**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF KANSAS**

**In re: CCA Recordings 2255 Litigation**,

**Petitioners,**

**v.** **Case No. 19-cv-2491-JAR-JPO**

**(This Document Relates to All Cases)**

**United States of America,**

**Respondent.**

---

**MEMORANDUM AND ORDER**

This matter is before the Court on petitioners' Motion for Spoliation Sanctions (Doc. 561). On April 28, 2021, the Court granted the government's Motion to Cancel the evidentiary hearing set for May 6 and 7, 2021, with this Memorandum and Order to follow addressing the issues raised in the motion to cancel and the motion for sanctions.[1] For the reasons discussed in detail below, the Court finds that petitioners' request for spoliation sanctions is not moot but denies the motion on the merits.

## I. Background

### *Procedural History*

Petitioners in this consolidated habeas matter allege that the government violated the Sixth Amendment by intentionally and unjustifiably becoming privy to their attorney-client communications. As a remedy, petitioners ask the Court to vacate their judgments with prejudice

[1] Docs. 894, 906.

to refiling or alternatively, to reduce their term of imprisonment by approximately 50% and vacate any term of supervised release.

On September 15, 2020, petitioners filed two motions for sanctions under Fed. R. Civ. P. 37 based on the government's: (1) violation of the Court's discovery orders pursuant to Rule 37(b)(2);[2] and (2) spoliation of electronically stored information ("ESI") that resided on its Audio Visual Personal Computer ("AVPC").[3] On October 15, 2020, the Court denied in most part petitioners' request for Rule 37(b)(2) sanctions, including their request for default judgment, but stated that it

> intend[ed] to take as established petitioners' claim that before each petitioner entered a plea, was convicted, or was sentenced, each member of the prosecution team became 'privy to' each recording listed in the petitioner's privilege log, either by watching or listening to them or by directly or indirectly obtaining information about them from someone who did.[4]

The Court explained that it intended to apply the sanction "with respect to any petitioner who establishes that he or she is entitled to an evidentiary hearing under 28 U.S.C. § 2255."[5]

In the same order, the Court set petitioners' motion for spoliation sanctions for an evidentiary hearing, without addressing the government's argument that petitioners had failed to satisfy the threshold elements of ESI spoliation under Rule 37(e).[6] The Court observed, however, that the request for spoliation sanctions "will likely be moot" in light of the Rule

[2] Doc. 560. This motion was precipitated by the government's Notice of Intent Not to Provide Further Discovery in these habeas proceedings. Doc. 540.

[3] Doc. 561.

[4] Doc. 587 at 13.

[5] *Id.* at 16.

[6] *Id.* at 15.

37(b)(2) sanction the Court intended to impose.[7] The evidentiary hearing on spoliation sanctions was to begin February 1, 2021, but was cancelled due to COVID-related restrictions.[8]

The Court proceeded to review the pending § 2255 motions to determine which motions survived the government's procedural and jurisdictional challenges. Highly summarized, between January 18 and March 3, 2021, the Court made the following rulings: First, the Court ruled that three petitioners in this consolidated litigation who proceeded to trial in their underlying criminal proceedings are entitled to evidentiary hearings on their audio recording Sixth Amendment claims. In so doing, the Court referenced its stated intent to enter the Rule 37(b)(2) privy-to sanction.[9] Second, the Court determined that the rule in *Tollett v. Henderson* procedurally barred petitioners who alleged pre-plea Sixth Amendment violations from advancing those claims.[10] The Court dismissed one petitioner's § 2255 motion on these grounds and certified the issue for appeal; thirty-nine petitioners have successfully moved the Court to stay dismissal of their claims pending the appeal of that case.[11] Third, the Court determined that approximately twenty petitioners lacked standing to advance their Sixth Amendment claims for various reasons, including: claims that alleged post-sentencing violations; claims where petitioners who had been deported challenged only their sentence; claims where petitioners challenging their sentence had been sentenced to the mandatory-minimum sentence; and claims involving binding pleas that were accepted by the court at the change-of plea-hearing.[12]

---

[7] *Id.* at 16.

[8] Doc. 650.

[9] Doc. 777 at 31.

[10] Doc. 730 (citing 411 U.S. 258 (1973)).

[11] Docs. 874, 922.

[12] Docs. 730, 784.

Over thirty § 2255 motions remain pending in which the petitioner asserts a Sixth Amendment claim that is not subject to dismissal under the above-mentioned orders. Pursuant to the rulings referenced above, these petitioners allege post-plea, pre-sentencing violations and thus lack standing to challenge their convictions but not their sentences.[13] The Court has not yet determined which, if any, of these petitioners' motions will proceed to evidentiary hearing.

***Black Hearing and Order***

The Court assumes the reader is familiar with its ruling in *United States v. Carter* ("*Black* Order") that precipitates the § 2255 motions before the Court.[14] That comprehensive opinion was intended to provide a record for future consideration of the many anticipated motions filed pursuant to § 2255 and is incorporated by reference herein. The Court does not restate the underlying facts and conclusions of law in detail but will provide excerpts from the record as needed to frame its discussion of the issues presently before it.

As discussed in the *Black* Order, after hearing evidence, the Court made extensive findings on the government's failure to preserve evidence, including with respect to the so-called AVPC hard drives at issue in this matter.[15] The AVPC was a desktop computer assigned to and under the control of Litigation Support Specialist Pauletta Boyd.[16] Boyd had downloaded the proprietary Pelco Media Player software on the AVPC that was required for United States Attorneys' Office for the District of Kansas ("USAO") personnel to view the CCA video

[13] *Id.*

[14] Case No. 16-20032-JAR, Doc. 758 (D. Kan. Aug. 13, 2019). As discussed in that Order, petitioners' Sixth Amendment claims stem from recordings of conversations and meetings with counsel while they were detained at Corrections Corporation of America ("CCA"). That facility has since been renamed CoreCivic. For convenience, the Court refers to CCA in this Order.

[15] *Black* Order at 23–49, 129–30.

[16] *Id.* at 34.

recordings.[17] The AVPC was the only computer on which USAO staff could view the video recordings obtained from CCA, and the Pelco software was loaded under Boyd's login and only she could directly access it.[18] Any metadata identifying who, when, and how the Pelco Media Player software was used to view the CCA videos would have resided on the two hard drives of the AVPC. On September 6, 2016, as part of a scheduled PC refresh project of computers used by the USAO, Systems Manager David Steeby testified that he "refreshed in place" the AVPC by reformatting its two hard drives and installing the Windows 10 operating system,[19] which wiped the hard drives.[20] And despite the Court's claw back order issued August 30, 2016, followed by a flurry of emails between Federal Public Defender ("FPD") and the USAO management team about the need to preserve the AVPC hard drives, no one at the USAO ever consulted either Boyd or Steeby to tell him not to refresh in place the AVPC computer.[21]

The FPD requested spoliation sanctions, arguing that the September 2016 upgrade to the operating systems used by the USAO destroyed ESI in the form of metadata stored on the AVPC that would have shown whether anyone viewed the video recordings that now form the basis of the majority of petitioners' Sixth Amendment claims in this consolidated matter.[22] All of the USAO attorneys and agents involved in petitioners' cases deny viewing the video recordings obtained from CCA.

---

[17] *Id.* at 35.

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id*. at 33–34.

[22] *See Black*, No. 16-20032-JAR, Doc. 747 at 31–33.

In support of their current motion for sanctions, petitioners submit the report of Tami Loehrs, dated April 20, 2020 ("Loehrs Report").[23] Loehrs, a forensic computer expert, previously testified in the *Black* case that the only reason to have two hard drives on a computer is to use one hard drive for the operating system and one to store data.[24] She testified that if the AVPC had one hard drive devoted to data and one to the operating system, the Pelco player and video recordings would have been stored on the data hard drive, and installation of Windows 10 on the operating system hard drive would not have compromised the Pelco player and video recordings.[25] The Court found that Loehrs credibly and persuasively opined that there was no reason for Steeby to install Windows 10 on both drives and risk overwriting data, unless the objective was to destroy the data. Nonetheless, Loehrs could not opine as to how much data, if any, was overwritten on the AVPC between the time it was reformatted and when it was taken out of service on November 7, 2016, about two months later. She did not conduct a forensic examination of the computer and could not opine that the data, including any logging information that may have existed, was completely lost.[26] Loehrs and Steeby both testified that a forensic evaluation of the AVPC's unallocated space would show how much data was overwritten.[27]

At the *Black* evidentiary hearing, the Court heard from Steeby and Loehrs on this issue. Counsel for the Special Master asked Steeby if there was "any way to get back the data that was on that AVPC on September 5th, 2016," to which Steeby responded, "I'm not a forensic expert;

[23] Doc. 561-1.

[24] *Black* Order at 35.

[25] *Id.* at 36.

[26] *Id.*

[27] *Id.*

however, I would be interested in—in looking at the unallocated space on that hard drive if I were asked to try to get the data back."[28] Loehrs, who is a computer forensics expert, further explained the concept of unallocated space on the hard drive and opined that data on a hard drive that has been reformatted is not necessarily unrecoverable.[29] When asked if "it [is] common to recover either partial or entirely intact files from unallocated space," Loehrs replied, "[d]o it every day."[30]

The Court ultimately denied the FPD's request for spoliation sanctions, concluding that "[t]here is no evidence that establishes whether metadata resided on the AVPC hard drive showing information about users' access to the P[elco] player other than [Litigation Support Specialist Pauletta] Boyd."[31] The Court explained, "there is no record that any party asked Loehrs to conduct a forensic analysis of the AVPC to determine whether logging data, if it exists, sought by the Special Master and the FPD could be restored."[32]

***Tami Loehrs Expert Report***

In the April 2020 Loehrs Report, Loehrs describes finding no evidence that the Pelco Media Player was ever installed or used from HD01 or HD02.[33] Loehrs concluded that, to the extent that the Pelco Media Player was ever installed and/or used on HD02, that data cannot be restored.[34] Based on her testing and research, it was Loehrs' opinion that "viewing the CCA videos with the Pelco Media Player would have left behind forensic evidence in numerous

[28] *Id.* at 131.

[29] *Id.*

[30] *Id.*

[31] *Id.* at 131–32.

[32] *Id.*

[33] Doc. 561-1 at 6.

[34] *Id.*

locations on the AVPC that should have been recoverable with forensic tools."[35] She went on to hypothesize, "[t]he fact that no forensic evidence of such activity was located in allocated or unallocated space on either HD01 or HD02 may indicate any of the following: the Pelco Player was not installed and/or used on either HD01 or HD02; the data was wiped using software created specifically for that purpose; or the data was overwritten by the continued use of the computer such as the creation of over 450,000 files between September 14 and November 7, 2016."[36] In addition, Loehrs states that she would have expected that use of the Pelco account to log in and view the CCA videos would have generated system log files, as described by the manufacturer.[37]

Loehrs describes doing initial testing with Pelco Media Player software version 1.9.5.1, chosen because it was in existence when the Pelco Media Player was used with the AVPC in 2016.[38] She details the installation of this software onto a test machine running Windows 7, which was the operating system in use on the AVPC prior to the upgrade.[39] She then explains that "[a]lthough [she] was unable to use the Pelco Media Player on the test computer, [she] forensically analyzed the computer to identify artifacts created by installing the software."[40] Loehrs went on to discuss her conclusion that to "better understand how the Pelco Media Player would have functioned for Ms. Boyd when she viewed CCA videos and identify what sort of

[35] *Id.*

[36] *Id.*

[37] *Id.* at 6–7.

[38] *Id.* at 7.

[39] *Id.*

[40] *Id.* at 8.

forensic artifacts it would have left behind as a result of that activity," Loehrs needed additional information, "including the version of the Pelco Media Player used by Ms. Boyd in 2016."[41] Loehrs stated that because the Pelco Media Player is a web browser plugin,

> certain forensic artifacts would have been left behind within the Internet history on the AVPC prior to the operating system upgrade. That internet history should have existed in the unallocated space after the formatting and the upgrade, had the hard drives not been wiped or otherwise overwritten. Based on Pelco's website, there should be websites with URLs following the format of the camera's IP address followed by "/index_admin.html" if someone had logged into Pelco to view cameras and/or videos. I ran searches for URLs following that format in allocated and unallocated space but located no forensic evidence of such activity.[42]

On March 10, 2020, Loehrs received a DVD with the DX8100 Client software purported to be the version of the software installed on the AVPC.[43] Loehrs searched the Pelco website and learned that the DX8100 client software required a user to download and install Control Point in order to function on a computer running the Windows 7 operating system.[44] Loehrs installed the DX8100 client software onto a Windows 7 test computer and verified that it did not function with the additional Control Point software.[45] She then downloaded the Control Point software onto the computer and was able to run the DX8100 client software.[46] Loehrs then "forensically analyzed the Windows 7 test computer to identify artifacts created by installing both DX8100 and Control Point software applications."[47] Her analysis revealed the software to

---

[41] *Id.* at 7.

[42] *Id.* at 8.

[43] The government states that the disc was used by Boyd to install the DX8100 software originally. Doc. 571 at 3.

[44] Doc. 561-1 at 8.

[45] *Id.*

[46] *Id.*

[47] *Id.*

be "very similar" to the Pelco Media Player software previously analyzed, and thus the forensic searches previously run for "pelco" should have brought up artifacts for all three software applications.

Loehrs searched the unallocated and allocated space of both hard drives and was unable to recover from either any data associated with the installation or use of the DX8100 software the government says it installed to view the CCA video.[48] She further reports that between September 14, 2016 and October 18, 2016, more than 365,000 files and folders were created on HD01, thereby overriding data in unallocated spaces.[49] Further, on November 3, 2016, Steeby stored new data on HD02.[50] Loehrs' examination confirmed that of the two AVPC hard drives, only HD02 had received installation of Windows 10 on September 6, 2016.[51] Loehrs found no forensic evidence that any operating system had ever been installed on HD01, meaning the hard drive was used for data storage only.[52] Loehrs noted this was contrary to the testimony of Steeby that both AVPC hard drives were upgraded to Windows 10 on September 6, 2016.[53]

***DOJ Evidence Processing Report***

Petitioners also attach to their motion the Evidence Processing Report prepared by the Department of Justice ("DOJ") Computer Crime and Intellectual Property Section/Cybercrime Lab, dated June 9, 2020 ("DOJ Report").[54] The DOJ report states that the Cybercrime Lab reviewed the Loehrs Report and found some omissions and incorrect conclusions, including

[48] *Id.* at 18–22 (discussing HD01); 23–32 (discussing HD02).

[49] *Id.* at 3–4.

[50] *Id.* at 5.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] Doc. 561-2

Loehrs' report that "over 80,000 files were created on HD02, thereby overwriting data in unallocated space potentially causing a significant loss of data that existed prior to the operating system being upgraded on September 6, 2016."[55] The DOJ Report concedes that all ESI residing on HD02 was permanently and irretrievably destroyed on September 6, 2016, during the system upgrade.[56] Specifically, because that hard drive was a solid state drive, the execution of the trim command during the reformatting process resulted in all the data on the drive being completely cleared.[57]

***Declaration of Glenn Shrieves***

As noted, Loehrs opined in *Black* that there was no reason for Steeby to reformat both HD01 and HD02 to install Windows 10 on the AVPC and risk overwriting data unless the objective was to destroy the data.[58] In its response to petitioners' spoliation motion, the government submits the Declaration of Glenn Shrieves, the Office Automation Assistant Director for the Executive Office of the United States Attorneys, dated September 24, 2020.[59] As described by Shrieves, the reformatting of all hard drives in a computer upgraded in place was a standard part of the procedure:

> To upgrade an existing computer during the 2016 PC Refresh project, the systems manager had to download and install a BIOS update on the existing computer and then reboot the computer to the network instead of to the hard drive. *Once the computer rebooted to the network, the upgrade process was completely automatic. This automated process included reformatting all hard drives in the computer, regardless of the number of hard drives in the computer*. Office Automation's standard practice is to reformat all hard drives when reimaging or when a new OS is installed.

[55] *Id.* at 5 (citing Loehrs Report at 4).

[56] *Id.*

[57] *Id.*

[58] *Black* Order at 36.

[59] Doc. 571-1.

> Reformatting identifies any deficiencies and removes any corrupted sectors in the hard drive creating new partitions to store data.[60]

Shrieves goes on to explain,

> Reformatting of all the hard drives in the computer during the in-place upgrade was standard operating procedure. An individual U.S. Attorney's Office and systems manager had no role in that decision. The automated in-place upgrade process was uniform, mandatory, and applied across all U.S. Attorney's Offices. If the Systems Manager in the District of Kansas followed the procedures in Appendix A07 for the in-place upgrade of existing equipment during the 2016 PC Refresh, then the systems manager played no role in how the upgrade from Windows 7 to Windows 10 was accomplished.[61]

## II. Discussion

The government opposes petitioners' motion for sanctions on two grounds: (1) no petitioner can satisfy the threshold elements of spoliation, specifically that relevant ESI was lost; and (2) the ESI was not lost as a result of any bad faith intent, but instead was a regrettable failure of communication. The government renews these arguments in its motion to cancel the spoliation hearing, with the additional ground that petitioners' motion is moot because the Court intends to impose an essentially identical sanction under Rule 37(b)(2). Petitioners respond that their motion is not moot because it informs the remedy sought in all the cases and both bolsters and offers alternative grounds for the Court to impose the sanction on the privy-to element of their Sixth Amendment claims. Petitioners also argue that they have demonstrated the requisite intent to deprive and, as a result, they need not establish actual relevance. The Court first addresses the standards under Fed. R. Civ. P. 37(e), then addresses the mootness argument followed by analysis of the merits.

[60] *Id.* ¶ 5 (emphasis added).

[61] *Id.* ¶ 6.

### A. Rule 37(e)

The seminal case of *Zubulake v. UBS Warburg LLC* defines spoliation 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."[62] In the case of ESI, Rule 37(e) governs and provides two tracks for spoliation sanctions:

> (e) If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.[63]

The burden of proof by a preponderance of the evidence is on "[t]he party seeking sanctions based on the spoliation of evidence."[64]

The sanction requested in petitioners' motion—an adverse inference/presumption that each member of the relevant prosecution team intentionally became privy to the video recordings listed in petitioners' privilege logs—falls under subsection (e)(2). Before reaching the sanctions

---

[62] 229 F.R.D. 422, 430 (S.D.N.Y. 2004) (quoting *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999)).

[63] Fed. R. Civ. P. 37(e) (effective Dec. 1, 2015).

[64] *See Turner v. United States*, 736 F.3d 274, 282 (4th Cir. 2013).

provision of subsection (e)(2), however, the Court must find that four prerequisites are met: (1) ESI was lost; (2) a party had a duty to preserve the lost ESI; (3) the party failed to take reasonable steps to discharge its duty; and (4) the lost ESI cannot be restored or replaced.[65] Once these requirements are met, the Court may go on to determine whether there has been a requisite showing of bad-faith intent necessary to impose the sanctions requested by petitioners under subsection (e)(2).[66]

Subsection (e)(1)—loss and prejudice— informs the application of subsection (e)(2)—loss and intent to deprive. Rule 37(e)(1) provides that, when the court finds that a party suffered prejudice from the loss of ESI that another party had a duty to preserve but failed to take reasonable steps to preserve, and the ESI is not otherwise available, then the court "may order measures no greater than necessary to cure the prejudice." "Spoliation of evidence causes prejudice when, as a result of the spoliation, the party claiming spoliation cannot present 'evidence essential to the underlying claim.'"[67]

Pursuant to Rule 37(e)(2), the court may impose more severe sanctions than those available under subsection (e)(1) if the court finds that "the party acted with the intent to deprive another party of the information's use in the litigation."[68] "Negligent or even grossly negligent behavior" does not suffice.[69] Instead, the ESI must be unavailable due to "a party's intentional loss or destruction of [it] to prevent its use in litigation," because this is the conduct that "gives

---

[65] Fed. R. Civ. P. 37(e); *Stovall v. Brykan Legends, LLC*, No. 17-2412-JWL-JPO, 2019 WL 480559, at *2 (D. Kan. Feb. 7, 2019).

[66] *Stovall*, 2019 WL 480559, at *2.

[67] *Brittney Gobble Photography, LLC v. Sinclair Broad. Grp., Inc.*, No. SAG-18-3403, 2020 WL 1809191, at *4 (D. Md. Apr. 9, 2020) (quoting *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 522–23 (D. Md. 2010)).

[68] Fed. R. Civ. P. 37(e)(2).

[69] Fed. R. Civ. P. 37(e)(2) advisory committee's note to 2015 amendment.

rise to a reasonable inference that the evidence was unfavorable to the party responsible for [its] loss or destruction."[70] Upon such finding, the court may impose the sanctions listed in subsection (e)(2), regardless of whether there is prejudice.[71]

**B. Mootness**

Citing *Black's Law Dictionary*, the government argues that petitioners' motion for spoliation sanctions is moot because it "ha[s] no practical significance."[72] The government urges that the Court's intent to impose an essentially identical sanction under Rule 37(b)(2) renders petitioners' request for spoliation sanctions moot.

Petitioners offer two reasons why their spoliation motion is not moot. First, petitioners argue that the spoliation issue informs the remedy question in all cases, including the three audio claim cases set for evidentiary hearing. The Court agrees in part. As this Court discussed in the *Black* Order, petitioners may argue that the government's discovery misconduct, including the circumstances surrounding the failure to preserve the AVPC hard drives, is a factor for the Court to consider in fashioning a remedy in cases where the Court determines a Sixth Amendment violation has occurred.[73] However, the issue of an appropriate remedy is both premature and beyond the scope of the discrete discovery relief sought in the motion for spoliation sanctions.

Second, petitioners argue that given the government's position that the existing record before the Court is insufficient to warrant the taken-as-established privy to element under Rule 37(b)(2), proceeding on the request for spoliation sanctions may both bolster the Court's existing

---

[70] *Id.*

[71] *Id.* ("Subdivision (e)(2) does not include a requirement that the court find prejudice to the party deprived of the information.").

[72] Doc. 894 at 7.

[73] *Black* Order at 7.

Rule 37(b)(2) analysis or provide an alternative basis for entering the privy-to adverse inference. The Court agrees. Although the requested spoliation sanction mirrors the sanction that the Court intends to impose under Rule 37(b)(2), the grounds for the sanction are alternative and distinct. Petitioners' pending motion for spoliation sanctions may provide the Court with alternative or additional grounds for its ruling and does not render the motion—which petitioners have not withdrawn—moot.

Moreover, the Court agrees that deciding the motion for spoliation sanctions is appropriate in this case. The government has previously asserted that the Court cannot treat its factual findings in the *Black* Order as binding on the government while at the same time, the government cites to, supplements, and explains evidence and testimony from *Black* in opposing the motion for spoliation motion. Given the focus on the government's conduct with respect to the AVPC hard drives in the *Black* investigation and Order, and the government's apparent intent to challenge the Court's Rule 37(b)(2) finding on appeal, it is critical to ensure the record is both accurate and complete. Certainly, under the government's cited standard, such a ruling has "practical significance."[74] As discussed below, however, that does not mean that an evidentiary hearing is required.

### C. Foundational Requirements/Existence of Relevant ESI

The first threshold finding required before reaching the issue of sanctions is that ESI was lost. The government argues that to have a viable spoliation claim, petitioners must establish that *relevant* ESI—logging metadata relevant to their claim that a USAO employee or a law enforcement official watched one or more video recordings of meetings with legal counsel—was

[74] *See Abajue v. Holder*, 453 F. App'x 853, 855 (10th Cir. 2012) ("A case is moot when it is impossible for the court to grant any effectual relief whatever to a prevailing party.") (quoting *Off. of Thrift Supervision v. Overland Park Fin. Corp.*, 236 F.3d 1246, 1254 (10th Cir. 2001)).

lost through the government's actions. The government argues that petitioners have been on clear notice of the need to make such a showing since August 13, 2019, when the Court denied the FPD's request for spoliation sanctions in the *Black* Order. It argues that because petitioners have again failed to show that any relevant metadata would have been created if anyone viewed the videos, they therefore have failed to show that any relevant data was lost in September 2016 when the AVPC's hard drives were reformatted for purposes of installing a new operating system as part of a regularly-scheduled DOJ-wide upgrade. Instead, the government contends, the Loehrs Report offers only assertions about certain ESI that is created during the installation—not operation—of the Pelco viewing software and generalized conclusory statements that ESI of some sort is created by operation of the viewing software. The government concludes that the FPD's failure to provide the evidence the Court said it was lacking in *Black* is fatal to petitioners' motion for spoliation sanctions, and therefore no hearing is warranted. It asks the Court to deny petitioners' motion for the same reason it denied the FPD's motion in *Black*: there is no evidence that establishes whether metadata resided on the AVPC hard drive showing information about users' access to the Pelco Media Player other than Boyd.

Petitioners respond that they do not need to show that any ESI on the AVPC hard drives that was lost in September 2016 was actually relevant to their cases. They argue that the plain language of Rule 37(e)(2) contains no actual relevance requirement and that the Court should not read one into it. Because Rule 37(e)(2) is based "on the premise that a party's intentional . . . destruction of evidence to prevent its use in litigation gives rise to a reasonable inference that the evidence was unfavorable to" that party, once a court determines a party acted with the requisite intent to deprive, this finding triggers both "an inference that that lost information was

unfavorable to" the party and "an inference that the opposing party was prejudiced."[75] In other words, they argue, Rule 37(e)(2)'s intent element renders proof of prejudice superfluous because prejudice is presumed; and under that same rationale, so too is relevance because a party cannot be prejudiced by the loss of ESI in litigation if that ESI is irrelevant to the moving party's claims or defenses. Thus, petitioners urge, the dispositive question is not *what* ESI resided on the AVPC's hard drives, but *why* the government destroyed that ESI. If the government did so with the requisite intent to deprive another party of the ESI's use in litigation, they argue it does not matter whether petitioners can show the ESI was actually incriminating. Instead, it matters that the government believed that it was, and that it acted in bad faith based on that belief.

Petitioners seek sanctions against the government based on the loss of ESI that resided on the AVPC used by Boyd. Notably, they do not argue for spoliation based upon the loss of logging metadata specifically. There does not seem to be any dispute that ESI on the AVPC existed; the question is whether the particular logging metadata relevant to petitioners' Sixth Amendment video claims existed. But by losing any and all ESI, petitioners do not claim that they lost the ability to determine if that metadata existed at all.

As the government stresses, unlike with the testing of the Pelco Media Player software version 1.9.5.1, Loehrs did not identify any barriers to the actual use of the DX8100, and makes no mention that she used the DX8100 to view any video recordings or did any analysis to identify any metadata created thereby. The government argues that it is clear from the Loehrs Report that at the time of her testing using the DX8100 client software, she had a test machine running the same operating software as was in use on the AVPC in 2016, Windows 7, and was able to install and operate the DX8100 software once she followed the advice of the Pelco

[75] Fed. R. Civ. P. 37(e)(2) advisory committee's note to 2015 amendment.

website and installed Control Point.[76] In addition, at the time of Loehrs' testing, the FPD was in possession of the videos of the attorney-client meeting rooms at CCA. Accordingly, the government argues, the FPD and its expert had all of the components necessary to conduct forensic testing to determine whether logging metadata was created by the viewing of videos, and notice that it needed to do so from the Court's ruling in *Black*. Yet, inexplicably, the Loehrs Report is silent on that point.

The Court agrees that petitioners have failed to present the information they were advised was lacking in *Black*. Petitioners do not dispute—or even address—Loehrs' failure to conduct tests to determine whether the logging metadata ESI existed except to note that the government did not, either. Instead, they rely on the language of Rule 37(e)(2), which equates relevance with prejudice. But relevance in the context of a Rule 37(e) threshold determination is made in a different context as that in Rule 37(e)(2)—before the Court reaches the why at issue in the sanctions provision of subsection (e)(2), it must determine whether and what ESI was lost. In addition to the threshold requirements under Rule 37(e), there is the "obvious" requirement that "the evidence must have existed."[77] "The threshold issue in any motion for spoliation is that the items purportedly destroyed or lost actually existed."[78] "A successful claim for spoliation of evidence cannot be premised on mere speculation on the existence of such evidence."[79]

Here, petitioners claim that they were deprived of the use of ESI from the AVPC that would have shown if and when anyone viewed the video recordings at issue in petitioners' cases

---

[76] Doc. 561-1 at 8.

[77] *Ottoson v. SMBC Leasing & Fin., Inc.*, 268 F. Supp. 3d 570, 581 (S.D.N.Y. 2017) (quoting *Stephen v. Hanley*, No. 03-cv-6226, 2009 WL 1437613, at *2 (E.D.N.Y. May 20, 2009)).

[78] *Brittney Gobble Photography, LLC v. Sinclair Broad. Grp., Inc.*, No. SAG-18-3403, 2020 WL 1809191, at *5 (D. Md. Apr. 9, 2020) (quoting *Ozeki v. Prince George's Cty., Md.*, No. DKC-13-0168 (CBD), 2014 WL 1429183, at *2 (D. Md. Apr. 11, 2014)).

[79] *Id.* (quoting *Wimbush v. Matera*, No. SAG-11-1916, 2014 WL 7239891, at *11 (D. Md. Dec. 17, 2014)).

by using the AVPC. Indeed, the sanction they request seeks an adverse inference that each member of the prosecution team intentionally became privy to the video recordings listed in petitioners' privilege logs. The focus on whether or why unallocated space was overwritten, even accepted as true, is not germane to the threshold question before the Court, as it presupposes that the logging metadata actually existed in the first place prior to being destroyed on September 6, 2016. If there is no evidence that logging metadata ever existed, it could not have been intentionally destroyed to deprive petitioners of its use, and there can be no spoliation as it relates to that specific ESI relevant to petitioners' claims. Both petitioners' and Loehrs' speculation that logging metadata should have existed remains just that—speculation.

Absent any evidence that such ESI existed and was destroyed, the Court need not engage in a substantive spoliation analysis.[80] Petitioners' shortfall on this threshold legal determination compels the Court to deny the motion on the parties' submissions, without further hearing.

**IT IS THEREFORE ORDERED BY THE COURT** that petitioners' Motion for Spoliation Sanctions (Doc. 561) is **denied**.

**IT IS SO ORDERED.**

Dated: June 1, 2021

S/ Julie A. Robinson
JULIE A. ROBINSON
CHIEF UNITED STATES DISTRICT JUDGE

[80] *See Bragg v. Sw. Health Syst., Inc.*, No. 18-cv-00763-MSK-NRN, 2020 WL 3963714, at *6 (D. Colo. July 13, 2020) (citing *Zbylski v. Douglas Cty. Sch. Dist.*, 154 F. Supp. 3d 1146, 1160 (D. Colo. 2015) ("Courts have found, and this court agrees, that a party seeking spoliation sanction must offer some evidence that relevant documents have been destroyed.")).