only "[t]o the extent that any of these employees sent or received text messages on their personal mobile devices relevant" to the case).

13 *Cotton v. Costco Wholesale Corp.*, No. 12-2731-JWL, 2013 WL 3819974, at *6 (D. Kan. July 24, 2013) (stating that the plaintiff "does not contend that Costco issued the cell phones to these employees, that the employees used the cell phones for any work-related purpose, or that Costco otherwise has any legal right to obtain employee text messages on demand. Accordingly, it appears to the court that Costco does not likely have within its possession, custody, or control text messages sent or received by these individuals on their personal cell phones."). *But see In re Pradaxa (Dabigatran Etexilate) Prods. Liab. Litig.*, MDL No. 2385, 2013 WL 6486921, at *18 (S.D. Ill. Dec. 9, 2013) (finding that the requesting party did not have to assume that the defendant's employees followed the policy prohibiting "substantive text messaging" with physicians).

14 *See* Keeling, *supra* note 10, at 182–83 (noting that costs can range from $1,000 to more than $1 million).

15 *See Heller v. City of Dallas*, 303 F.R.D. 466, 489–90 (N.D. Tex. 2014) (stating that "if all or part of a discovery request seeks documents or information not even reasonably calculated to lead to the discovery of admissible evidence, the responding party should make a specific objection explaining how and to what extent the requested documents or information are not relevant and discoverable under the Rule 26(b) standard and stand on that objection as to the portion of the request that is so objectionable while specifically describing the portion, if any, of the request to which the responding party is answering or producing documents"); *see also Ehrlich v. Union Pac. R.R. Co.*, 302 F.R.D. 620, 626 (D. Kan. 2014) (stating that the objecting party must show "undue burden or expense" and that the burden or expense would be unreasonable).

16 *Horizon Holdings, L.L.C. v. Genmar Holdings, Inc.*, 209 F.R.D. 208, 213 (D. Kan. 2002) (stating that an objecting party has the burden to "show facts justifying [its] objection by demonstrating that the time or expense involved in responding to requested discovery is unduly burdensome").

17 *Cardenas v. Dorel Juvenile Grp., Inc.*, 232 F.R.D. 377, 380 (D. Kan. 2005) (stating that the objecting party has "the burden to show not only undue burden or expense, but that the burden or expense is unreasonable in light of the benefits to be secured from the discovery"). For a broader discussion of the recent amendments to Rule 26, see our September 2015 *White Paper*, "Significant Changes to the Federal Rules of Civil Procedure Expected to Take Effect December 1, 2015: Practical Implications and What Litigators Need to Know."

18 *See* Keeling, *supra* note 10.

19 Fed. R. Civ. P. 37(e).

20 *Adorno v. Port Auth. of N.Y. & N.J.*, 258 F.R.D. 217, 227 (S.D.N.Y. 2009).

21 *See* Steven Baicker-McKee, *Mountain or Molehill?*, 55 Duq. L. Rev. 307, 317–23 (2017).

22 *Waymo, L.L.C. v. Uber Techs., Inc.*, No. C 17-00939 WHA (N.D. Cal. Jan. 29, 2018) (order granting Waymo the ability to present evidence of Uber's Wickr use).

23 *Id.* (concluding that "[t]he litigation hold and the requirement to produce relevant text messages, without question, applies to that space on employees' cell phones dedicated to the business which is relevant to this litigation"); *see, e.g.*, *Alter v. Rocky Point Sch. Dist.*, No. 13–1100 (JS) (AKT), 2014 WL 4966119, at *10 (E.D.N.Y. Sept. 30, 2014) (requiring school-district employees to preserve relevant information on "whatever devices contained the information" without taking into account whether the employees were instructed or permitted to use their cell phones for business purposes); *Small v. Univ. Med. Ctr. of S. Nev.*, No. 2:13–cv–00298–APG–PAL, 2014 WL 4079507, at *11 (D. Nev. Aug. 18, 2014) (finding that employees' use of personal mobile devices for work-related purposes conferred on the employer an affirmative duty to preserve text messages); *cf. United States v. Vaughn*, No. 14-23 (JLL), 2015 WL 6948577, at *19–20 (D.N.J. Nov. 10, 2015) (finding that the government's failure to preserve text messages on a detective's personal phone in a criminal case warranted sanctions).

24 *Browder v. City of Albuquerque*, 187 F. Supp. 3d 1288, 1299–1300 (D.N.M. 2016) (ordering sanctions when the defendant failed to preserve evidence on an officer's cell phone and requiring the offending party to pay all reasonable expenses incurred by the plaintiff in bringing the motion for sanctions); *see, e.g.*, *Congregation Rabbinical Coll. v. Vill. of Pomona*, 138 F. Supp. 3d 352, 388 (S.D.N.Y 2015) (finding that the defendants were obligated to preserve a Facebook post and related text messages, that a clear intent to deprive existed when the defendants deleted the post, and providing adverse inference sanctions as a result); *see also Cat3, LLC v. Black Lineage, Inc.*, 164 F. Supp. 3d 488, 497–98 (S.D.N.Y. 2016) (stating that "sanctions would be available under the court's inherent authority even if Rule 37(e) did not apply").

25 Fed. R. Civ. P. 37(e); *see also Living Color Enters., Inc. v. New Era Aquaculture, Ltd.*, Case No. 14–CV–62216–MARRA-MATHEWMAN, 2016 WL 1105297, at *4 (S.D. Fla. Mar. 22, 2016) (finding that text messages constitute ESI and framing Rule 37(e) within three threshold questions).

26 *Cat3, LLC*, 164 F. Supp. 3d at 497–98 (finding that a showing of "bad faith" is required to apply sanction powers if Rule 37(e) is not applicable).

27 For further discussion on how recent amendments to Rule 37(e) set these new standards, see our September 2015 *White Paper* "Significant Changes to the Federal Rules of Civil Procedure Expected to Take Effect December 1, 2015: Practical Implications and What Litigators Need to Know" and our February 2018 *White Paper* "Courts Are Closely Following Amended Rule 37(e)'s Limits on Sanctions for Lost Electronically Stored Information."

28 *Steves and Sons, Inc. v. JELD–WEN, Inc.*, Civil Action No. 3:16–cv–545, 2018 WL 2023128, at *5 (E.D. Va. May 1, 2018) (finding that "[a] party's inability to describe the nature and contents of the spoliated evidence with some particularity might be a problem if, for instance, there was no showing that any documents ever existed that could have been lost or destroyed"); *see also Linlor v. Polson*, No. 1:17CV0013, 2017 WL 7310076, slip op. at 2 (E.D. Va. Dec. 6, 2017) (finding "no evidence that other recordings of the incident actually existed and were not preserved or that any additional recordings would provide significant new information. Therefore plaintiff's motion also fails to establish any significant prejudice from the loss of any other video recordings…."); *Eshelman v. Puma Biotechnology, Inc.*, 2017 WL 2483800, at *5 (E.D.N.C.) (stating that "the court must have some evidence regarding the particular nature of the missing ESI in order to evaluate the prejudice it is being requested to mitigate"). The requesting party bears the burden of establishing that "all elements of a claim for spoliation of evidence" have been satisfied and must also provide "plausible, concrete suggestions as to what the evidence might have been" in order to identify relevant ESI and how that evidence could be used. *See TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo*, No. 15-2121 (BJM), 2017 WL 1155743, at *1 (D.P.R. Mar. 27, 2017); *see also Snider v. Danfoss, LLC*, No. 15 CV 4748, 2017 WL 2973464, at *5–8 (N.D. Ill. July 12, 2017) (finding insufficient evidence "regarding the particular nature of the missing ESI").

29 *Matthew Enter., Inc. v. Chrysler Grp. LLC*, No. 13-cv-04236-BLF, 2016 WL 2957133, at *3–4 (N.D. Cal. May 23, 2016) (noting that the court may order corrective measures when parties fail "to take reasonable steps" to preserve data and that the plaintiff's "lackadaisical attitude toward document preservation" prejudiced Chrysler).

30 *GN NetCom, Inc. v. Plantronics, Inc.*, No. 12–1318–LPS, 2016 WL 3792833, at *8 (D. Del. July 12, 2016).

31 Fed. R. Civ. P. 37(e)(2). If prejudice exists, courts are permitted to impose "measures no greater than necessary to cure the prejudice." Fed. R. Civ. P. 37(e)(1); *see First Fin. Sec., Inc. v. Freedom Equity Grp., LLC*, No. 15–CV–1893–HRL, 2016 WL 5870218, at *4 (N.D. Cal. Oct. 7, 2016) (noting that the "remedy should fit the wrong" and accordingly imposing monetary and adverse inference instruction sanctions on the offending party); *see also Ronnie Van Zant, Inc. v. Pyle*, 270 F. Supp. 3d 656, 668–69 (S.D.N.Y. 2017) (finding an adverse inference sanction appropriate where the defendant failed to preserve the relevant nonparty's text messages within its control); *Hsueh v. NY State Dep't of Fin. Servs.*, No. 15 Civ. 3401 (PAC), 2017 WL 1194706, at *6 (S.D.N.Y. Mar. 31, 2017) (finding adverse inference as an appropriate remedy where the plaintiff failed to preserve a relevant recording and acted in bad faith).

32 *Brown Jordan Int'l*, 2016 WL 815827, at *36–37 (ordering adverse inference instruction sanctions after finding that the defendant acted with an intent to deprive by using his personal iPad to take hundreds of screenshots of corporate emails and then subsequently "losing" the tablet).

33 *Ronnie Van Zant, Inc.*, 270 F. Supp. 3d at 669 (finding that the nonparty's text messages were under the defendant's control and should have been preserved because: (i) the nonparty was contracted by the defendant and they worked closely together, (ii) the nonparty participated in the litigation by providing documents and taking a deposition, and (iii) the nonparty had a financial interest in the outcome of the litigation).

34 *Timms v. LZM, L.L.C.*, 657 Fed. Appx. 228, 231 (5th Cir. 2016).

35 *Roadrunner Transp. Servs. v. Tarwater*, 642 Fed. Appx. 759, 759–60 (9th Cir. 2016) (reasoning that because the "primary evidence of [the defendant's] alleged misappropriation and related misconduct" had been destroyed, a less severe sanction would not have properly cured the prejudice).