# In the United States Court of Federal Claims

No. 15-945C
(Filed: April 23, 2019)
(Re-Filed: May 10, 2019)[1]

* * * * * * * * * * * * * * * * * * * * * * * * * * *

4DD HOLDINGS, LLC, and
T4 DATA GROUP, LLC,

*Plaintiffs*,

v.

THE UNITED STATES,

*Defendant*,

and

IMMIX TECHNOLOGY, INC.,

*Third-Party*.

* * * * * * * * * * * * * * * * * * * * * * * * * * *

Contracts; partial motion to dismiss for lack of subject matter jurisdiction; motion for sanctions; RCFC 12(b)(1); RCFC 37(e); 28 U.S.C. § 1498(b) (2012); authorization or consent; spoliation; electronically stored information

*Edward H. Meyers*, Washington, DC, for plaintiffs, with whom were *Robert B. Gilmore* and *Philip J. O'Beirne*.

*John J. Todor*, Senior Trial Counsel, United States Department of Justice, Civil Division, Commercial Litigation Branch, Washington, DC, with whom were *Joseph H. Hunt*, Assistant Attorney General, *Robert E. Kirschman, Jr.*, Director, *Elizabeth M. Hosford*, Assistant Director, for defendant.

---

[1] This opinion was originally issued under seal to permit the parties an opportunity to propose redactions on or before May 7, 2019. The government filed a response on May 7, 2019, representing that "it has conferred with counsel for plaintiffs and does not propose any redactions to the April 23, 2019 opinion." ECF No. 183. We thus reissue this opinion unredacted.

*Sara M. Lord*, Washington, DC, for third-party defendant.

OPINION

BRUGGINK, *Judge.*

Plaintiffs, 4DD Holdings, LLC and T4 Data Group, LLC (collectively, "4DD"), filed a claim for copyright infringement in August 2015, alleging that the United States infringed plaintiffs' copyright in its data federation[2] software. 4DD claims that the government, acting through its contractors, infringed on 4DD's copyright by copying[3] 4DD's software and installing the software in excess of the purchased license.

Defendant filed a motion to partially dismiss plaintiffs' claim in June 2016. The government argues that the court does not have subject matter jurisdiction over the claim as it relates to alleged infringement by the agency's contractor Systems Made Simple, Inc. ("SMS") when SMS was working with 4DD's copyrighted software in SMS labs. The court stayed the motion to allow for discovery and lifted the stay in December 2018. The motion is fully briefed, and we held oral argument on April 9, 2019. Because plaintiffs have established that the government authorized and consented to its contractor's use of TETRA in SMS labs, we deny defendant's motion to dismiss.

On November 21, 2018, plaintiffs filed a motion for sanctions against the government for the spoliation of evidence. That motion also is fully briefed, and we held oral argument on plaintiffs' motion on April 9, 2019, as well. Because we find that the government destroyed relevant evidence that it had a duty to preserve, we grant plaintiffs' motion for sanctions.

---

[2] Data federation "refers to the systems and processes that permit disparate data sources to be combined into a single source of data." Def.'s Mot to Dismiss 2. Where databases are concerned, data federation permits information from multiple databases to be combined without creating a new database in the process. *Id.*

[3] The parties use the terms copying and cloning interchangeably when referring to an action that allegedly infringed on 4DD's copyright. We use the same terms throughout to describe the allegedly infringing activity. We do not draw a conclusion regarding whether the agency's actions constitute copyright infringement.

## BACKGROUND[4]

When providing healthcare to servicemembers, veterans, and their families, the Department of Defense ("DoD") and Department of Veterans Affairs ("VA") historically have been unable to share healthcare records among data systems. In 2011, DoD and VA committed to finding a data federation solution that would allow the agencies to share health records. The effort was coined the integrated Electronic Health Record ("iEHR") and would be developed by the Interagency Program Office ("IPO"). After a few years of working together, DoD and VA agreed to develop their own solutions to data federation. The Defense Medical Information Exchange ("DMIX") project emerged in 2013 as DoD's effort to develop interoperability among the systems. IPO supervised the DMIX project with assistance from DoD's Defense Health Agency ("DHA"). The Chief Engineer on the DMIX project was David Calvin.

The configuration and testing of data federation software for the DMIX project would be carried out by the agency's Systems Integration and Engineering Support contractor, SMS. SMS performed its work through task orders issued under an indefinite delivery indefinite quantity contract, the Chief Information Officer – Solutions and Partners 3 contract. David Calvin was also the agency's Contracting Officer's Representative on the SMS contract.

Before the agency licensed 4DD's software, SMS prepared to test and configure data federation software. The agency had planned to develop a software solution in the agency's Development Test Center ("DTC").[5] But the DTC fell behind schedule and the agency provided more resources to SMS so that SMS could perform some of its DMIX project work in its own labs. Throughout the course of its work, SMS performed its duties both in

[4] The background section is drawn from the parties' briefing on both motions and the appendices attached to the briefing.

[5] This center housed computer servers and supported various projects, including the DMIX project. Programmers, including SMS employees, used remote access through a Virtual Private Network or similar connection to work on the DTC servers. The DMIX project on DTC servers was housed in nine data environments divided into two areas, including DotCOM environments and DotMIL environments that were more secure.

its own labs and by remote access to the DTC. Furthermore, the agency repeatedly required SMS to perform work on the DMIX project using 4DD's copyrighted software in the contractor's own labs. *E.g.*, Pls.' Mot. Exs. E, F, G, X.

The first recorded SMS installation of 4DD's software in the SMS labs occurred in August 2013, before the agency purchased a license to use 4DD's software. 4DD and SMS apparently had agreed to a limited license to allow SMS to do preliminary work on the DMIX project prior to the agency licensing 4DD's products.

Following an Analysis of Alternatives and a fly-off competition, the agency chose to license two of 4DD's copyrighted software products: TETRA Healthcare Federator and TETRA Enterprise Studio. 4DD's software hopefully would provide the ability to seamlessly connect data across legacy systems.

Although plaintiffs' claim includes copyright infringement of both products, the present motions discuss only TETRA Healthcare Federator, referred to as TETRA. TETRA is a package of server components that provides data federation capability, allowing medical records to be transferred and viewed between systems. TETRA runs in the background on a computer server. A computer server may have varying numbers of central processing unit cores; anywhere from one to several dozen cores. Thus, TETRA server components are licensed per core to account for numbers of cores on different devices. In other words, the number of cores the user should license depends on the number and type of machines on which the user plans to install TETRA.[6] The agency purchased a TETRA license from 4DD's authorized reseller ImmixTechnology, Inc. ("Immix") for 64 cores.

Immix and the agency also incorporated an End User License Agreement ("EULA") into their contract. The EULA provides that TETRA could be used "solely for the purpose of supporting your organization's objectives in accordance with the terms of this EULA." Def.'s Mot. to

[6] 4DD's other software product, TETRA Enterprise Studio, is a graphic interface that enables a user to instruct TETRA Healthcare Federator to use data. TETRA Enterprise Studio is purchased separately and licensed by user seat instead of core.

Dismiss Ex. 9 at 423.[7] The EULA permitted the agency to make "one (1) copy of the object code to [TETRA] solely for back-up purposes," which it could only use "if the original copy is damaged or destroyed." *Id.* Other than the single back-up copy, the license agreement forbade copying TETRA, distributing copies of TETRA, or permitting others to copy or distribute copies of TETRA.

The agency required 4DD to disable its TETRA tracking feature, which otherwise would communicate with 4DD's systems to inform 4DD if a TETRA installation occurred. Consequently, as of September 26, 2013, the agency had purchased a license to deploy TETRA on up to 64 cores and to make only one back-up copy of TETRA, but 4DD could not track the use of its software.[8] Sheila Swenson was the Contracting Officer's Representative on the contract with Immix for the TETRA license.

After the agency entered into the TETRA license, SMS testing and configuration work began in earnest. Mr. Calvin, deposed as a designated representative on October 3, 2018, confirmed that, "yes," "the general workflow was, SMS would conduct development or testing, integration activities, in their environment, and then move the results of that into a production environment on the SMS side before it came over to the DTC[.]" Pls.' Resp. Mot. to Dismiss Ex. C at 14. Mr. Calvin also agreed, "yes," "the overall workflow involves the cloning of OVA images, and copying fully configured virtual machines from the SMS lab to the DTC[.]" *Id.* at 15.

Mr. Calvin went on to say "yes," SMS's work "in the SMS lab with TETRA would have involved cloning TETRA virtual machines in their labs[.]" *Id*. When asked, "And you understood [that SMS was] doing that, and they had your authorization to do so," Mr. Calvin responded, "Yes." *Id.* Similarly, when asked if SMS's testing activities "to the extent that it included cloning virtual machines of TETRA" were carried out with his

[7] Citations to the government's appendices refer to the page number at the bottom of the appendix page. Citations to plaintiffs' appendices refer to the page number at the top of the appendix page.

[8] The agency did not have an effective way to track TETRA use either. Communications between Ms. Swenson, 4DD, Mr. Calvin, and SMS demonstrate that the agency took responsibility for TETRA installations, but also that it spent several months in late 2013 attempting to find an accurate way to track TETRA use on the DMIX project. *E.g.*, Pls.' Resp. Ex. N, Ex. O at 196, Ex. P at 198.

authorization, Mr. Calvin responded, "Yes." *Id.* at 16. In short, Mr. Calvin explained, "Did they discuss with me what their plans were? Yes. Did they say this is the direction we're going with, and get concurrence? Yes." *Id.*

On December 27, 2013, the agency issued a change order for environment builds. It directed copying service-oriented architecture software from the initial DTC domain where TETRA was installed to other DTC environments. Mr. Calvin stated in his July 30, 2018 declaration that, when that software was copied, "the TETRA software, being also installed in that environment, would have been copied as well . . . ." Def.'s Resp. Mot. for Sanctions Ex. B.

Following the December 2013 copying on DTC servers, on March 7, 2014, SMS Deputy Project Manager William Eubank provided a status report to Mr. Calvin on activities in the DTC for the week. Mr. Eubank wrote,

> It appears the DFA software was cloned and moved[.] This should not have happened[;] SMS did not request this to be completed . . . . I need to know how you would like us to proceed: (Delete, Leave or Reimage) . . . . We will have to reimage in the future with newer version of DFA since we have delivered new versions since the clone of ICO1.

Pls.' Mot. for Sanctions Ex. T.

The attached "Weekly Project Status Report" states that TETRA had been copied in at least three environments. *Id.* Mr. Calvin responded on March 10, "I would say delete at this point." Pls.' Mot. Ex. U.

On May 14, 2014, Mr. Eubank reported in a "TETRA License Tracker" document that reconciling the number of cores in use had been completed

> and all licenses from Tetra that were installed in the DTC have not been pulled due to government not wanting to break down the environments. We have been told to leave the DTC and we have stopped all work in those environments. *I have also advised the government that they do not have enough licenses to support all the current environments within the DTC.* I'm confirming with 4DD on how we can remove the keys from the DTC. 4DD is confirming the information.

Pls.' Resp. Ex. BB (emphasis added).

In short, as early as May 2014, the agency knew that the project required broader use of TETRA than the agency had contracted for on the servers in the DTC alone, not accounting for the work being performed in SMS labs.

On May 20, 2014, Mr. Matus emailed the SMS test plan proposal for the DTC to Mr. Calvin. Mr. Calvin responded by asking, "Do we have enough TETRA licenses to cover testing?" Pls.' Mot. Ex. W. Mr. Matus responded with an accounting of TETRA downloads obtained by SMS. He noted that the DTC had "the same licenses in multiple environments," concluding "[t]hose TETRA instances really need to be deleted." *Id.*

4DD contacted Ms. Swenson on August 29, 2014, alleging that more than 64 cores were in use. 4DD's 4DD Vice President of Business Development Patrick Truxillo wrote, "The original purchase was for a block of 64 cores, which was fulfilled on November 20, 2013." Pls.' Mot. Ex. Z. Mr. Truxillo concluded that "68 additional cores" were in use for a total of 132 cores. Ms. Swenson replied, "Thank you for this report[.] We will evaluate the data and get back to you to discuss." *Id.* Ms. Swenson promptly forwarded Mr. Truxillo's email to Mr. Calvin, writing, "This is what I need to talk to you about…….!!!! over[-]installs, I should have been paying attention." Pls.' Mot. Ex. X.

The agency agreed to engage in a true up with 4DD regarding the use of TETRA. By this point Mr. Calvin had directed SMS to "remove the cloned copie[s] (if there were any) from DMS in other environments." Pls.' Mot. Ex. AA. 4DD was not informed at the time that the agencies intended to delete copies.

Communications within the agency from September 2-4, 2014, illustrate that the agency had not been keeping a detailed, easily accessible record of TETRA use. After fifteen months of TETRA use, on September 2, 2014, Mr. Calvin asked: "Anyway for someone to tell me how many licenses of TETRA are in the DTC?" *Id.* When Ken Allgood, involved in DTC oversight, asked, "Would TETRA be included as part of each DMS install/build that SMS has deployed," Mr. Calvin responded, "Should be." *Id.*

Just as the true up was getting underway, on September 6, 2014, SMS's Mr. Eubank emailed the agency, "Attached are the servers, IP's and environments that we will be deleting from the DTC environments. . . . Our COR has purchased enough licenses and wants to maintain the ICO1 environment as it was set up and installed in the beginning." Pls.' Mot. Ex. BB. A September 9, 2014 change request signed by Mr. Calvin, states, "Need to remove all cloned VM of TETRA from .com and .mil except ICO1 environment," and, "Remove all DMS/TETRA instances in the DTC on the .com/.mil environments. The only exception is the ICO1 environment." Pls.' Mot. Ex. CC. The scheduling explanation section states, "This is a license issue that we must clear up with ICO1 environment being the only environment that we have paid for this year." *Id.*

Regarding this change request, during his May 16, 2018 deposition in his personal capacity, Mr. Calvin stated that he would have discussed the change request approving the deletion of TETRA copies with Ms. Swenson. Pls.' Mot. Ex. C. He stated that she could have shared the decision to delete copies of TETRA with 4DD but that she did not do so. *Id.*

Ms. Swenson indeed did not inform 4DD of the deletions. During November 10 and 14, 2014 conference calls, the agency agreed to research the cores in use in the DTC and SMS environments. Between these calls, on November 12, Mr. Calvin emailed Ms. Swenson and other agency employees, "I'm attaching the original request to delete the VMs that have been talked about and a new request to delete the one remaining environment that was left in .com." Pls.' Mot. Ex. HH. He attached the September deletion order as well as a new November order, which states, "Remove all DMS/TETRA instances in the DTC on the .com/.mil environments." *Id.* The new deletion order also refers to the reason for deletion as "a license issue." *Id.* A third deletion order was created November 14. Pls.' Mot. Ex. CC.

During a conference call on December 12, 2014, the agency represented that it was continuing to gather information and confirm the number of cores allocated to the DTC. By December 16, 2014, the agency reported to 4DD that 64 cores were in use on DTC servers. The agency also had "identified an over deployment of 168 core licenses to development servers." Def.'s Mot. Ex. 12 at 459.

Despite these representations, Ms. Swenson explained in her May 21, 2018 deposition that 64 cores were reported because that was the number of cores the agency had originally paid for in the TETRA license. In fact,

although she "knew something was wrong" and was "suspicious," she had "no idea" how many cores were in use on DTC servers when the agency represented to 4DD that only 64 cores were in use. Pls.' Mot. Ex. JJ.

As the true up continued, a few relevant events occurred in early 2015. In January 2015, SMS communicated to the agency through a slide presentation that it was the contractor's position that SMS labs "was not Government directed or tasked" and that 4DD was aware it would not receive compensation for TETRA installations in SMS labs. Def.'s Mot. Ex. 5 at 202–07. In its privilege log, defendant claimed work product protection for a document dated January 23, 2015, because it was an "[e]mail [that] contains information for the purpose of receiving legal advice, and prepared in anticipation of 4DD Holdings, LLC v US litigation." Pls.' Mot. Ex. OO. Finally, in February 2015, the agency began the preliminary steps of decommissioning the DTC. Personnel from DHA were staffed with the decommissioning process, namely Joshua Zamarripa and Lauro Salais, who worked with contractors from ICS Nett and KSJ, particularly KSJ's Denise Stokely.

The true up concluded on March 16, 2015, with the agency and Immix modifying the TETRA license to increase the licensed quantity by 168 cores. The agency thus paid for 232 cores: 64 cores under the 2013 TETRA license, which the agency represented were used on DTC servers, and 168 cores under the 2015 modification, which the agency represented were used in SMS labs. The modification also states, "[T]he contractor hereby releases the Government from any and all liability under this contract for further equitable adjustments attributable to such facts and circumstances giving rise to this particular modification. All other terms and conditions remain unchanged." Def.'s Mot. Ex. 3 at 194. TETRA ultimately did not continue in use beyond the DMIX project.

4DD filed this lawsuit on August 28, 2015. On September 9, 2015, the Department of Justice sent the statutorily-required call letter to DoD, alerting DoD of its responsibility to provide a litigation report and to furnish all evidence in DoD's possession. Def.'s Resp. Ex. H. The letter includes these notes regarding evidence preservation:

> IMPORTANT: In the past it has been discovered that documents and papers necessary to the defense of an already pending suit were destroyed by an agency under its regular records screening and destruction program. In order to obviate

> such costly and detrimental occurrences, it is requested that all records storage centers and other facilities where records are kept be immediately notified to forthwith identify, physically segregate and withhold from destruction all documents and papers touching upon the claims set forth in the complaint. As soon as practicable, you are requested to send me a separate report designating each location where records are being held, together with a brief description of the nature of the records being held.
>
> It has also been our experience that in some cases there has been a failure to communicate with all field offices and installations having knowledge of the facts. . . . To assist you in communicating with these field offices, we are enclosing an extra copy of this document. If you need further copies, we shall be glad to furnish them.

*Id.*

Despite that notice, the decommissioning process did not change or stop to accommodate the need for evidence preservation. A month after 4DD filed its complaint, on September 22, 2015, Ms. Stokely emailed DHA personnel, "It looks like we are a go for the destruction of the hard drives on Saturday." Pls.' Mot. Ex. MM. She copied DHA's Mr. Zamarripa who was responsible for DTC oversight. The DTC hard drives were shredded, destroying all of the information on those hard drives, on September 26, 2015.

Nearly three months after 4DD filed this lawsuit, on November 13, 2015, the government sent out litigation hold notices. Mr. Salais, supervisor of the DTC decommissioning, did not receive a litigation hold notice until two years later, shortly before he was deposed.

As SMS concluded its work on the DMIX project, it began returning agency-issued laptops. On August 10, 2015, SMS returned 15 laptops to the agency. On October 1, 2015, SMS returned an additional 19 laptops. The government represents, based on DHA's deposition preparation chart, that most of the laptops that SMS returned were reimaged or retired and destroyed around or during March 2016. Def.'s Resp. 13. Reimaging erases the laptop's hard drives. The reimaging occurred months after the preservation hold had been issued.

During this period, Ms. Stokely also returned a laptop to the agency and was issued a second laptop. On March 16, 2016, the agency reimaged Ms. Stokely's first laptop, erasing all data on its hard drive.

Ms. Swenson testified as the government's representative regarding the laptop reimaging. In her October 19, 2017 deposition, Ms. Swenson acknowledged that she was aware of the lawsuit as of October 2015. She explained that her focus was gathering data relating to the true up. She stated that she "[d]id not even consider that SMS was a player in relevance of the case, since we already had their data from the true-up." Def.'s Resp. Ex N. Furthermore, she explained that SMS had other ways than the project laptops to document their work and communicate with the government. She explained the process of reimaging as follows: "I followed my standard process of I get laptops in, I give them to IT, I reissue them as needed. I inadvertently didn't even consider those laptops having anything relevant to this case because they are laptops, not servers, with 4DD documentation." *Id.*

In a subsequent December 21, 2017 deposition as a designated representative, Ms. Swenson stated that she was responsible for accepting the laptops at the end of the contract. She explained that neither she, nor any other agency employee, evaluated the laptops returned by SMS for relevant material that should have been preserved. She stated, "It became a blinding flash of the obvious when it was discussed in May of 2017." Pls.' Mot. Ex. TT.

The government was able to produce responsive documents from a few of the laptops that had not been reimaged. Furthermore, the government produced the contents of laptops issued to contractor ICS Nett, which was involved in both the execution of the 2014 deletion orders and the later DTC decommissioning.

The government filed its partial motion to dismiss plaintiffs' claim on June 24, 2016. The court ultimately stayed this motion to allow for discovery.

In July 2016, Mr. Zamarripa corresponded with DHA contractors regarding a preservation and search order from Glinda Hodgkin, DHA's Records Management Officer. He was seeking information regarding where TETRA had been installed in the past and whether any instances of it were

presently installed in listed labs. Some contractors responded that they did not find a record of TETRA, but Ms. Stokely responded on July 12, 2016, "[W]e can substantiate the existence of TETRA software in our prior lab. . . . the TETRA software did reside on a number of VMs in the DTC that were decommissioned . . . . Attached is a document containing a list of the VMs that were in the DTC as well as the CR requesting the decommission of said VMs." Pls.' Mot. Ex. UU.

Mr. Zamarripa reported this information to the government's counsel at the time. He explained that he had "just been informed that the DTC did indeed have the software in the decommissioned DTC. Prior to decommissioning the DTC all Virtual Machines which contained the software were permanently deleted." Pls.' Mot. Ex. VV.

Ms. Stokely returned her second laptop to the agency on November 14, 2016. On May 3, 2017, the government's counsel reminded DHA of its obligations to follow-up regarding data from these various agency-issued laptops. Despite its preservation obligation, on August 28, 2017, DHA erased the hard drive on the second Stokely laptop. The government was able to produce the emailed referenced above and the attached spreadsheet.

As discovery wound down, plaintiffs filed their motion for sanctions on November 21, 2018.

## DISCUSSION

Plaintiffs claim that the government infringed 4DD's copyright by making more copies of TETRA than the single back-up copy permitted by the EULA and by using TETRA beyond the number of installations that the TETRA license permitted. At issue here are both the government's partial motion to dismiss for lack of jurisdiction and plaintiffs' motion for sanctions due to the government's spoliation of evidence.

### I. We Deny The Partial Motion To Dismiss, Because Plaintiffs Established That The Government Authorized Or Consented To Its Contractor's Excessive Use Of TETRA In The Contractor's Labs.

Plaintiffs bear the burden of establishing this court's subject matter jurisdiction by a preponderance of the evidence. *Trusted Integration, Inc. v. United States*, 659 F.3d 1159, 1163 (Fed. Cir. 2011) (citing *Reynolds v. Army & Air Force Exch. Serv.*, 846 F.2d 746, 748 (Fed. Cir. 1988)). When

considering a motion to dismiss for lack of jurisdiction, the court accepts as true the undisputed facts in plaintiffs' complaint and draws reasonable inferences in plaintiffs' favor. *Id.* To determine whether it has jurisdiction, however, the court also may consider other relevant evidence. *Reynolds*, 846 F.2d at 748.

Defendant argues that this court does not have jurisdiction over part of plaintiffs' claim because 28 U.S.C. § 1498(b) (2012) requires that the government authorize or consent to its contractor's infringement for the government to be held responsible for that infringement.[9] The government concedes that it authorized or consented to any infringing activity that occurred when SMS, or other contractors, worked with TETRA on DTC servers, but it contends that it did not authorize or consent to infringing activity that occurred when SMS worked with TETRA in SMS labs.

Section 1498(b) states,

> [W]henever the copyright in any work protected under the copyright laws of the United States shall be infringed . . . by a contractor, subcontractor, or any person, firm, or corporation acting for the Government and with the authorization or consent of the Government, the exclusive action which may be brought for such infringement shall be an action by the copyright owner against the United States in the Court of Federal Claims . . . .

The question here is whether SMS was acting (1) "for the Government" and (2) "with the authorization or consent of the Government" when it performed any infringing activity in SMS labs. *Id.* The answer is plainly yes.

To establish that the contractor was acting for the government, plaintiffs must show that the "infringing activity has been performed by a government contractor pursuant to a government contract and for the benefit

---

[9] Defendant also argues that plaintiffs cannot rely on the EULA as a substantive source of subject matter jurisdiction. Because 4DD states unequivocally that its "sole claim is for copyright infringement under 17 U.S.C. §§ 106, 504 and 28 U.S.C. § 1498(b)—not a breach of contract claim under the EULA," Pls.' Resp. 35, the EULA is not the potential source of jurisdiction.

of the government . . . ." *Sevenson Environ. Servs., Inc. v. Shaw Environ., Inc.*, 477 F.3d 1361, 1366 (Fed. Cir. 2007) (interpreting "for the United States" in the patent infringement section, 28 U.S.C. § 1498(a)). The evidence presented shows that SMS was at all relevant times the agency's contractor for testing and configuring TETRA on the DMIX project. The communications between SMS and the government also reflect that the only reason SMS was using TETRA was for the DMIX project, despite SMS statements to the agency that SMS did not believe that its TETRA use was agency-directed. Thus, SMS's actions were undertaken for the government.

Plaintiffs also must establish that the government "authorize[d] or consent[ed] to infringement by a third party acting for it." *Boyle v. United States*, 200 F.3d 1369, 1373 (Fed. Cir. 2000). The Federal Circuit in *Boyle* cited *Auerbach v. Sverdup Corp.*, 829 F.2d 175, 179 (D.C. Cir. 1987), to explain that although the government is liable for infringing activity it authorizes, it is not responsible for "any copyright infringement the third party may choose to undertake within the sphere of the authorized action," i.e., on its own initiative.

Plaintiffs must point to "explicit acts or extrinsic evidence sufficient to prove the government's intention to accept liability for a specific act of infringement." *Id.* at 177. Authorization or consent may be either express, such as a contract clause, or implied, such as when infringement is necessary to the contractor's performance of its contract. *Id.* at 180.

In *TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060 (Fed. Cir. 1986), the Federal Circuit found that the government's authorization could be implied where bidding procedures required the offeror to include certain allegedly infringing material. The court reasoned that "[t]he mere fact that the Government specifications for the targets did not absolutely require Blane to infringe TVI's patent at that demonstration does not extinguish the Government's consent." *Id.* at 1060. The court explained that the "coverage of § 1498 should be broad so as not to limit the Government's freedom in procurement . . . ." *Id.* Similarly, in *Advanced Software Design Corp. v. Fed. Reserve Bank of St. Louis*, 583 F.3d 1371, 1376 (Fed. Cir. 2009), the Federal Circuit found government authorization when the Treasury had sent letters and made statements to certain banks directing the allegedly infringing use of a technology. The Court of Claims summarized in *Hughes Aircraft Co. v. United States*, 534 F.2d 889, 901 (Ct. Cl. 1976), that

> 'authorization or consent' on the part of the Government may be given in many ways other than by letter or other direct form of communication—e.g., by contracting officer instructions, by specifications or drawings which impliedly sanction and necessitate infringement, [or] by post hoc intervention of the Government in pending infringement litigation against individual contractors.

On the other hand, the fact that the government simply benefits from infringement is insufficient to demonstrate authorization or consent. In *Auerbach*, a contractor copied an architect's plans to build a garage for the government. The court held that "[t]he fact that the federal government might benefit from the copying because it subsequently will have ownership of the building does not make the United States a party to the copyright violation." 829 F.2d at 180. Since there was not an authorization clause, a statement or action authorizing copying the plans, or some requirement that necessitated using the plans, the government did not authorize or consent to that infringing activity. *Id.*

The government argues that any infringing use of TETRA in SMS labs was on the contractor's own initiative, perhaps within the range of options SMS could have used to accomplish its tasks but not endorsed by the agency. The government explained that although it would have authorized actions relating to the DTC, it did not know how SMS was using TETRA in its own labs. Defendant points out that there was no authorization clause in the contract and that the agency attempted to determine how many cores the license should include. Defendant also relies on SMS statements to the agency that it did not believe the agency had directed its actions.

We find that the agency did authorize or consent to its contractor's allegedly infringing use of TETRA in SMS labs, namely making additional copies of TETRA and installing TETRA in excess of the purchased license. Plaintiffs allege that any copying would have exceeded the license and any direction to copy would have constituted a direction to exceed the license. Plaintiffs also allege that any use beyond the purchased cores exceeds the license and constitutes infringement. Plaintiffs have demonstrated authorization or consent to these actions by SMS in at least two ways. First, the agency directed SMS to engage in actions that necessitated copying TETRA and it approved SMS's plan to copy virtual machines containing

TETRA. Second, the agency accepted liability for SMS's excessive use of TETRA in SMS labs in the 2015 TETRA license modification.

First, Mr. Calvin approved SMS's plan to copy virtual machines containing TETRA and directed SMS to accomplish tasks that required cloning the software. When it directed SMS to perform work in its own labs, the agency understood that SMS's work necessarily would have involved cloning virtual machines containing TETRA, and Mr. Calvin stated that such copying was done with his authorization. The agency expressly directed a DTC environment that contained TETRA to be cloned in December 2013. Furthermore, the agency's approved workflow in the DTC alone required SMS to exceed the licensed amount of TETRA use, meaning that, of necessity, SMS's work in its own labs would exceed the licensed number of cores. Even if SMS could have accomplished the tasks another way, which defendant did not argue, "the mere fact that" options exist "does not extinguish the Government's consent." *TVI Energy Corp.*, 806 F.2d at 1060.

Defendant is correct that SMS's contract lacked an authorization clause, but such a clause is not the only way to demonstrate authorization. Here, the agency directed software copying and SMS's reports on its work further alerted the agency to SMS's copying. Mr. Calvin did not shy away from the fact that the agency approved the copying. SMS's statements that it did not believe the agency was directing its work are contradicted by the agency's directions, SMS's reports, and Mr. Calvin's statements.

Moreover, defendant's attempt to draw a distinction between SMS engaging in infringing activity in its own labs versus in the DTC is unavailing. There is no appreciable difference between the work completed in the two locations. The agency expressly authorized SMS to perform TETRA testing and configuration in both SMS labs and the DTC. Mr. Calvin confirmed that SMS accomplished its duties by copying software from its own labs into the DTC—the work performed in the different locations was inextricably linked.

Second, when 4DD requested an investigation into whether TETRA was being used in accordance with the license agreement, the agency included SMS labs in its assessment and chose to pay for over-installations of TETRA in SMS labs. The agency did not treat the use of TETRA in SMS

labs any differently than the use of TETRA in the DTC. Instead, the agency assumed responsibility for SMS activities in both locations. In fact, the agency maintained that the 168 additional cores that it paid for in March 2015 were those cores found in SMS labs, not those on the DTC servers.

Furthermore, the TETRA license modification flowed naturally from the agency's statements at the beginning of project that it was responsible for how TETRA was deployed. Mr. Calvin and Ms. Swenson expressly communicated to both 4DD and SMS, just after purchasing the TETRA license, that the agency would manage the TETRA license and that it was responsible for TETRA use on virtual machines. SMS was not given a general objective and permitted to execute it however it saw fit. Instead, Mr. Calvin and Ms. Swenson sought accounting of TETRA installations; SMS reported to the agency weekly; and Mr. Calvin conceded that he approved the virtual machine copying. When SMS thought that its use of TETRA between the DTC and its labs would exceed the license purchased, SMS sought direction from Mr. Calvin, involving him at every turn. The government may not have known exactly how widespread the usage was, but it was certainly hands-on in its directions on where to use the TETRA software. Its hand-on approach culminated in accepting responsibility for excessive use of TETRA in SMS labs.

Taken together, the agency's instructions, concessions, and acceptance of responsibility demonstrate that the agency authorized or consented to SMS's allegedly infringing use of the TETRA software.

## II. The Government With A Culpable State Of Mind Destroyed Relevant Evidence That It Had A Duty To Preserve And Sanctions Are Appropriate.

We now turn to plaintiffs' motion for sanctions. 4DD argues that the government destroyed evidence relevant to prove that infringement occurred and to determine the damages associated with any infringement. Plaintiffs contend that the court should impose all available sanctions for this destruction of evidence, including granting 4DD a default judgment on liability and imposing an adverse inference against the government with respect to damages. It argues that the court also should preclude the government from cross-examining 4DD's witnesses, submitting secondary evidence, and arguing that evidentiary gaps should be construed in the government's favor. Finally, plaintiffs ask the court to award it fees and costs

for bringing the motion and for conducting additional discovery necessary to assess and ameliorate the government's spoliation.

The parties agree on the key events: The agency deleted instances of TETRA during the true-up period without informing 4DD. The agency destroyed the DTC servers' hard drives. The agency erased all the information on many laptops used on the DMIX project. The government nevertheless argues that these three categories of evidence destruction do not constitute spoliation. It contends that the agency had no duty to preserve this evidence, that some of it was not relevant, and that the evidence can be replaced by other discovery. The government also contends that the most severe sanctions cannot be imposed because the evidence was not destroyed with intent to deprive 4DD of its use in litigation.

Spoliation occurs when a party destroys or materially alters relevant evidence that it had a duty to preserve. *United Med. Supply Co. v. United States*, 77 Fed. Cl. 257, 268 (2007). The court may impose sanctions for spoliation based on the court's inherent authority to govern the judicial process and pursuant to Rule 37 of the Rules of the United States Court of Federal Claims. *Chambers v. NASCO, Inc.*, 501 U.S. 32, 45–46 (1991).

Parties have a duty to preserve evidence when litigation is "'pending or reasonably foreseeable.'" *Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311, 1320 (Fed. Cir. 2011) (quoting *Silvestri v. General Motors Corp.*, 271 F.3d 583, 590 (4th Cir. 2001)). Determining when litigation is reasonably foreseeable "is a flexible fact-specific standard," allowing the court to exercise its discretion. *Id.* The duty is not triggered by the "distant possibility of litigation" but does not require imminent litigation. *Id.* at 1319–20. "This is an objective standard, asking not whether the party in fact reasonably foresaw litigation, but whether a reasonable party in the same factual circumstances would have reasonably foreseen litigation." *Id.* at 1320. When determining what sanctions are warranted, the spoliator's state of mind is relevant. *United Med. Supply Co.*, 77 Fed. Cl. at 268–70. Ordinary negligence may be sufficient to show the culpable state of mind, but for more severe sanctions, the showing of culpability may require more than negligence. *Id*.

When the evidence at issue is electronically stored information, Rule 37(e) sets out the framework for imposing sanctions. Rule 37(e) adopts the traditional spoliation standards but adds the requirement that the court find

"intent to deprive another party of the information's use in litigation" before imposing the most severe sanctions:

> 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 as unfavorable to the party; . . . or (C) dismiss the action or enter a default judgment.

Since the evidence at issue here is electronically stored information, we will follow the elements set out in Rule 37(e)(2).[10] The first question is whether the government had a duty to preserve any of this evidence. Plaintiffs successfully demonstrated that the evidence at issue is relevant. The deleted copies of TETRA and data stored on DTC servers are at the heart of the claim: the copying on DTC servers is one of the alleged infringing acts. In addition, based on the limited laptop production, plaintiffs have shown that the reimaged laptops likely contained communications and other information relevant to how TETRA was used.

The government argues that the deleted copies of TETRA are not evidence that the agency should have preserved because they were "nonfunctional," in other words not configured or not usable. The notion of "nonfunctional" installations of TETRA arose after litigation commenced during discovery disagreements. Mr. Calvin appears to have first raised the concept. At oral argument defendant took the position that if an installation of TETRA either could not work in a particular environment because it was not properly configured or because of security constraints, it was

[10] Rule 37(e) does not define electronically stored information, but plaintiffs concede that the deleted copies of TETRA and the data erased from the project laptops are electronically stored information. Plaintiffs argue that the shredded DTC hard drives could be viewed as physical evidence. We disagree: the hard drives are not the relevant evidence here; the evidence is the data that the DTC servers stored prior to their destruction. Thus, all three categories are electronically stored information.

"nonfunctional" and the agency could delete those copies with impunity; it had no duty to preserve, or make reasonable efforts to preserve, such copies and the deletion was not prejudicial because the agency would not need to pay 4DD for those copies.

The government is unable to point to a single instance, during the DMIX project, in which anyone referred to copies of TETRA as "nonfunctional." Nor could defendant point to an instance where anyone suggested that certain copies of or use of TETRA would not need to be paid for if they exceeded the rights granted under the TETRA license— functional or otherwise. The evidence shows the opposite: the deletion orders explain the reason for deletion as a concern with "a license issue," not because the software was not fully configured or because it was inconsistent with security protocols.

Turning to when the duty to preserve evidence arose, at the point at which the DTC hard drives were shredded and when many of the laptops were reimaged, litigation was already pending. Defendant undoubtedly had a duty to preserve the evidence contained on the DTC servers and the laptops after litigation had commenced.

The agency should have preserved evidence in the anticipation of litigation before 4DD filed its complaint, however. On August 29, 2014, 4DD placed the agency on notice that it believed the agency had used its software inconsistently with the agency's rights under the TETRA license. The agency agreed to investigate the use of TETRA in agency- and contractor-owned labs. A reasonable party would certainly anticipate litigation when faced with an allegation that it had exceeded rights under a contract and when it agreed to investigate that allegation.

Furthermore, the agency spent several months agreeing to investigate the extent of copying while simultaneously deleting evidence of what 4DD had asked the agency to enumerate. Indeed, during the true up process, the agency created documents that the government later marked as work product on its privilege log, stating that this material was created in anticipation of litigation. Although defendant later waived its claim of privilege for those documents, the fact remains that the agency had reason to anticipate litigation with plaintiffs at the beginning of the true up period. The agency in fact foresaw litigation as early as January 2015.

Since the government had a duty to preserve the evidence at issue, the next question is whether the government took reasonable steps to preserve it. Regarding copies of TETRA deleted during the true up process, the agency chose to destroy rather than preserve evidence. Also, the government never attempted to accurately account for TETRA used on the DTC servers. It simply arbitrarily assigned the original 64 paid-for cores to the DTC and allowed the DTC to continue along the path to decommissioning without making records of how many copies of TETRA had existed. During the true up process and thereafter, the agency did the opposite of taking reasonable steps to preserve a record of TETRA use, leaving the DTC servers and other environments where TETRA was installed as the only complete record.

After 4DD filed its complaint, the government delayed nearly three months in issuing preservation notices, by which point data on the DTC hard drives was lost. The exact danger that the call letter predicted came to pass. Had the government more promptly notified DHA, perhaps the DTC destruction could have been averted or the data stored there archived for future access. Even when the government did issue a preservation hold, that notice failed to reach the personnel responsible for the decommissioning until nearly two years later. In addition to the delayed release of the preservation hold, the government continued to allow evidence to slip through the cracks: laptop reimaging occurred long after the complaint was filed, apparently because no process was in place to check for relevant data. Even though the government eventually produced some information from a few laptops, the effort to preserve electronically stored information was inexcusably shoddy.

The government argues that sanctions are inappropriate because the information that has been lost can be replaced by other discovery. For instance, the government contends that images of hard drives containing data made before decommissioning, server diagrams, change orders, and SMS weekly progress reports are sufficient to demonstrate where and in what quantities TETRA was installed. Those copies, however, are incomplete. Also, as plaintiffs note, the change orders list environments in which to delete TETRA without an accompanying instruction to note the copies of TETRA or the cores in use. SMS weekly reports merely reflect TETRA use in general terms. Likewise, license trackers were incomplete and voluntary from the beginning, making them unreliable sources of data.

Furthermore, plaintiffs argue that SMS project data could have been stored on the project laptops and plaintiffs represent that SMS production has

not included a replacement way to account for TETRA copies and cores. Although plaintiffs have been able to access some evidence of where TETRA was present, this evidence is partial and cannot offer a comprehensive, reliable picture.

To impose sanctions, the only remaining step is to determine whether plaintiffs suffer prejudice because of the agency's spoliation. Prejudice may appear in many forms, such as plaintiffs being "unable to fully respond to the secondary evidence" or being required to go to great lengths in discovery to fill in the gaps in the evidence. *Lab. Corp. v. United States*, 108 Fed. Cl. 549, 562 (Fed. Cl. 2012); *see also United Med. Supply Co.*, 77 Fed. Cl. at 274–75. We find that the government's destruction of evidence prejudices plaintiffs in their attempt to demonstrate both the fact of infringement and any damages flowing from that infringement. First, the government's consistent deletion of evidence—whether purposeful or inadvertent—created gaps that plaintiffs must now try to fill by cobbling together secondary evidence. Plaintiffs note that the government's argument that the deleted copies of TETRA were nonfunctional is a perfect example of how the deletion works in the government's favor. If that allegation were relevant, plaintiffs effectively cannot combat the assertion because the copies no longer exist. The government's failure to preserve also dramatically added to the time and resources dedicated to discovery.

We find that it is appropriate to award 4DD fees and costs for bringing this motion and conducting additional discovery necessary to assess and ameliorate the government's spoliation. Furthermore, the government will be precluded from arguing that evidentiary gaps created by its spoliation should be construed in the government's favor.

Rule 37(e)(2) imposes a prerequisite to going further, however, to presume that the lost information is unfavorable to the spoliator. The court first must find that the party acted with the intent to deprive another party of the information's use in litigation. This 2015 addition to Rule 37 has been interpreted by various trial courts to require a showing of anything from bad faith to irresponsible behavior that lacks any other explanation than intent to deprive. *E.g.*, *Brewer v. Leprino Foods Co.*, 2019 WL 356657, *10 (E.D. Cal. Jan. 29, 2019) (finding that the "pattern of conduct suggests intentional spoliation"); *Oracle Am., Inc. v. Hewlett Packard Enter. Co.*, 328 F.R.D. 543, 549 (N.D. Cal. 2018) ("not merely negligent or even grossly negligent, but an intentional effort to keep the ESI from the opposing party"); *Alabama Aircraft Indus. v. Boeing Co.*, 319 F.R.D. 730, 746 (N.D. Ala. 2017)

("blatantly irresponsible behavior"); *Ottoson v. SMBC Leasing & Finance, Inc.*, 268 F. Supp. 3d 570, 584 (S.D.N.Y 2017) ("acted willfully or in bad faith"). The matching Federal Rule of Civil Procedure 37(e)(2) Advisory Committee Notes state that the amendment rejects cases "that authorize the giving of adverse-inference instructions on a finding of negligence or gross negligence."

Here, Mr. Calvin's orders directing contractors to delete instances of TETRA in listed environments because of "a license issue" is sufficient to demonstrate that he intentionally deprived 4DD of the use of that information in litigation. 4DD had made the agency aware of its contention that it was owed money for over-installation of the software at a time when the agency held out that it was engaged in a "true up." While the agency represented to 4DD that it was still counting instances of TETRA, Mr. Calvin was ordering that evidence of installation be deleted. We can conclude based on Mr. Calvin's direction and his explanation that the agency intended to deprive 4DD of the use of that information at a time when litigation was plainly foreseeable. Therefore, it is appropriate to presume that a preserved, accurate count of the number of copies of TETRA on DTC servers would have been unfavorable to the government.

The DTC decommissioning and laptop reimaging are not as clear cut. Regarding the SMS laptops, Ms. Swenson apparently did not consider whether those laptops contained relevant information at all, much less whether to delete information intentionally to avoid its disclosure to another party. But that explanation is conveniently narrow: why would the agency only be retaining information related to the true up when the complaint and preservation hold were not limited in that way? Long after litigation had begun, there was no effort made to alert people who had been intimately involved with TETRA installations, like Ms. Swenson, to the need to retain all relevant information and not undertake any deletions. The lack of any credible explanation for the deletion of the laptop data months into this litigation and in the face of a preservation hold is sufficient to infer that the agency deleted information that was detrimental to it.

The decommissioning, on the other hand, appears to have occurred according to regular process rather than an intentional effort to keep that information from plaintiffs. We agree with plaintiffs that, at a minimum, the agency acted negligently regarding the information stored on DTC servers. The agency should have availed itself of alternatives to retaining those hard drives, such as creating a record of how software was used and where it was

installed on DTC and its contractor's servers. The result of the destruction is that both parties are left without any complete record of the contents of the DTC servers.

But there is not a pattern of willful behavior here as there is with repeated laptop reimaging. Instead, the agency suffered from the exact problem that the Department of Justice call letter predicted: a failure to communicate within this sprawling project. The process began in February 2015 as the project wound down and continued to completion without any regard for this lawsuit. The appropriate personnel apparently did not know about the litigation hold prior to the decommissioning. The contractors responsible for giving the "go" for shredding similarly did not know the effect that decommissioning would have. This communication failure is undoubtedly negligent but falls short of the intentional behavior expected under Rule 37(e)(2). We therefore will not draw an adverse inference against the government regarding the content of the destroyed hard drives.

Ultimately, all three sources of evidence discussed in this section would have aided in determining the extent of the government's use of 4DD's software, and, if it exceeded the government's rights in the software, in determining what damages are owed. As discussed at oral argument, we will not enter a default judgment on liability, but we will draw the necessary adverse inferences against the government to account for deletion of TETRA on DTC servers and deletion of project data from agency laptops. This remedy is sufficient, particularly when coupled with fees and costs associated with this motion and conducting additional discovery and precluding the government from arguing that evidentiary gaps created by its spoliation should be construed in its favor. Because the parties currently are working toward the conclusion of discovery, we will defer until summary judgment or trial the question of how specifically to apply the inferences that plaintiffs ask us to draw against defendant.

## CONCLUSION

Because plaintiffs established that the government authorized or consented to SMS's allegedly infringing activity when working in SMS labs, we deny defendant's motion to dismiss. Furthermore, we grant plaintiffs' motion for sanctions because the government destroyed relevant evidence that it had a duty to preserve. Plaintiffs are directed to file a motion, appropriately supported, seeking a recovery of its costs and fees related to the motion for sanctions and with respect to discovery prompted by the

destruction of evidence. The court will defer until summary judgment or trial the application of the evidentiary implications of this ruling.

s/Eric G. Bruggink
ERIC G. BRUGGINK
Senior Judge