**3. A decision from the U.S. District Court for the District of Utah denying without prejudice a motion for spoliation sanctions where the plaintiff had taken possession of a former employee's phone without the passcode to access the phone but requiring the plaintiff to produce the phone and secure its passcode.**

In *OL Private Counsel, LLC v. Olson*, No. 2:21-cv-00455, 2024 WL 1973340 (D. Utah May 3, 2024), U.S. Magistrate Judge Daphne A. Oberg addressed whether the failure to preserve cell phone data, including the password to a cell phone, constituted spoliation requiring the imposition of sanctions.

In this action alleging that Defendant, a former employee of Plaintiff's, misappropriated Plaintiff's confidential client documents and shared them with a third party, Plaintiff alleged that Defendant communicated with Timothy Akarapanich, a former employee of a related entity's, through a messaging app called Telegram. *Id.* at *1. Defendant sought discovery of Akarapanich's mobile phone, but Plaintiff did not have the password for the phone and could not access its contents.

Defendant moved for the sanction of dismissal against Plaintiff, arguing that Plaintiff "willfully facilitated the loss of key data from Mr. Akarapanich's telephone and cloud storage." In his motion, Defendant claimed that Plaintiff knew Akarapanich had retained access to Plaintiff's documents through an email application on his phone, and Plaintiff met with Akarapanich in October 2020 to review the contents of the phone and to start collecting evidence against Defendant. *Id.* at *3. Defendant also claimed that during this meeting, Plaintiff took possession of the phone (without learning the phone's password) and deleted information from the cloud storage on the phone. Akarapanich later communicated with Plaintiff and said he wished to delete certain personal information from the phone. Plaintiff apparently deleted such data as well as other data related to Plaintiff.

In response to Defendant's motion, Plaintiff argued that when it met with Akarapanich in October 2020 to collect the phone data, it was not anticipating litigation but was merely "investigating the events surrounding" Akarapanich's taking of Plaintiff's confidential information. Plaintiff also argued that it had no duty to preserve Akarapanich's phone data and password as 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) Plaintiff did not think the password would be relevant data to preserve because Plaintiff copied "the entire contents of the phone and preserved the phone itself."

In 2023, an ESI vendor (Consilio) was retained to perform a forensic review of Akarapanich's phone, but the resulting log of information regarding the phone's content lacked information regarding relevant applications such as Facebook, Telegram, or Line. *Id.* at *2. Consilio reported that because it did not have the phone's password, it could not perform a comprehensive "Full File System" collection that included application information.

Magistrate Judge Oberg began her analysis by explaining that 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." *Id.* at *2. She noted that spoliation applies only

"where the offending party has a duty to preserve the evidence" and therefore requires the moving party to demonstrate that the nonmovant had a duty to preserve evidence.

Magistrate Judge Oberg further explained that Rule 37(e) governs sanctions for spoliation of ESI, which 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." She stated that if spoliation has prejudiced the moving party, the court "may order measures no greater than necessary to cure the prejudice" and severe sanctions like 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."

Turning to the merits of Defendants' motion, Magistrate Judge Oberg first concluded that Plaintiff had a duty to preserve Akarapanich's phone and associated cloud data as early as October 2020. She explained that a duty to preserve arises "when a litigant knows, or should know, litigation is imminent," and courts "consider the extent to which a party was on notice that litigation was likely and that the information would be relevant." Magistrate Judge Oberg agreed with Defendant that once the ownership of the phone transferred to Plaintiff, the duty to preserve was extended to include preservation of the phone's password and associated cloud data because Plaintiff "knew litigation was likely and the phone's data was relevant to it." Magistrate Judge Oberg relied on the facts that immediately after the October 2020 meeting, Plaintiff "took sole possession of Mr. Akarapanich's phone . . . thus gaining sole and complete control of the phone" and deleted documents related to Plaintiff from the phone.

Magistrate Judge Oberg rejected Plaintiff's claim that it did not anticipate litigation when it learned that potentially confidential documents had been accessed by former employees, concluding that "the factual circumstances under which [Plaintiff] gained access to the phone also suggest imminent future litigation was reasonably foreseeable." *Id.* at *4.

Magistrate Judge Oberg similarly rejected Plaintiff's reliance on a prior case, *Rains v. Westminster Coll.*, No. 2:20-CV-00520, 2023 WL 2894506 (D. Utah Apr. 11, 2023), in which the court had concluded that the plaintiff failed to show that the defendant had a duty to preserve information in the possession of a third party at the time it was lost. Magistrate Judge Oberg noted that Plaintiff 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 contain[ed]." And, once Plaintiff took physical possession of the phone, "it was reasonable to expect it to also obtain the password from Mr. Akarapanich" because "without the password, the data [could not] be fully accessed." Accordingly, she concluded that Plaintiff "had a duty to preserve the password (the means for accessing the data) because the password [was] reasonably calculated to lead to the discovery of admissible evidence."

Finally, Magistrate Judge Oberg rejected Plaintiff's argument that it could not spoliate the cloud data associated with Akarapanich's phone because it was "simply a backup of the phone" and "duplicative of the phone's data." *Id.* at *5. She noted that Plaintiff offered no evidence to support its assertion that the data was duplicative and reiterated that Plaintiff had a duty to preserve relevant information, including the phone and its data, the cloud data, and the phone's password (as the access point for the data).

Turning to Defendant's request for sanctions, Magistrate Judge Oberg explained that Rule 37(e) dictates that "evidence must be lost and irretrievable before a court can consider the appropriateness of sanctions," requiring an assessment of "whether the ESI which [Plaintiff] should have preserved can be restored or replaced through additional discovery." *Id.* at *6. She concluded that "the answer to that question is not apparent" because "production of the password may cure the access problem such that the ESI which [Plaintiff] should have preserved may be restored."

Although the parties disputed who should have the obligation to obtain the password, Magistrate Judge Oberg found there was "no question that the burden of obtaining the password f[ell] on" Plaintiff because Plaintiff "should have preserved that information in the first place." She noted that production of information outside a party's actual possession may be required pursuant to Rule 34 if the party has "any right or ability to influence the person in whose possession the documents lie," and she considered that Plaintiff may have had "the ability to influence or request Mr. Akarapanich to provide the phone's password, undoubtedly in his possession, to gain access to the phone."

Accordingly, Magistrate Judge Oberg denied Defendant's motion for sanctions without prejudice and ordered Plaintiff to produce to Consilio (1) Akarapanich's phone, (2) the phone's password, and (3) the full data copy of the phone for further examination.