
UNITED STATES DISTRICT COURT FOR THE DISTRICT OF UTAH
CENTRAL DIVISION

OL PRIVATE COUNSEL, LLC, a Utah
limited liability company,

Plaintiff,

v.

EPHRAIM OLSON, an individual,

Defendant.

**MEMORANDUM DECISION AND
ORDER DENYING WITHOUT
PREJUDICE DEFENDANT'S MOTION
FOR SPOILIATION SANCTIONS
(DOC. NO. 200)
AND ORDERING OLPC TO PRODUCE
DATA COPY, PHONE, AND
PASSWORD**

Case No. 2:21-cv-00455

District Judge David Barlow

Magistrate Judge Daphne A. Oberg

In this action, Plaintiff OL Private Counsel, LLC (“OLPC”) alleges its former employee, Ephraim Olson,¹ misappropriated OLPC’s confidential client documents and shared them with his mother, Carolyn Olson, and/or her attorneys.² OLPC alleges Ephraim communicated with Timothy Akarapanich, a former employee of a related entity, through a messaging app called Telegram³ and Mr. Akarapanich, at Ephraim’s

¹ Because several of the parties and individuals involved share the same last name, the court refers to each by first name, for clarity.

² (See Ex. C to Notice of Removal, First Am. Compl., Doc. No. 2-2 at 35–52.)

³ (First Am. Compl. ¶ 24, Doc. No. 2-2 at 39.)

request, then accessed the documents and transmitted them to Ephraim.⁴ Mr. Akarapanich kept the alleged confidential documents on his phone, using the email application and cloud storage.⁵ OLPC claims Carolyn then used the misappropriated documents in litigation against Ephraim's father, Thomas Olson (OLPC's sole member/managing partner).⁶

Ephraim now moves for the sanction of dismissal against OLPC, alleging OLPC willfully facilitated the loss of key data from Mr. Akarapanich's telephone and cloud storage—and asserting this loss of information has interfered with Ephraim's ability to defend against OLPC's claims.⁷ Because the data may be restorable, the motion for sanctions is denied as premature. However, OLPC is ordered to produce the phone at issue, its password,⁸ and the data copy in its possession to third-party vendor Consilio for purposes of possible data restoration.

BACKGROUND

In his motion, Ephraim alleges that on October 2020, Mr. Akarapanich, phone in hand, met with OLPC to review the phone—and OLPC then proceeded to delete

⁴ (*See id.*) OLPC asserts claims for conversion, breach of contract, breach of fiduciary duty, and violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*, among others. (*Id.* ¶¶ 42–87.)

⁵ (Mot. for Spoliation Sanctions Re Tim Akarapanich Tel. and Cloud Data (“Mot.”) 1, Doc. No. 200 (sealed, unredacted version at docket number 202).)

⁶ (See First Am. Compl. ¶ 23, Doc. No. 2-2 at 39.)

⁷ (Mot. 2, Doc. No. 200.)

⁸ As set forth below, OLPC must make reasonable efforts to obtain the password.

information from the cloud storage on his phone.⁹ OLPC then gained ownership of the physical phone,¹⁰ allegedly without securing the phone’s password.¹¹ In 2023, Consilio, a third-party electronic storage information (“ESI”) vendor, was retained “to run forensics on the phone”¹² and, following the review of the phone, provided a detailed log of information it contained.¹³ Noting that the log lacked information regarding relevant applications, Ephraim asked OLPC and Consilio to provide information about whether the phone contained Facebook, Telegram, or Line applications.¹⁴ Consilio responded that:

The issue with this phone collection was the lack of having the device password. As a result, only a limited “logical” collection could be performed instead of a more comprehensive “Full File System” collection. This means that various data areas and application information could not be collected and thus were not available for reporting due to the examiner not having the password.¹⁵

⁹ (Mot. 1, Doc. No. 200.)

¹⁰ (Mot., Statement of Facts (“SOF”) ¶ 36, Doc. No. 200; OLPC’s Opp’n to Mot. (“Opp’n”) ¶ 14, Doc. No. 212 (sealed, unredacted version at docket number 214).)

¹¹ (Mot., SOF ¶ 54, Doc. No. 200; Opp’n ¶ 21, Doc. No. 212.)

¹² (Mot., SOF ¶ 49, Doc. No. 200.)

¹³ (*Id.* ¶ 50.)

¹⁴ (*Id.* ¶¶ 51–52.)

¹⁵ (*Id.* ¶ 52.)

Ephraim now asserts that relevant key data from the phone is unobtainable.¹⁶ Ephraim requests a spoliation sanction of dismissal, asserting that OLPC willfully facilitated the loss of important phone and cloud data from Mr. Akarapanich's phone.¹⁷

LEGAL STANDARDS

Spoliation is 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.”¹⁸ Spoliation only applies where the offending party has a duty to preserve the evidence.¹⁹ Therefore, before a court can impose sanctions for spoliation, a movant must first demonstrate the nonmovant had a duty to preserve evidence.²⁰

Rule 37(e) of the Federal Rules of Civil Procedure governs sanctions for spoliation of ESI. Pursuant to Rule 37(e), ESI spoliation occurs when 1) a party has a duty to preserve the evidence, 2) the ESI “is lost because a party failed to take reasonable steps to preserve it, and 3) it cannot be restored or replaced through additional discovery.”²¹ If spoliation has prejudiced the moving party, the court “may

¹⁶ (Mot. 1, Doc. No. 200.)

¹⁷ (*Id.* at 1–2.)

¹⁸ *Philips Elecs. N. Am. Corp. v. BC Tech.*, 773 F. Supp. 2d 1149, 1194–95 (D. Utah 2011).

¹⁹ *Id.* at 1195.

²⁰ *See id.* (“[S]poliation is both the destruction of evidence *and/or* the failure to preserve evidence.” (emphasis added)).

²¹ Fed. R. Civ. P. 37(e).

order measures no greater than necessary to cure the prejudice.”²² More severe sanctions, such as dismissal, may be imposed only if the nonmovant also “acted with the intent to deprive another party of the information’s use in the litigation.”²³

ANALYSIS

Ephraim contends OLPC willfully and intentionally spoliated the evidence contained in Mr. Akarapanich’s phone when it gained possession of the phone but failed to obtain the password, and deleted data from the cloud storage.²⁴ As discussed below, OLPC had a duty to preserve the information and data related to the phone. However, Ephraim’s request for sanctions is premature as it is unclear whether the information in question is lost completely or remains obtainable through other means.

1. Duty to Preserve

To assess spoliation, it is necessary to first consider whether OLPC had a duty to preserve evidence. The duty to preserve arises when a litigant knows, or should know, litigation is imminent.²⁵ This duty is the same regardless of whether the evidence

²² Fed. R. Civ. P. 37(e)(1).

²³ Fed. R. Civ. P. 37(e)(2).

²⁴ (Mot. 17, Doc. No. 200.)

²⁵ *Burlington N. & Santa Fe Ry. Co. v. Grant*, 505 F.3d 1013, 1032 (10th Cir. 2007); see also *Grabenstein v. Arrow Elecs., Inc.*, No. 10-cv-02348, 2012 U.S. Dist. LEXIS 56204, at *10 (D. Colo. Apr. 23, 2012) (unpublished) (explaining that “the duty to preserve relevant documents should require more than a mere possibility of litigation,” and therefore “the court’s decision must be guided by the facts of each case”) (internal quotation marks omitted).

consists of hard copy documents or ESI.²⁶ Evidence a party “knows or should know is relevant to imminent or ongoing litigation” must be preserved.²⁷ In evaluating when a duty to preserve has been triggered, courts “consider the extent to which a party was on notice that litigation was likely and that the information would be relevant.”²⁸

Ephraim argues OLPC had a duty to preserve evidence in its control (Mr. Akarapanich’s phone and cloud data) because OLPC was well on its way to pursuing litigation at the time it acquired access to the phone.²⁹ According to Ephraim, as of at least June 2020, OLPC knew Mr. Akarapanich had retained access to OLPC documents through an email application on his phone.³⁰ Then, in late October, OLPC had Mr. Akarapanich bring in the phone to start collecting evidence against Ephraim—all of which supports the notion that OLPC anticipated imminent litigation.³¹ Ephraim contends this was further confirmed when Mr. Akarapanich and Thomas communicated after OLPC obtained the phone, during which time Mr. Akarapanich indicated he wished

²⁶ See *Russell v. Nebo Sch. Dist.*, No. 2:16-cv-00273, 2018 U.S. Dist. LEXIS 166491, at *5–6 (D. Utah Sept. 26, 2018) (unpublished) (“[R]ule 37(e) does not alter existing federal law concerning when the duty to preserve attaches.”); *Philips Elecs. N. Am. Corp.*, 773 F. Supp. 2d at 1203 (noting the defendant had a duty “to take the necessary steps to ensure that relevant records—including ESI—were preserved when [the] litigation was reasonably anticipated or began”).

²⁷ *Russell*, 2018 U.S. Dist. LEXIS 166491, at *6.

²⁸ *Zybliski v. Douglas Cnty. Sch. Dist.*, 154 F. Supp. 3d 1146, 1163 (D. Colo. 2015) (quoting the advisory committee notes to Rule 37(e)).

²⁹ (Mot. 15, Doc. No. 200.)

³⁰ (*Id.* ¶¶ 16–18.)

³¹ (*Id.* at 15.)

to delete some personal items on his phone unrelated to “the case,”³² and Thomas later confirmed information relevant to OLPC had been deleted from the cloud storage.³³

OLPC does not dispute these basic underlying facts—namely that Mr. Akarapanich brought in the phone and wished to delete some personal items from the cloud—but contends that at the time of the phone data collection and deletion, it was not anticipating litigation.³⁴ Rather, OLPC asserts “it was investigating the events surrounding [Mr. Akarapanich’s] confession.”³⁵ OLPC also argues it had no duty to preserve the data and password of Mr. Akarapanich (a third party) because 1) both the password and cloud storage were in his control when he voluntarily chose to delete the stored data, and 2) OLPC did not think the password would be relevant data to preserve because OLPC copied “the entire contents of the phone and preserved the phone itself.”³⁶ In reply, Ephraim argues that once the ownership of the phone transferred to OLPC, the duty to preserve was extended to include preservation of the password and cloud data.³⁷ Ephraim is correct.

³² (Mot., SOF ¶ 34, Doc. No. 202 (sealed); Ex. 15 to Mot., Line Chat Hist. With T. (“Line Chat”), Doc. No. 202-15 at 7 (sealed).)

³³ (Mot. 15, Doc. No. 200.)

³⁴ (Opp’n ¶ 19, Doc. No. 212.) OLPC supports this argument by referring to Thomas Olson’s Rule 30(b)(6) deposition testimony, where he denied anticipating litigation at the time the phone was searched and copied. (*Id.*)

³⁵ (*Id.* at 15.)

³⁶ (*Id.*)

³⁷ (Reply in Support of Mot. for Spoliation Sanctions Re Tim Akarapanich Tel. and Cloud Data (“Reply”) 1, Doc. No. 240.)

OLPC's actions surrounding the phone indicate OLPC knew litigation was likely and the phone's data was relevant to it. The unauthorized access of confidential documents was a serious enough incident, and OLPC took swift steps to investigate and mitigate damage. For instance, upon accessing the phone, OLPC confirmed Mr. Akarapanich had unauthorized access to OLPC documents and took immediate steps to copy the phone.³⁸ Additionally, OLPC took sole possession of Mr. Akarapanich's phone when the copy was made,³⁹ in exchange for funds to purchase a new phone,⁴⁰ thus gaining sole and complete control of the phone.⁴¹ But OLPC did not stop there: it also deleted OLPC-related documents from Mr. Akarapanich's cloud storage data, ostensibly to prevent further unauthorized access.⁴² OLPC testified that rather than

³⁸ (Opp'n ¶¶ 10–11, Doc. No. 212.) In OLPC's Rule 30(b)(6) deposition, Thomas testified that when Mr. Akarapanich brought in the phone to help OLPC determine "how the documents got out" and made admissions, OLPC checked the phone "then and there" and, after seeing "the chats," took steps to copy the phone. (Ex. C to Opp'n, 30(b)(6) Dep. of OLPC through: Thomas Olson ("OLPC Dep.") 206:16–25, Doc. No. 212-3.)

³⁹ (OLPC Dep. 229:6–9, Doc. No. 212-3.)

⁴⁰ (See Mot., SOF ¶ 36, Doc. No. 200; Opp'n ¶¶ 13–14, Doc. No. 212; Ex. 19 to Mot., Handwritten Note, Doc. No. 200-19.)

⁴¹ (See Opp'n 3, Doc. No. 212.) OLPC explains it "preserved the actual phone in a sealed envelope," which was then provided to counsel and then given to Consilio. (*Id.*)

⁴² (See OLPC Dep. 232:23–25, 233:1–4, 10–12, Doc. No. 212-3 (OLPC "had somebody going through [Mr. Akarapanich's] cloud. Those [documents relating to OLPC] were deleted so there was not a second copy of it, and [OLPC] had the only original copy of anything deleted. Anything related to the firm, [OLPC] had a copy of that. . . . [H]e was with the IT people when they were clearing up his cloud on the stuff that related to [OLPC]").)

searching the rest of the phone once OLPC's documents were deleted off the cloud, Mr. Akarapanich offered to completely delete his cloud data himself.⁴³

The claim that OLPC did not anticipate litigation when it learned potentially confidential documents had been accessed by former employees is unconvincing—particularly where those documents pertained to the ongoing litigation (divorce proceedings) between Thomas and Carolyn.⁴⁴ At the very least, OLPC knew of the marital litigation at the time it accessed Mr. Akarapanich's phone, and the factual circumstances under which OLPC gained access to the phone also suggest imminent future litigation was reasonably foreseeable. There is no dispute the evidence was relevant. Accordingly, OLPC's duty to preserve the phone and cloud data was triggered at least as of October 2020.

2. Mr. Akarapanich's Password and Cloud Data

OLPC's argument that it had no duty to preserve Mr. Akarapanich's cloud data and password (even if it had a duty to preserve the phone), is unpersuasive. In support of this claim, OLPC relies on a decision in *Rains v. Westminster College*.⁴⁵ OLPC asserts that the court in *Rains* concluded the plaintiff failed to establish the

⁴³ (*Id.* at 200:13–25, 234:8–14.)

⁴⁴ (See First Am. Compl. ¶¶ 23, 30, Doc. No. 2-2 at 39 (referencing “the Marital Dispute”).)

⁴⁵ No. 2:20-cv-00520, 2023 U.S. Dist. LEXIS 64548 (D. Utah Apr. 11, 2023) (unpublished).

defendant had a duty to preserve evidence in the control of a third party.⁴⁶ According to OLPC, the same premise applies here: like the third party in *Rains*, where Mr. Akarapanich had control over the phone’s password, not OLPC, OLPC had no duty to preserve the password.⁴⁷

But *Rains* falls short of the mark. In *Rains*, the court assessed whether the defendant had control over lost or destroyed evidence.⁴⁸ Finding the plaintiff failed to argue or provide evidence that the defendant had possession or control of the information at any point, the court concluded the plaintiff had failed to show the defendant had a duty to preserve the information.⁴⁹ However, *Rains* does not address circumstances like this—where a party to the case gains control over evidence originally held by a third party. The “fundamental factor” in assessing the duty to preserve is whether “potential objects of evidence” are in “the party’s possession, custody, or control.”⁵⁰ “[C]ontrol comprehends not only possession but also the right, authority, or ability to obtain” the information.⁵¹

⁴⁶ (Opp’n 16, Doc. No. 212.)

⁴⁷ (*Id.* at 17.)

⁴⁸ *Rains*, 2023 U.S. Dist. LEXIS 64548, at * 9.

⁴⁹ *Id.*

⁵⁰ *Phillips v. Netblue, Inc.*, No. C-05-4401, 2007 U.S. Dist. LEXIS 67404, at * 6 (N.D. Cal. Jan. 22, 2007) (unpublished).

⁵¹ *Super Film of Am., Inc., v. UCB Films, Inc.*, 219 F.R.D. 649, 653 (D. Kan. 2004).

Unlike the defendant in *Rains*, OLPC had control and possession of Mr. Akarapanich's phone—it purchased the phone from him clearly for purposes of obtaining and controlling the data it contains.⁵² And it is undisputed that OLPC accessed the contents of the phone and cloud in Mr. Akarapanich's presence, to review, copy, and delete items from the cloud.⁵³ Once OLPC took physical possession of the phone, it was reasonable to expect it to also obtain the password from Mr. Akarapanich.⁵⁴ OLPC's own actions to secure the phone make clear that it knew this access would be important, if not vital. Without access to the phone's data, the ability to establish the timeline and manner of document access is greatly impeded. And without the password, the data cannot be fully accessed.⁵⁵ Because OLPC had access to and retained control over the phone, it had a duty to preserve the password (the means for accessing the data) because the password "is reasonably calculated to lead to the discovery of admissible evidence"⁵⁶ pertinent to both parties in this action. By failing to

⁵² (See Opp'n 3, Doc. No. 212 ("Immediately upon learning that Akarapanich had improperly accessed the law firm server and sent confidential information to Ephraim, OLPC took possession of Akarapanich's phone.").)

⁵³ (See Mot., SOF ¶¶ 37, Doc. No. 200; Opp'n ¶¶ 10–11, Doc. No. 212.)

⁵⁴ It is difficult to conceive of any reason for OLPC not to obtain and preserve the password—other than a desire to impede access to the phone's contents.

⁵⁵ (See Mot., SOF ¶¶ 51–52 (without a password, Consilio was unable to do a "Full File System" collection"); Opp'n ¶ 21, Doc. No. 212 (Consilio reports that without a password, it was unable to provide a "lay person list of applications on the phone").)

⁵⁶ *Marten Transp., Ltd. v. Plattform Adver., Inc.*, No. 14-cv-02464, 2016 U.S. Dist. LEXIS 15098, at *15 (D. Kan. Feb. 8, 2016) (unpublished).

preserve the means for accessing the data, OLPC effectively failed to preserve the data—the net effect is the same.

This is particularly true where the phone’s data was deleted from the cloud storage when OLPC took possession of the phone. Ephraim claims OLPC shirked its duty to preserve the evidence by deleting from the cloud storage evidence that is vital to OLPC’s claims and Ephraim’s ability to defend against them.⁵⁷ There is no question the cloud data has been deleted and it was deleted after the duty to preserve attached.⁵⁸ For instance, from a review of the record, it appears that OLPC obtained Mr. Akarapanich’s phone the day he first met with OLPC representatives.⁵⁹ Once in OLPC’s control, OLPC reviewed the phone and the cloud storage,⁶⁰ and cloud data was deleted (both by OLPC or Mr. Akarapanich) at some point during and after the initial

⁵⁷ (Mot. 18–19, Doc. No. 200.)

⁵⁸ In its opposition, OLPC contends Mr. Akarapanich himself deleted the cloud storage. (Opp’n 2, 17, Doc. No. 212.) But as evidenced by the statements from the Rule 30(b)(6) deposition and OLPC’s opposition, there is some disconnect as to who deleted what. (See OLPC Dep. 232:23–25, 233:1–4, 10–12, Doc. No. 212-3 (indicating that OLPC deleted OLPC-related documents); Opp’n ¶ 17, Doc. No. 212 (“Neither OLPC nor any other agents of or affiliates of OLPC deleted Akarapanich’s cloud storage that contained a backup copy of his phone. Akarapanich himself deleted the cloud copy so there could be no question of him again gaining access to OLPC’s confidential documents and information.”).) In any event, it’s undisputed that the cloud storage data was deleted, and after OLPC gained possession and control of the physical phone.

⁵⁹ (See OLPC Dep. 207:14–20 229:6–9, Doc. No. 212-3 (“[H]e provided [the phone] the day he came in. . . . I don’t think he was expecting to turn over his phone that day. . . . [H]e handed us the phone I believe that the day he came in, the cell phone IT people copied everything off there relating to the firm, and retained the phone. And he never retrieved the phone again.”).)

⁶⁰ (See *id.* at 206:16–25 (OLPC saw “the chats” and commenced copying the phone).)

meeting.⁶¹ OLPC knew Mr. Akarapanich wished to delete some of the cloud data, and OLPC does not purport to have objected to or hesitated when Mr. Akarapanich commenced deletion of the cloud data.⁶² Indeed, Thomas testified after OLPC “went through the cloud with [Mr. Akarapanich] and removed all the documents which were simply backed up at Ephraim’s request on his cloud account,” instead of OLPC “going through everything else,” Mr. Akarapanich said “‘I’ll just delete all my cloud’ and then he dealt with deleting the rest of his cloud account.”⁶³

OLPC argues that because the cloud data was simply a backup of the phone, and because OLPC has a separate copy of the phone’s data, there is no lost evidence, despite the deletion of the cloud data.⁶⁴ In other words, OLPC asserts that where the cloud data was “duplicative” of the phone’s data, all data deleted off of the cloud is still represented in OLPC’s copy of the phone.⁶⁵ But OLPC offers no evidence to support this assertion. And the data was deleted, with OLPC’s knowledge, at a time OLPC had a duty to preserve relevant information. In short, OLPC had a duty to preserve the

⁶¹ (See Line Chat, Doc. No. 202-15 at 6–7 (sealed).) The communications between Thomas and Mr. Akarapanich show they discussed when Mr. Akarapanich was initially going to come in, sometime between October 27 and 29, 2020; Thomas asked Mr. Akarapanich on October 30, 2020 if he could “come in again” the following day, October 31, 2020; and Mr. Akarapanich asked if he could come in earlier on October 31, 2020, to “delete some personal data like banking/credit card some messenger [sic] that does not involved with [sic] the case.” (*Id.*)

⁶² (See OLPC Dep. 234:2–4, 8–12, Doc. No. 212-3.)

⁶³ (*Id.*)

⁶⁴ (Opp’n 17, Doc. No. 212.)

⁶⁵ (*Id.*)

phone and its data, the cloud data, and the phone's password (as the access point for the data).

3. "Lost" Evidence and Sanctions

Turning to Ephraim's request for spoliation sanctions, Rule 37(e) dictates that evidence must be lost and irretrievable before a court can consider the appropriateness of sanctions.⁶⁶ As noted, Ephraim asserts OLPC breached its duty to preserve the evidence by failing to obtain the phone's password and by deleting the cloud data.⁶⁷ OLPC claims its actions in preserving a copy of and maintaining physical control of the phone prevented any loss of data (notwithstanding its failure to preserve access to the phone and the deletion of cloud data).⁶⁸

Under Rule 37, before imposing sanctions, the court must assess whether the ESI which OLPC should have preserved can "be restored or replaced through additional discovery."⁶⁹ At this juncture, the answer to that question is not apparent. It seems at least possible that further discovery may restore the evidence, in whole or part. For instance, both parties agree OLPC does not have the phone's password, creating an access problem.⁷⁰ OLPC argues Ephraim has failed to show the password has been

⁶⁶ See Fed. R. Civ. P. 37(e).

⁶⁷ (Mot. 17, Doc. No. 200.)

⁶⁸ (Opp'n 17, Doc. No. 212.)

⁶⁹ Fed. R. Civ. P. 37(e).

⁷⁰ (See Mot. ¶ 52, Doc. No. 200 (Consilio has indicated access to the "Full File System collection" on the phone, including "various data areas and application information," requires the phone's password); Opp'n ¶¶ 21–22, Doc. No. 212.)

lost and contends other discovery means could recover the password—or Ephraim could contact Mr. Akarapanich to obtain it.⁷¹ In the alternative, OLPC suggests the court could order OLPC to retrieve the password, and concedes that “of course, OLPC would comply.”⁷² In reply, Ephraim alleges he has unsuccessfully tried to reach Mr. Akarapanich,⁷³ and argues OLPC’s suggestion inappropriately places the burden on Ephraim to obtain the password.⁷⁴ What this dispute makes clear is that production of the password may cure the access problem such that the ESI which OLPC should have preserved may be restored.

There is no question that the burden of obtaining the password falls on OLPC. As noted above, OLPC should have preserved that information in the first place. Even under the most basic discovery principles, the burden is OLPC’s. Under Rule 34 of the Federal Rules of Civil Procedure, production of information outside a party’s actual possession may be required if the party has “any right or ability to influence the person in whose possession the documents lie.”⁷⁵ Again, OLPC purchased Mr. Akarapanich’s phone for purposes of controlling the data it contained. It is possible that OLPC has the

⁷¹ (Opp’n 20, Doc. No. 212.)

⁷² (*Id.* at 4.)

⁷³ (Reply 9, Doc. No. 240.)

⁷⁴ Ephraim cites to evidence showing Thomas and Mr. Akarapanich have been in contact during the course of this case. (*Id.* at 9 (citing to Line chat messages between Thomas and Mr. Akarapanich dated between May 2022 and July 2022); Line Chat, Doc. No. 202-22 at 1–3 (sealed).)

⁷⁵ *Super Film of Am.*, 219 F.R.D. at 651 (internal quotation marks omitted).

ability to influence or request Mr. Akarapanich to provide the phone's password, undoubtedly in his possession, to gain access to the phone. And there is a possibility that producing the password, with the phone, for further inspection may be sufficient to restore the ESI which OLPC should have preserved.

OLPC also claims it has a copy of the phone's data⁷⁶—which Ephraim says is “news” to him.⁷⁷ It is not apparent whether OLPC has disclosed the existence of this data copy. For example, Ephraim previously requested that OLPC “[p]roduce a copy of all files *copied* or deleted from Mr. Akarapanich's cell phone or computer . . . by OLPC.”⁷⁸ In response, OLPC claimed the request was “overly broad and unduly burdensome in that it seeks all files from a third-party's cell phone.”⁷⁹ But OLPC did not disclose whether it had a copy of the phone's data in its possession, noting only that it did not have a copy of Mr. Akarapanich's computer.⁸⁰ OLPC now asserts it has “run searches for relevant documents on *the copy of Akarapanich's phone*,”⁸¹ while citing

⁷⁶ (Opp'n ¶ 18, Doc. No. 212 (“OLPC did not delete anything from the phone, but rather preserved a copy.”); *id.* at 17 (“OLPC was careful to ensure a copy of the phone” was preserved.).)

⁷⁷ (Reply 9, Doc. No. 240.)

⁷⁸ (Mot., SOF ¶ 44, Doc. No. 200 (emphasis added); Ex. 23 to Mot., OLPC's Resps. to Sixth Set of Written Disc. (“OLPC's Resps.”) 9, Doc. No. 200-23.)

⁷⁹ (Mot., SOF ¶ 45, Doc. No. 200; OLPC's Resps. 10, Doc No. 200-23.)

⁸⁰ (Mot., SOF ¶ 45, Doc. No. 200; OLPC's Resps. 10, Doc No. 200-23.)

⁸¹ (Opp'n ¶ 20, Doc. No. 212 (emphasis added).)

discovery responses stating OLPC searched the *cell phone*, not its data copy.⁸² This discrepancy adds to the confusion. Moreover, it is unclear whether the data copy represents the entire contents of the phone or just OLPC-related documents. For example, in its Rule 30(b)(6) deposition, OLPC represented that it “took copies,”⁸³ but then clarified what “was copied off that phone” was “everything dealing with [OLPC].”⁸⁴ In other words, it is unclear what this data copy contains. However, there is a possibility that the copy, in combination with the phone and its password, may be sufficient to restore lost ESI, such that sanctions are unwarranted.

Ephraim asks that OLPC be ordered to produce the data copy of the phone to Consilio for inspection.⁸⁵ OLPC must also make reasonable efforts to obtain the phone’s password and must produce the phone (with the password)⁸⁶ and the phone’s data copy to Consilio for inspection. This is necessary to assess whether the lost ESI

⁸² (Ex. 24 to Mot., OLPC’s Resps. to Eighth Set of Written Disc. 6, Doc. No. 202-24 (sealed) (emphasis added).)

⁸³ (OLPC Dep. 206:23–24, Doc. No. 212-3.)

⁸⁴ (*Id.* at 207:20–21; *see also id.* at 198:22–25 (“At the time we received his phone . . . everything that was on there *that related to the firm* was copied. So all the stuff was copied off there.” (emphasis added)).)

⁸⁵ (Reply 9–10, Doc. No. 240.)

⁸⁶ It is unclear if the phone is still in Consilio’s possession, as explained in OLPC’s opposition, or if OLPC has possession of the phone. (See Opp’n 3, Doc. No. 212.) If the phone is no longer in Consilio’s possession, OLPC must again provide the phone to Consilio for inspection.

can be restored or replaced.⁸⁷ If the lost ESI is unable to be restored or replaced through this process, Ephraim may file a renewed motion for sanctions. At that point, it will be more apparent whether the evidence has been irretrievably lost.⁸⁸ At this juncture, however, Ephraim's motion for spoliation sanctions is premature and therefore denied without prejudice.⁸⁹

CONCLUSION

Ephraim's motion⁹⁰ is denied without prejudice. However, within twenty-one days of this order, OLPC is ordered to produce to Consilio (1) the phone, (2) the phone's password, and (3) the full data copy of the phone for further examination.

⁸⁷ See Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment ("Nothing in the rule limits the court's powers under Rule 16 and 26 to authorize additional discovery.").

⁸⁸ See Fed. R. Civ. P. 37(e) (If ESI is (1) "lost because a party failed to take reasonable steps to preserve it," and (2) "cannot be restored or replaced through additional discovery," the court can contemplate imposing varying levels of sanctions.).

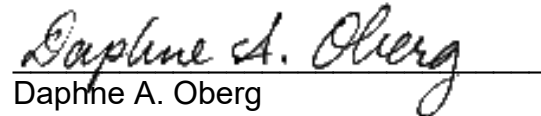
⁸⁹ Ephraim also requests the attorney fees incurred for bring this motion, as an additional sanction. (Mot. 23–24, Doc. No. 200.) His request for fees is denied as premature, where his request for sanctions is premature.

⁹⁰ (Mot., Doc. No. 200.)

Ephraim may file a renewed motion for sanctions if the ESI cannot be replaced or restored.

DATED this 3rd day of May, 2024.

BY THE COURT:



Daphne A. Oberg
United States Magistrate Judge