APPENDIX

APPENDIX

TABLE OF CONTENTS

APPENDIX A

UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

No. 22-40020
Summary Calendar

[Filed January 10, 2023]

UNITED STATES OF AMERICA, *Plaintiff—Appellee*,	)
versus	)
CLAY MELTON DENTON, *Defendant—Appellant*.	)

Appeal from the United States District Court
for the Eastern District of Texas
USDC No. 4:19-CR-241-1

Before WIENER, ELROD, and ENGELHARDT, *Circuit Judges*.

PER CURIAM:[*]

Clay Melton Denton was found guilty by a jury of distribution of child pornography, receipt of child pornography, and possession of child pornography

[*] This opinion is not designated for publication. *See* 5TH CIR. R. 47.5.

involving a prepubescent minor. He was sentenced within the applicable guidelines range to 240 months of imprisonment, followed by eight years of supervised release. On appeal, Denton challenges the district court's denial of his motion to dismiss his indictment and its rejection of his requested spoliation jury instruction. He also contends that the district court procedurally erred in its analysis of 18 U.S.C. § 3553(a)(6) and failed to consider disparities among defendants nationwide in denying his request for a downward sentencing variance.

We review a district court's denial of a motion to dismiss an indictment de novo and the underlying factual findings, including a bad faith determination, for clear error. *United States v. McNealy*, 625 F.3d 858, 868-69 (5th Cir. 2010). To prevail on his motion to dismiss his indictment, Denton was required to show that potentially useful evidence was lost or destroyed by the Government in bad faith. *See Arizona v. Youngblood*, 488 U.S. 51, 57–58 (1988) (government's failure to preserve "material exculpatory evidence" constitutes a denial of due process irrespective of good or bad faith but "merely potentially useful evidence" requires a showing of bad faith); *McNealy*, 625 F.3d at 868. There is no evidence that law enforcement personnel intentionally lost or destroyed any digital evidence in order to impede Denton's defense. Rather, the record reflects that the search team followed what they believed to be standard procedures and conducted a risk analysis before powering down and seizing devices at Denton's home. Denton therefore has failed to show that the district court clearly erred in

determining there was no bad faith and denying his motion to dismiss. *See McNealy*, 625 F.3d at 868-70.

Next, we review the district court's denial of a spoliation jury instruction for abuse of discretion. *United States v. Valas*, 822 F.3d 228, 239 (5th Cir. 2016). "[T]he party seeking the instruction must demonstrate bad faith or bad conduct by the other party." *Id.*; *see United States v. Wise*, 221 F.3d 140, 156 (5th Cir. 2000). "Bad faith, in the context of spoliation, generally means destruction for the purpose of hiding adverse evidence." *Guzman v. Jones*, 804 F.3d 707, 713 (5th Cir. 2015) (addressing spoliation in the civil context). Although Denton urges this court to adopt a lesser standard of culpability, such as negligence, we are bound by the rule of orderliness. *See United States v. Berry*, 951 F.3d 632, 636 (5th Cir. 2020) (later panel cannot overrule an earlier panel's decision). Denton maintains that the agents failed to properly power off his devices, seize all components of his computer system, and map the system. Nothing in the record, however, establishes that the agents intentionally failed to do these things for the purpose of hiding exculpatory evidence. Thus, because Denton failed to show bad faith, we find no abuse of discretion. *See Valas*, 822 F.3d at 239.

Because Denton did not preserve his claim of procedural error, our review of his sentence is for plain error. *See United States v. Mondragon-Santiago*, 564 F.3d 357, 361 (5th Cir. 2009). In support of his argument that the district court improperly limited its analysis and construction of § 3553(a)(6), and failed to consider disparities among defendants nationwide,

Denton relies on the district court's remarks that it had never granted a downward variance in a child pornography case based on the nationwide statistics submitted by Denton. This argument, however, fails to recognize that the district court's remarks were made in response to Denton's contentions—in support of his requested downward variance—that inconsistencies in child pornography sentences exist across the federal districts and that application of the Sentencing Guidelines in his case is against public policy. Denton has not shown that the district court committed a clear or obvious procedural error. *See Puckett v. United States*, 556 U.S. 129, 135 (2009).

To the extent that Denton's arguments may be viewed as a challenge to the substantive reasonableness of his sentence, our review is for abuse of discretion. *See Holguin-Hernandez v. United States*, 140 S. Ct. 762, 766–67 (2020); *see also United States v. Douglas*, 957 F.3d 602, 609 (5th Cir. 2020). Denton's argument that the district court erred by not considering the nationwide sentencing disparities among similarly situated defendants is unpersuasive. *See United States v. Waguespack*, 935 F.3d 322, 337 (5th Cir. 2019); *United States v. Hernandez*, 633 F.3d 370, 379 (5th Cir. 2011). Denton is essentially asking us to reweigh the § 3553(a) factors, which we will not do. *See Gall v. United States*, 552 U.S. 38, 51 (2007). Moreover, his argument does not suffice to rebut the presumption of reasonableness that applies to his within-guidelines sentence. *See United States v. Ruiz*, 621 F.3d 390, 398 (5th Cir. 2010).

The judgment of the district court is AFFIRMED.

APPENDIX B

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

[Filed January 7, 2022]

UNITED STATES OF AMERICA	)
	)
v.	)
	)
CLAY MELTON DENTON	)
	)

JUDGMENT IN A CRIMINAL CASE

Case Number: **4:19-CR-00241-ALM-KPJ(1)**
USM Number: **28850-078**
James Joseph Mongaras
Defendant's Attorney

THE DEFENDANT:

□	pleaded guilty to count(s)	
□	pleaded guilty to count(s) before a U.S. Magistrate Judge, which was accepted by the court.	
□	pleaded nolo contendere to count(s) which was accepted by the court	

☒	was found guilty on count(s) after a plea of not guilty	**1, 2, and 3 of the First Superseding Indictment**

The defendant is adjudicated guilty of these offenses:

Title & Section / Nature of Offense		**Offense Ended**	**Count**
18:2252A(a)(2)(A), 18 U.S.C. §§ 2252A(b)(1)	Distribution Of Child Pornography	04/25/2018	1
18:2252A(a)(2)(A), 18 U.S.C. §§ 2252A(b)(1)	Receipt Of Child Pornography	04/25/2018	2
18:2252A(a)(5)(B), 18 U.S.C. §§ 2252A(b)(2)	Possession Of Child Pornography	04/25/2018	3

The defendant is sentenced as provided in pages 2 through 9 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

□ The defendant has been found not guilty on count(s)

□ Count(s) □ is □ are dismissed on the motion of the United States

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid.

If ordered to pay restitution, the defendant must notify the court and United States attorney of material changes in economic circumstances.

January 5, 2022
Date of Imposition of Judgment
/s/ Amos Mazzant
Signature of Judge
AMOS L. MAZZANT, III
UNITED STATES DISTRICT JUDGE
Name and Title of Judge
January 7, 2022
Date

DEFENDANT: CLAY MELTON DENTON
CASE NUMBER: 4:19-CR-00241-ALM-KPJ(1)

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a total term of: 240 months on each of Counts 1, 2, and 3 of the First Superseding Indictment, all to be served concurrently.

☒ The court makes the following recommendations to the Bureau of Prisons: The Court recommends that Defendant be designated to a BOP facility in Seagoville Texas, if appropriate. The Court recommends the Defendant receive appropriate sex offender treatment while imprisoned.

☒ The defendant is remanded to the custody of the United States Marshal.

□ The defendant shall surrender to the United States Marshal for this district:

□ at □ a.m. □ p.m. on

□ as notified by the United States Marshal.

□ The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:

□ before 2 p.m. on

□ as notified by the United States Marshal.

□ as notified by the Probation or Pretrial Services Office.

RETURN

I have executed this judgment as follows:

Defendant delivered on _____ to
at _____, with a certified copy of this judgment.

UNITED STATES MARSHAL

By
DEPUTY UNITED STATES MARSHAL

SUPERVISED RELEASE

Upon release from imprisonment, the defendant shall be on supervised release for a term of: **eight (8) years.** This term consists of terms of 5 years on each of Counts 1, 2, and 3 of the First Superseding Indictment, all such terms to run concurrently.

MANDATORY CONDITIONS

1. You must not commit another federal, state or local crime.

2. You must not unlawfully possess a controlled substance.

3. You must refrain from any unlawful use of a controlled substance. You must submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.

   ☐ The above drug testing condition is suspended, based on the court's determination that you pose a low risk of future substance abuse. (*check if applicable*)

4. ☐ You must make restitution in accordance with 18 U.S.C. §§ 3663 and 3663A or any other statute authorizing a sentence of restitution. *(check if applicable)*

5. ☒ You must cooperate in the collection of DNA as directed by the probation officer. (*check if applicable*)

6. ☒ You must comply with the requirements of the Sex Offender Registration and Notification Act (34 U.S.C. § 20901, et seq.) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in which you reside,

work, are a student, or were convicted of a qualifying offense. (*check if applicable*)

7. ☐ You must participate in an approved program for domestic violence. (*check if applicable*)

You must comply with the standard conditions that have been adopted by this court as well as with any additional conditions on the attached page.

STANDARD CONDITIONS OF SUPERVISION

As part of your supervised release, you must comply with the following standard conditions of supervision. These conditions are imposed because they establish the basic expectations for your behavior while on supervision and identify the minimum tools needed by probation officers to keep informed, report to the court about, and bring about improvements in your conduct and condition.

1. You must report to the probation office in the federal judicial district where you are authorized to reside within 72 hours of your release from imprisonment, unless the probation officer instructs you to report to a different probation office or within a different time frame.
2. After initially reporting to the probation office, you will receive instructions from the court or the probation officer about how and when you must report to the probation officer, and you must report to the probation officer as instructed.
3. You must not knowingly leave the federal judicial district where you are authorized to

reside without first getting permission from the court or the probation officer.

4. You must answer truthfully the questions asked by your probation officer.
5. You must live at a place approved by the probation officer. If you plan to change where you live or anything about your living arrangements (such as the people you live with), you must notify the probation officer at least 10 days before the change. If notifying the probation officer in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.
6. You must allow the probation officer to visit you at any time at your home or elsewhere, and you must permit the probation officer to take any items prohibited by the conditions of your supervision that he or she observes in plain view.
7. You must work full time (at least 30 hours per week) at a lawful type of employment, unless the probation officer excuses you from doing so. If you do not have full-time employment you must try to find full-time employment, unless the probation officer excuses you from doing so. If you plan to change where you work or anything about your work (such as your position or your job responsibilities), you must notify the probation officer at least 10 days before the change. If notifying the probation officer at least 10 days in advance is not possible due to unanticipated circumstances, you must notify

the probation officer within 72 hours of becoming aware of a change or expected change.

8. You must not communicate or interact with someone you know is engaged in criminal activity. If you know someone has been convicted of a felony, you must not knowingly communicate or interact with that person without first getting the permission of the probation officer.
9. If you are arrested or questioned by a law enforcement officer, you must notify the probation officer within 72 hours.
10. You must not own, possess, or have access to a firearm, ammunition, destructive device, or dangerous weapon (i.e., anything that was designed, or was modified for, the specific purpose of causing bodily injury or death to another person such as nunchakus or tasers).
11. You must not act or make any agreement with a law enforcement agency to act as a confidential human source or informant without first getting the permission of the court.
12. If the probation officer determines that you pose a risk to another person (including an organization), the probation officer may require you to notify the person about the risk and you must comply with that instruction. The probation officer may contact the person and confirm that you have notified the person about the risk.
13. You must follow the instructions of the probation officer related to the conditions of supervision.

U.S. Probation Office Use Only

A U.S. probation officer has instructed me on the conditions specified by the court and has provided me with a written copy of this judgment containing these conditions. For further information regarding these conditions, see *Overview of Probation and Supervised Release Conditions*, available at: www.uscourts.gov.

Defendant's Signature _____ Date _____

SPECIAL CONDITIONS OF SUPERVISION

You must provide the probation officer with access to any requested financial information for purposes of monitoring restitution payments and employment.

You must not incur new credit charges or open additional lines of credit without the approval of the probation officer unless payment of any financial obligation ordered by the Court has been paid in full.

You must participate in a sex offender treatment program. You must abide by all rules and regulations of the treatment program, until discharged. The probation officer, in consultation with the treatment provider, will supervise your participation in the program. You must pay any costs associated with treatment and testing. Should you fail to pay as directed, you must perform 3 hours of community service for each unpaid session.

You must submit to periodic polygraph testing at the discretion of the probation officer as a means to ensure that you are in compliance with the requirements of your supervision or treatment program and pay any

costs associated with testing as required by the U.S. Probation Office.

You must submit to periodic psycho-physiological assessments and/or testing for the purpose of sex offender evaluation through the sex offender treatment provider at the discretion of the probation officer. You must pay any costs associated with the assessment and/or testing.

You must not have contact of any kind with children under the age of 18 unless supervised by an adult approved by the probation officer.

You must not purchase, possess, have contact with, or otherwise use any device that can be connected to the Internet or used to store digital materials, other than that approved by the U.S. Probation Office. You must allow the U.S. Probation Office to install software on any approved device that is designed to record any and all activity on the device the defendant may use, including but not limited to capture of keystrokes, application information, Internet use history, e-mail correspondence, pictures, and chat conversations. You will pay any costs related to the monitoring of their authorized device and must advise anyone in your household that may use any authorized device in question that monitoring software has been installed. If you need access to an employer owned Internet-equipped device for employment purposes, you must advise your probation officer before using the device. The probation officer will ensure your employer is aware of your criminal history, and you must agree to use the device for work purposes only.

You must not attempt to remove, tamper with, or in any way circumvent the monitoring software.

You must disclose all on-line account information, including user names and passwords, to the U.S. Probation Office. You must also, if requested, provide a list of all software/hardware on your computer, as well as telephone, cable, or Internet service provider billing records, and any other information deemed necessary by the probation office to monitor your computer usage.

You must also refrain from the purchase, possession, or use of digital cameras; digital recorders; or any other type of recording and/or photographic equipment.

You must not possess or view any images in any form of media or in any live venue that depicts sexually explicit conduct. For the purpose of this special condition of supervision, the term "sexually explicit conduct" is as defined under 18 U.S.C. § 2256(2)(A) and is not limited to the sexual exploitation of children. You must provide the probation officer with access to any requested financial information to determine if you have purchased, viewed, or possessed sexually explicit material.

You must submit to a search of your person, property, house, residence, vehicle, papers, computer, other electronic communication or data storage devices or media, and effects at any time, with or without a warrant, by any law enforcement or probation officer with reasonable suspicion concerning unlawful conduct or a violation of your conditions of supervision.

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments page.

	Assess-ment	Restit-ution	Fine	AVAA Assess-ment*	JVTA Assess-ment**
TOTALS	$300.00	$.00	$.00	$10,000.00	$.00

☐ The determination of restitution is deferred until An *Amended Judgment in a Criminal Case (AO245C)* will be entered after such determination.

☐ The defendant must make restitution (including community restitution) to the following payees in the amount listed below.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment. However, pursuant to 18 U.S.C. § 3664(I), all nonfederal victims must be paid before the United States is paid.

---

* Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018, Pub. L. No. 115-299.

** Justice for Victims of Trafficking Act of 2015, Pub. L. No. 114-22.

*** Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

☐ Restitution amount ordered pursuant to plea agreement $

☐ The defendant must pay interest on restitution and a fine of more than $2,500, unless the restitution or fine is paid in full before the fifteenth day after the date of the judgment, pursuant to 18 U.S.C. § 3612(f). All of the payment options on the schedule of payments page may be subject to penalties for delinquency and default, pursuant to 18 U.S.C. § 3612(g).

☐ The court determined that the defendant does not have the ability to pay interest and it is ordered that:

☐ the interest requirement is waived for the ☐ fine ☐ restitution

☐ the interest requirement for the ☐ fine ☐ restitution is modified as follows:

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

A ☒ Lump sum payments of $ 10,300.00 due immediately, balance due

☐ not later than , or

☒ in accordance ☐C, ☐D, ☐E, or ☒F below; or

B ☐ Payment to begin immediately (may be combined with ☐C, ☐D, or ☐F below); or

C ☐ Payment in equal ___ *(e.g., weekly, monthly, quarterly)* installments of $ ___ over a period of ___ *(e.g., months or years)*, to commence ___ *(e.g., 30 or 60 days)* after the date of this judgment; or

D ☐ Payment in equal ___ *(e.g., weekly, monthly, quarterly)* installments of $ ___ over a period of ___ *(e.g., months or years)*, to commence ___ *(e.g., 30 or 60 days)* after release from imprisonment to a term of supervision; or

E ☐ Payment during the term of supervised release will commence within ___ *(e.g., 30 or 60 days)* after release from imprisonment. The court will set the payment plan based on an assessment of the defendant's ability to pay at that time; or

F ☒ Special instructions regarding the payment of criminal monetary penalties:
It is ordered that the Defendant shall pay to the United States a special assessment of $300.00 for Counts 1, 2 and 3 , which shall be due immediately. Said special assessment shall be paid to the Clerk, U.S. District Court.

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

- ☐ Joint and Several
  See above for Defendant and Co-Defendant Names and Case Numbers *(including defendant number)*, Total Amount, Joint and Several Amount, and corresponding payee, if appropriate.
  - ☐ Defendant shall receive credit on his restitution obligation for recovery from other defendants who contributed to the same loss that gave rise to defendant's restitution obligation.
- ☐ The defendant shall pay the cost of prosecution.
- ☐ The defendant shall pay the following court cost(s):
- ☐ The defendant shall forfeit the defendant's interest in the following property to the United States:

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) AVAA assessment, (5) fine principal, (6) fine interest, (7) community restitution, (8) JVTA Assessment, (9) penalties, and (10) costs, including cost of prosecution and court costs.

ADDITIONAL FORFEITED PROPERTY

a. Asustor Model AS5110T Network Area Storage device, bearing serial number AS15115110TM0040FG;

b. Asustor Model AS5110T Network Area Storage device, bearing serial number AS15035110TM0115FG;

c. Asustor Model AS5110T Network Area Storage device, bearing serial number AS15035110TM0087FG;

d. Lenovo ThinkPad P70 laptop computer, bearing serial number PC09YBZR and containing a Samsung 2TB SSD with serial number 52HCNWAG801268L;

e. White Motorola Verizon 4G cellular phone;

f. SanDisk Ultra 128GB micro SD card, bearing serial number 4491DM18T08M;

g. Lenovo ThinkPad Z61p laptop computer, bearing serial number L3- AF74107/03;

h. Lenovo ThinkStation E32 desktop computer, bearing serial number MJ003G8Y;

I. Compaq StorageWorks SAN Array 1000 server, bearing serial number EB688A1X3TH07R;

j. Compaq server, bearing serial number 9J13FLW1L3FS;

k. HP server, bearing serial number 9J32JN71B6F3;

l. Compaq server, bearing serial number 9J1BDFD1GBM6;

m. Compaq server model DA-55NJA-FA, bearing serial number NI94206101; and

n. HP server model A7566A, bearing serial number USE052002H.

APPENDIX C

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

No. 4:19-cr-241
Judge Mazzant

[Filed June 11, 2021]

UNITED STATES OF AMERICA	)
	)
v.	)
	)
CLAY MELTON DENTON	)
	)

VERDICT OF THE JURY

COUNT ONE

As to the offense charged in Count One of the first superseding indictment, we, the Jury, find CLAY MELTON DENTON:

○ Guilty _____ Not Guilty

COUNT TWO

As to the offense charged in Count Two of the first superseding indictment, we, the Jury, find CLAY MELTON DENTON:

○ Guilty _____ Not Guilty

COUNT THREE

As to the offense charged in Count Three of the first superseding indictment, we, the Jury, find CLAY MELTON DENTON:

○ Guilty _____ Not Guilty

June 11, 2021
Date

_____
FOREPERSON

APPENDIX D

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN, TEXAS

CAUSE NO. 4:19-CR-00241
(ECF)

[Filed June 1, 2021]

UNITED STATES OF AMERICA	)
	)
VS.	)
	)
CLAY MELTON DENTON	)
	)

PROPOSED JURY INSTRUCTION

Comes now the Defendant, Clay Denton, by and through undersigned counsel, and, pursuant to the Court's Pretrial Order, submits this proposed jury instruction and would show the following:

1. <u>Spoilation of Evidence</u>

In this case, evidence has been received which the Defendant contends shows that electronically stored information existed that should have been preserved but was lost because the government failed to take reasonable steps to preserve it and it cannot be restored or replaced. If you find, by a preponderance of the evidence, that the government or its agents

destroyed or caused to be destroyed such evidence by acting negligently, recklessly, or by acting in bad faith, you may assume that such evidence would have been favorable to the defense. You may give any such inference whatever force or effect as you think it appropriate under all the facts and circumstances.[1]

A "preponderance of the evidence" means that you find that something it is more likely true than not true.

A party acts "negligently" when the party does an act that a reasonably prudent person would not do, or fails to do something that a reasonably prudent person would do under the same or similar circumstances to preserve available evidence.

A party acts "recklessly" when the party is aware of, but consciously disregards relevant facts and circumstances pertaining to the preservation of available evidence.

A party acts in "bad faith" when its conduct in failing to preserve available evidence is intentional.

2. <u>Authority</u>

"The adverse inference instruction has been called 'the oldest and most venerable remedy' for spoilation' and is perhaps the most common remedy in federal

---

[1] *See Mali v. Federal Ins. Co.*, 720 F.3d 387 (2d Cir. 2013); *see also United States v. Laurent*, 607 F.3d 895 (1st Cir. 2010); *United States v. Wise*, 221 F.3d 140 (5th Cir. 2000).

courts for the loss or destruction of evidence."[2] "A 'spoilation' instruction, allowing an adverse inference, is commonly appropriate in both civil and criminal cases where there is evidence from which a reasonable jury might conclude that evidence favorable to one side was destroyed by the other." *United States v. Laurent*, 607 F.3d 895, 902 (1st Cir. 2010) (citing *Modern Federal Jury Instructions § 75.01*); *see also United States v. Wise*, 221 F.3d 140, 156 (5th Cir. 2000) ("A district court has discretion to admit evidence of spoilation and to instruct the jury on adverse inferences). In *Wise*, Fifth Circuit affirmed the denial of an adverse-inference instruction because "the government did not destroy [the] computer; in fact, the computer was not even in the government's custody." *Id* at 156-57. Here, testimony during a pretrial hearing on the defendant's motion to dismiss the indictment, establishes that the computer was in the government's custody when they sought to execute a search warrant and it was during such execution that electronically stored information was irretrievably lost because government agents failed, for example, to retrieve all system interfaces (e.g. switches and routers). The evidence also demonstrates that government agents did not follow their own procedures for electronic data collection as outlined in their affidavit in support of the search warrant.

There is a split among the circuits with regard to what must be shown to support a request for an

---

[2] Hon. Shira A. Sheindlin and Natalie M. Orr, *The Adverse Inference Instruction After Revised Rule 37(e): An Evidence-Based Proposal*, 83 Fordham L. Rev. 1299 (2014).

adverse inference instruction.[3] *See Laurent*, 607 F.3d 895 at 902-03 ("the instruction usually makes sense only where the evidence permits a finding of bad faith destruction; ordinarily, *negligent* destruction would not support the logical inference that the evidence was favorable to the defendant…But the case law is not uniform in the culpability needed for the instruction and, anyway, unusual circumstances or even other policies might warrant exceptions."); *see also Stocker v. United States*, 705 F.3d 225, 235 (6th Cir. 2013) ("The requisite 'culpable state of mind' may be established through a 'showing that the evidence was destroyed knowingly, even if without an intent to breach a duty to preserve it…"), *Hodge v. Wal-Mart Stores, Inc.*, 360 F.3d 446, 450 (4th Cir. 2004) (holding that an adverse inference may not be drawn from merely negligent loss or destruction but requires a showing that willful conduct – something less than bad faith – resulted in the loss or destruction); *Sacramona v. Bridgestone/Firestone, Inc.*, 106 F.3d 444, 447 (1st Cir. 1997) ("Certainly bad faith is a proper and important consideration…But bad faith is not essential. If such evidence is mishandled through carelessness, and the other side is prejudiced, we think the district court is entitled to consider imposing sanctions, including

---

[3] "[T]he circuits employ widely divergent approaches with respect to the level of culpability required. About half the circuits requires a showing of bad faith before imposing a jury instruction. On the other end of the spectrum, some circuits permit an adverse inference instruction even in cases of ordinary negligence. Several circuits take an intermediate approach requiring more than negligence – i.e. knowledge or recklessness – but less than bad faith." *See* footnote 1.

exclusion of the evidence."); *Glover v. BIC Corp.*, 6 F.3d 1318, 1329 (9th Cir. 1993) ("a trial court also has broad discretionary power to permit a jury to draw an adverse inference from the destruction or spoilation against the party or witness responsible for that behavior."); *Mosaid Techs*, *Inc. v. Samsung Elecs. Co.*, 348 F.Supp. 2d 332, 335 (D.N.J. 2004) (holding that bad faith was not required for an adverse inference instruction as long as there was a showing of relevance and prejudice); *Residential Funding Corp. v. DeGeroge Financial Corp.,* 306 F.3d 99, 108 (2d Cir. 2002) ("The sanction of an adverse inference may be appropriate in some cases involving the negligent destruction of evidence because each party should bear the risk of its own negligence."); *Grosdidier v. Broad Bd. Of Governors,* 709 F.3d 19, 27 (D.C. Cir. 2013) ("the spoilation inference was appropriate in light of the duty of preservation notwithstanding the fact that the destruction was negligent.").

Here, the defendant submits that the facts and circumstances warrant an adverse inference instruction based on the government's failure to preserve available evidence negligently, recklessly or by acting in bad faith. In any event, unlike the circumstances of the *Wise* case*,* which involved a defendant who wiped out data on his own computer system by upgrading his operating system (after the government failed to seize the computer), here the government did evidence bad conduct by not following their own procedures and intentionally failing to secure the electronic data configuration. An instruction on this defensive theory is thus warranted and a failure to so instruct would effectively deny Mr. Denton the

opportunity to present his defense. Based on the foregoing, Mr. Denton respectfully requests that this Court include the proposed jury instruction in the Court's charge to the jury.

Respectfully submitted,

/s/ Bruce Anton
BRUCE ANTON
SBTN: 01274700

UDASHEN & ANTON
8150 N. Central Expressway
M1101
Dallas, Texas 75206
(214) 468-8100
(214) 468-8104 fax

Attorney for Clay Denton

CERTIFICATE OF CONFERENCE

I, the undersigned, hereby certify that on June 1, 2021, I conferred with Marissa Miller, Assistant United States Attorney, and she confirmed that the government is OPPOSED to the defendant's additional proposed jury instruction.

/s/ Bruce Anton
BRUCE ANTON

CERTIFICATE OF SERVICE

I, the undersigned, hereby certify that on June 1, 2021, the foregoing document was electronically filed with the clerk of court for the U.S. District Court,

Eastern District of Texas, using the electronic case filing system of the court. The electronic case filing system sent a "Notice of Electronic Filing" to the attorney of record for the Government by electronic means.

/s/ Bruce Anton
BRUCE ANTON

APPENDIX E

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

No. 4:19CR241
Judge Mazzant

[Filed April 15, 2021]

UNITED STATES OF AMERICA	)
	)
v.	)
	)
CLAY MELTON DENTON	)
	)

FIRST SUPERSEDING INDICTMENT

THE UNITED STATES GRAND JURY CHARGES:

Count One

Violation: 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (Distribution of Child Pornography)

On or about March 24, 2018, in the Eastern District of Texas, **Clay Melton Denton**, defendant, did knowingly distribute any child pornography, as defined in Title 18, United States Code, Section 2256(8), using any means and facility of interstate and foreign commerce, and that had been shipped and transported

in and affecting interstate and foreign commerce by any means, including by computer. Specifically, the defendant, **Clay Melton Denton**, using the Internet, peer-to-peer file sharing software, and a Lenovo ThinkPad P70 laptop computer, distributed the following visual depictions:

FILE NAME	DESCRIPTION
vichatter pthc 11yo ballerina nacked dance bate love it.wmv	This 8-minute 9-second video depicts a prepubescent female wearing a floral dress. The child pulls the dress up, dances and lifts her leg, all exposing her genitals to the camera, which is the focus of the video.
[redacted]Candygirls 13 Yo Nice Tits & Pussyhair 003.1St Studio Siberian-Mouses.avi	This 15-minute 3-second video depicts a pubescent minor female undressing and sitting nude on a couch. The minor female places a foreign object into her mouth and genitals

In violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2).

Count Two

Violation: 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (Receipt of Child Pornography)

On or about March 27, 2018, in the Eastern District of Texas, **Clay Melton Denton**, defendant, did

knowingly receive any child pornography, as defined in Title 18, United States Code, Section 2256(8), using any means and facility of interstate and foreign commerce, and that had been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Specifically, the defendant, **Clay Melton Denton**, using the Internet, peer-to-peer file sharing software, and a Lenovo ThinkPad P70 laptop computer, received the following visual depiction:

FILE NAME	DESCRIPTION
+ ! Lolitashouse – Yogirl-11 Yo-Poses Plays-With-Vibrator-Into-Pussy-Clu-003909.avi	This 9-minute, 57-second video depicts a nude pubescent minor female in a kitchen. The minor female rubs oil on her body and then inserts foreign objects into her mouth and genitals.

In violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1).

Count Three

Violation: 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (Possession of Child Po ography)

On or about April 25, 2018, in the Eastern District of Texas, **Clay Melton Denton**, defendant, did knowingly possess material, namely, an Asustor Model AS5110T Network Area Storage device, bearing serial

number AS15115110TM0040FG, that contained child pornography, as defined in Title 18, United States Code, Section 2256(8), involving a prepubescent minor and a minor who had not attained 12 years of age, that had been shipped and transported using any means and facility of interstate and foreign commerce; that had been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer; and that had been produced using materials that had been mailed and shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Included among the images and videos that the defendant, **Clay Melton Denton**, possessed were the following:

FILE NAME	DESCRIPTION
Fantasia Models – [redacted] 11 Yr) – [redacted] Strip Dance – (Children – Sf – Model) Pth [00:05:31].mpg	This 5-minute 31-second video depicts a pubescent female who removes her clothing, dances, and lays down on blue plaid bedding while displaying her anus and genitals to the camera, which are the focus of the video.
Pthc 2014-03 Tropical Cutie 2013093003103 6 (Good,Ride, 03) [redacted] prostitute bocas del tora panama	This 10-minute, 10-second video depicts a nude, prepubescent female who performs oral sex on an adult male's penis. The adult male then rubs and presses his erect penis into the prepubescent female's genitals.

DELILATINA FRYTURAMA 2da parte SUPER GOOD EXC.mpg	
(pthc)[redacted] wet (new rare).mpg	This 1-minute, 32-second video depicts a prepubescent female lying asleep with her buttocks exposed. With the camera closely focused, an adult male repeatedly rubs his finger over the female's vagina.
[redacted] play with and dad 3.avi	This 5-minute, 24-second video depicts two prepubescent females lying in a bed. The females remove each other's clothes and digitally penetrate each other's genitals. The females also rub a foreign object on each other's genitals and perform mutual oral sex.

In violation of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2).

NOTICE OF INTENTION
TO SEEK CRIMINAL FORFEITURE

Upon conviction of the offense(s) alleged in this First Superseding Indictment, the defendant, **Clay Melton Denton**, shall forfeit to the United States his interest in the following property, including, but not limited to:

1. Asustor Model AS5110T Network Area Storage device, bearing serial number AS15115110TM0040FG;

2. Asustor Model AS5110T Network Area Storage device, bearing serial number AS15035110TM0115FG;

3. Asustor Model AS5110T Network Area Storage device, bearing serial number AS15035110TM0087FG;

4. Lenovo ThinkPad P70 laptop computer, bearing serial number PC09YBZR and containing a Samsung 2TB SSD with serial number 52HCNWAG801268L;

5. Apple iPhone model A1662 cellular phone with a floral case, and bearing serial number 355435076079457;

6. White Motorola Verizon 4G cellular phone;

7. Apple iPhone 6+ model A1522 cellular phone with a brown case, and bearing serial number 354454067875998;

8. Apple iPhone 7 model A1778 cellular phone with a black case;

9. X-Box One model 1540 gaming console, bearing serial number 055415133748;

10. Alienware laptop computer, bearing service tag number 78FFWM1;

11. Nintendo WII handheld gaming system, bearing serial number JW711329889;

12. Western Digital external hard drive, bearing serial number WXK0A99X4251;

13. Verbatim flash drive, bearing serial number 150304279008G68AAS;

14. Micro SD HC 16GB card, bearing serial number 1021CZ597GH;

15. X-Box 120GB hard drive, bearing serial number 05210076564939;

16. X-Box 250GB hard drive, bearing serial number 0521014729137;

17. Western Digital My Passport for Mac external hard drive, bearing serial number WXD1A6472V60;

18. MacBook Pro laptop computer, bearing serial number C02HF0S8DV10;

19. Nextstar external 2.5" hard drive enclosure containing a hard drive and USB cord;

20. Apple 32 GB iPad Air model A1475 with an Otterbox case and bearing serial number F6QNX035F4YF;

21. Samsung 1TB external hard drive, bearing serial number 525CNYAG100586P and labeled "CLAY";

22. Apple MacBook Pro A1286 laptop computer, bearing serial number C02G30ZSSDF8Y;

23. "Park Place" thumb drive;

24. "Grindr.com/jobs" thumb drive;

25. SanDisk Ultra 128GB micro SD card, bearing serial number 4491DM18T08M;

26. HTC tablet computer with a leather case;

27. Seagate Backup Plus Port hard drive, bearing serial number NA75TXPF;

28. SONY VAIO tablet computer with a keyboard and red leather case, and bearing serial number VJ8WKB1;

29. X-Box 360 gaming console, bearing serial number 501592693705;

30. Apple iPad A1490 with black Otterbox case, and bearing serial number DLXLR5TBFLMQ;

31. Lenovo ThinkPad with ThinkPad case, bearing serial number MP-05SX0N;

32. Nintendo WII handheld gaming system, bearing serial number FW705916293;

33. Lenovo ThinkPad laptop computer, bearing serial number MP-127EMJ;

34. Samsung 1TB solid state drive, bearing serial number S21CNWAG203529P;

35. Lenovo ThinkPad laptop computer, bearing serial number MP11NG70;

36. Apple Mac mini computer, bearing serial number C07MJ252DWYL;

37. Floral hard drive;

38. Apple MacBook Pro A1278 laptop computer, bearing serial number W8027G67ATM;

39. IBM Deskstar 27.3GB hard drive, bearing serial number JRF09479;

40. OCZ Technology 128GB solid state drive, bearing serial number A20TX011247000670;

41. Fujitsu 160GB hard drive, bearing serial number K30VT7C27BTW;

42. Samsung 1TB solid state drive, bearing serial number S21CNSAG105249T;

43. Samsung 1TB solid state drive, bearing serial number S1D9NSAF528404M;

44. Lenovo ThinkPad T60P latop computer, bearing serial number L3-4F21H06/12;

45. Lexar 4GB Express Card SSD;

46. PNY 256GB SD card and Transcend card reader, bearing serial number 491196-3559;

47. Apple Mac mini computer, bearing serial number C07LK07QD43H;

48. Lexar 3.0 USB thumb drive;

49. SanDisk 8GB Extreme III compact flash drive;

50. AData 32 Compact flash drive;

51. 23 assorted CDs;

52. Lenovo ThinkPad Z61p laptop computer, bearing serial number L3-AF74107/03;

53. X-Box One model 1540 gaming console, bearing serial number 194119334748;

54. Hitachi Travelstar 60GB hard drive, bearing serial number 07N8365;

55. Hitachi Travelstar 60GB hard drive, bearing serial number M4J7Z80B;

56. Venus T5 mini raid tower, bearing serial number 10032258JMR0099 (containing 5 hard drives);

57. Lenovo Think Center model M93P desktop computer, bearing serial number MJ003DT1;

58. Hitachi 40GB hard drive, bearing serial number 11S07N9673ZJ1TY0DMJK3H;

59. Western Digital My Passport Ultra external hard drive, bearing serial number WX51AC4DEZKJ;

60. Western Digital My Passport external hard drive, bearing serial number WX51C1029503;

61. Western Digital My Passport external hard drive, bearing serial number WX31A33J8230;

62. Seagate 4TB hard drive, bearing serial number NA7F1WGR;

63. Fujitsu 120GB hard drive, bearing serial number NZ2YT81266HM;

64. Hitachi external hard drive, bearing serial number BX5Y775324;

65. Samsung 340GB solid state drive, bearing serial number S2NNNCAGC00490M;

66. Samsung 1TB solid state drive, bearing serial number S21CNWAFC26799J and a post-it labeled "Bad";

67. Samsung 340GB solid state drive, bearing serial number S2NNNCAGC00424Z;

68. Crucial solid state drive, bearing serial number 132909465817;

69. Crucial solid state drive, bearing serial number 13290946A9BD;

70. Lenovo ThinkStation E32 desktop computer, bearing serial number MJ003G8Y;

71. Patriot 4GB thumb drive with label "W10";

72. Compaq StorageWorks SAN Array 1000 server, bearing serial number EB688A1X3TH07R;

73. Compaq server, bearing serial number 9J13FLW1L3FS;

74. HP server, bearings Serial number 9J32JN71B6F3;

75. Compaq server, bearing serial number 9J1BDFD1GBM6;

76. Compaq server model DA-55NJA-FA, bearing serial number NI94206101; and

77. HP server model A7566A, bearing serial number USE052002H.

This property is forfeitable pursuant to 18 U.S.C. § 2253(a) based upon the property being:

1. any visual depiction described in section . . . 2252 of this chapter, or any book, magazine, periodical, film, videotape, or other matter which contains any such visual depiction, which was produced, transported, mailed, shipped or received in violation of this chapter;

2. any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from such offense; or

3. any property, real or personal, used or intended to be used to commit or to promote the commission of such offense.

By virtue of the commission of the offense alleged in this First Superseding Indictment, any and all interest the defendant has in this property is vested in and forfeited to the United States pursuant to 18 U.S.C. §§ 2253(a)(1), (a)(2), and (a)(3).

A TRUE BILL

/s/
GRAND JURY FOREPERSON

NICHOLAS J. GANJEI
ACTING UNITED STATES ATTORNEY

/s/ Marisa J. Miller Date: 4/14/21
MARISA J. MILLER
Assistant United States Attorney

APPENDIX F

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

No. 4:19CR241
Judge Mazzant

[Filed April 15, 2021]

UNITED STATES OF AMERICA	)
	)
v.	)
	)
CLAY MELTON DENTON	)
	)

NOTICE OF PENALTY

Counts One and Two

Violation:	18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1)
Penalty:	Imprisonment for not less than five years and not more than twenty years; but if the defendant has a prior conviction under this chapter, section 1591, chapter 71, chapter 109A, chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual

abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography or sex trafficking of children, such person shall be imprisoned for not less than fifteen years and not more than forty years; a fine of not more than $250,000; and a term of supervised release of not less than five years to life.

Special Assessment: $ 100.00

JVTA Assessment: $ 5,000.00

Count Three

Violation: 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2)

Penalty: Imprisonment for not more than ten years; but if any image of child pornography involved in the offense involved a prepubescent minor or a minor who had not attained 12 years of age, such person shall be imprisoned for not more than twenty years; and, if the defendant has a prior conviction under this chapter, section 1591, chapter 71, chapter 109A, chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or

under the laws of any State relating to aggravated sexual abuse, sexual abuse, or abusive sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography or sex trafficking of children, such person shall be imprisoned for not less than ten years and not more than twenty years; a fine of not more than $250,000; and a term of supervised release of not less than five years to life.

Special Assessment: $ 100.00

JVTA Assessment: $ 5000.00

APPENDIX G

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN, TEXAS

CAUSE NO. 4:19-CR-00241
(ECF)

[Filed July 2, 2020]

UNITED STATES OF AMERICA	)
	)
VS.	)
	)
CLAY MELTON DENTON	)
	)

MOTION FOR DISMISSAL OF INDICTMENT

Comes now the Defendant, Clay Denton, by and through undersigned counsel, and pursuant to Fed. R. Crim. P. 12(b)(2) and (3), and 7(c)(2), respectfully requests that the Court dismiss the indictment because the government's misconduct in preserving evidence prevents Mr. Denton from presenting a defense to the charges and would show the following:

I. I. Statement of the Case

On September 11, 2019, Mr. Denton was charged by indictment with three counts of receiving and distributing child pornography. The indictment stems from a search conducted a search of Denton's home,

pursuant to a search warrant, in April 2020. In executing the search warrant, numerous electronic devices were taken from Mr. Denton's residence.

At the time the warrant was requested, the government agents well knew that Mr. Denton had operated and was in possession of business grade systems. The agent's search warrant specified that after an investigation involving downloading files from a P2P network, agents conducted the following investigation regarding the target IP address:

> "A search of the American Registry for Internet Numbers (ARIN) online database indicated that IP address 173.74.245.82 is registered to the Internet Service Provider MCI Communications Services, Inc. d/b/a Verizon. ARIN further detailed the IP net range of 173.74.245.80 through 173.74.245.87 was assigned to customer DS Services, 4503 Boulder Drive, Allen, Texas, with a registration date of July 27, 2009. FBI personnel issued an administrative subpoena to Frontier Communications to obtain subscriber records for the subscriber of IP address 173.74.245.82 between January 2, 2018 at 8:38 p.m. CT and January 15, 2018 at 4:11 p.m. CT. Frontier Communications responses to the administrative subpoena, identifying the subscriber of the IP address as DS Services at the SUBJECT PREMISES (4503 Boulder Drive, Allen, Texas 75002).
>
> Your affiant has searched various records indices for information regarding Clay Denton,

DS Services, and the SUBJECT PREMISES, and observed the following:

a. Open source internet queries indicated an individual named Clay M. Denton was the President/Director of DS Services, a company specializing in clustering technology on various platforms, cluster design, diagnosis and tuning. Clay Denton was listed as an HP Certified Professional in Alpha Server and Open VMS systems and had a listed address of 4503 Boulder Drive, Parker, Texas (the SUBJECT PREMISES).

b. A review of public records databases revealed that Clay Melton Denton is currently associated with the SUBJECT PREMISES. Other individuals associated with the SUBJECT PREMISES appeared to be Clay Denton's wife and teenaged children.

c. Texas Department of Motor Vehicles records for Clay Denton reflect that he resides at the SUBJECT PREMISES, as of September 1, 2017, when he last updated his records."

The description used in the warrant establishes that the agents read Mr. Denton's website. The website describes genus of the devices and operating systems used. The agents knew, for example, that Mr. Denton had one or more HP storage area networks, and HP enterprise class servers. The search team should have been prepared to seize and preserve such devices.

In fact, Mr. Denton had configured the system into multiple zones protected by perimeter firewalls. This

configuration isolated the network devices from the internet. Within these zones, all systems were presumably trusted. Materials downloaded from the internet were initially routed through an ethernet switch and then channeled into one of two zones, but primarily a Version owned router. Mr Denton's computer and storage framework encompassed literally dozens of devices and nearly one hundred terabytes of data.

The immense storage available on the Denton computer system and the highspeed internet link made it a valuable target for hackers who wished to surreptitiously store files. *See* Exhibit A. In addition, Mr. Denton's experience with government agencies working on classified materials made the system potentially more attractive to hackers.

The agents who conducted the search were, or should have been aware, that the execution of search warrant on a business configuration would be much different that simply seizing aa few computers from a private residence.

Nonetheless, when the agents executed the warrant, they randomly, and inexplicably seized various devices while ignoring others. *See* Exhibit B. (For example, government agents seized a Nintendo Game Boy, a device which has no ability to connect to the internet and no storage capacity). Upon first glance at the configuration the agents knew or should have known that precautions needed to be taken before the devices were removed and transported. The agents made no effort to preserve or map the manner in which the devices interfaced. The agents failed to document or

capture the cable connections and configuration of the SAN switch and controllers before disconnecting them and failed to provide for maintaining a battery backup.

When the agents took the devices to the FBI lab for inspection, they found that the amount of storage was so immense that they could not analyze it by making computer images. Nor did they attempt to reconstruct the configuration at the lab. Nor could they have done so because they left important elements of the configuration at the Denton home. Thus, chain of custody of the data was not preserved, making reconstruction now impossible.

The result is that, while the government can identify images on some of the devices, and may be able to show the date of download, they cannot specify the manner in which this was done. Nor can they identify the person performing the download. They cannot, for example, rule out the possibility that the files were manipulated by remote access.

The set-up of the system could allow a hacker, who had stolen Denton's credentials, to log into the system remotely. Once in, the hacker could create, access and manipulate files. A sophisticated hacker, once logged in, could store, share and delete files without leaving a trace of the remote access on the compromised device. The system would incorrectly show that Mr. Denton was the user.

This activity could have been discovered by reviewing the activity logs of the Verizon owned router. The logs would show the source IP of the accessing device, the date and time of access, and the internal

device IP address and port, and perhaps even the credentials of user. The activity logs were stored on a VMS cluster. But because the agents dismantled the cluster, and seized parts thereof, the logs have been irrevocably lost. Once the array had been powered down, the configuration lost and not fully restored fairly quickly, the backup batteries have failed and the logs cannot be retrieved. *See* Exhibit C.

This material, which is the crux the defense, is not available to the defense team. The Government undoubtedly disputes that hacking occurred, but has destroyed the only manner the defense has of proving it did occur.

Access to the materials was only permitted to the defense team's expert, Dan James. He is required to request specific copies. He cannot even attempt to reconfigure the devices held at the lab. With the access the defense team is permitted, the activity logs are not available. When agents executed the search warrant, they disconnected and powered off the router causing all data on the active systems or controls in memory on the router to be lost. The logs, if preserved, could and would show attempts by hackers to invade the system. With those logs, the defense could show that the system was hacked. Such evidence would be critical to establish what computers had been compromised. On information and belief, the FBI has seized and properly preserved much larger configurations than the instant one. The agency had the training and experience necessary to properly move, preserve and restore the configuration. Without justification, they simply refused to do so.

II. Motion to Dismiss

Due Process guarantees Mr. Denton the right to a fair trial and such right requires "that criminal defendants be afforded a meaningful opportunity to present a complete defense. *California v. Trombetta*, 467 U.S. 479, 485 (1984). Due Process is violated whenever the government withholds material exculpatory evidence. *Illinois v. Fischer*, 540 U.S. 544, 547 (2004) (citing *Brady v. Maryland*, 373 U.S. 83 (1963)) Due process is violated if the government fails to preserve evidence, which possessed apparent exculpatory value. *Trombetta*, 467 U.S. at 489. Likewise, if the government fails to preserve potentially exculpatory evidence due process is violated if the government is shown to have acted in bad faith. *Arizona v. Youngblood*, 488 U.S. 51, 57-58 (1988). Here, the government destroyed exculpatory or potentially useful evidence in violation of Mr. Denton's due process rights.

Here, the government cannot provide to the defendant, as he has requested, access to or forensic images of the exact configuration of the seized (and non-seized) equipment, which would provide access to exculpatory evidence showing remote access or hacking into the system pursuant to Denton's assertion of innocence. The electronic equipment and data contained within these systems is clearly material and "might be expected to play a significant role in [Denton's] defense." *Trombetta*, 467 U.S. at 488-49. The agents were on notice that electronic data would be focal point of a case involving an internet offense. The government's failure to properly seize the items,

document configuration, and failure to plan for a battery backup to prevent the loss of information after powering down the array, has irreparably harmed Denton's due process rights. The Supreme Court, in *Trombetta*, held that "the government violates the defendant's right to due process if the unavailable evidence possessed 'exculpatory value that was apparent before the evidence was destroyed, and [is] of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means." *United States v. Cooper*, 983 F.2d 928, 931 (9th Cir. 1993) (affirming dismissal of an indictment where the government failed to preserve laboratory equipment seized from defendant charged with manufacturing methamphetamine); *see also United States v. Bohl*, 25 F.3d 904 (10th Cir. 1994) (reversing district court and finding that defendant's due process rights were violated by the destruction of potentially exculpatory evidence and the remedy was dismissal of the indictment). Here, it would have been apparent to agents that the means of proving that the illegally downloaded files came from a foreign/outside/hacking source would be contained within the configuration, stored data, and logs of the electronic data seized the same as proving lab equipment's inability to make methamphetamine would be apparent in the equipment. *Id.* Like the laboratory equipment in *Cooper*, here no other evidence can support Denton's assertion of innocence i.e. that it was not him but someone with hacking or remote access to his systems configuration that downloaded any illegal files. *Id.*

That agents did not map or seize the configuration as is, work to reconfigure it, or maintain the battery so that data would not be lost. "*Youngblood's* bad faith requirement dovetails with the first part of the *Trombetta* test: that the exculpatory value of the evidence be apparent before its destruction. The presence or absence of bad faith turns on the government's knowledge of the apparent exculpatory value of the evidence at the time it was lost or destroyed." *Id* (citations omitted). That agents did not map or seize the configuration as is, work to reconfigure it, or maintain the battery so that valuable data would not be lost shows bad faith. The agents knew, according to their own search warrant, that the system they would find at Denton's home was not a typical residential operating system. Rather, they did, or reasonably should have, anticipated a system which hosted an OpenVMS operating system an HP StorageWorks storage arrays even just based on Denton's company's website.[1] Agents had an obligation to prevent the spoliation of this evidence by bringing an analyst or expert familiar with enterprise class systems and the OpenVMS operating system. Such a person would have known to document cable connections and the configuration of the SAN switch and controllers and maintain a battery backup to prevent the loss of data from this sophisticated system. Thus, even if this Court finds that the unavailable evidence contains only potentially useful evidence, bad faith has been established on the part of the agents who encountered

---

[1] Based just on the information on the website, a forensic analyst should have expected to see some combination of RA7000, RA8000, MSA and/or HSV storage arrays.

a sophisticated system and just randomly seized electronics without maintaining the configuration, battery power, and router to prevent data loss.

III. Conclusion

For the foregoing reasons Defendant, Clay Denton, respectfully asks this Court to set this matter for an evidentiary hearing to allow for the presentation of expert testimony regarding the spoliation of evidence in the context of Denton's class systems configuration and for an order dismissing the indictment.

Respectfully submitted,

/s/ Bruce Anton
BRUCE ANTON
SBTN: 01274700

UDASHEN & ANTON
2311 Cedar Springs Road
Suite 250
Dallas, Texas 75201
(214) 468-8100
(214) 468-8104 fax

Attorney for Clay Denton

CERTIFICATE OF CONFERENCE

The undersigned counsel certifies that he has communicated to Marisa Miller, Assistant United States Attorney, and she opposes this motion.

/s/ Bruce Anton
BRUCE ANTON

CERTIFICATE OF SERVICE

I, hereby certify that on July 3, 2020, I electronically filed the foregoing document with the clerk of court for the U.S. District Court, Eastern District of Texas, using the electronic case filing system of the court. The electronic case filing system sent a "Notice of Electronic Filing" to the attorney of record for the Government by electronic means.

/s/ Bruce Anton
BRUCE ANTON

EXHIBIT A

Written by Jeff Stone
JAN 28, 2019 | CYBERSCOOP

An online marketplace that facilitated more than $68 million in fraud and cybercrime has been shut down following an international law enforcement operation, the U.S. Department of Justice announced Monday.

Hackers and thieves used the website, known as xDedic, to sell access to compromised computers located around the world and personal information belonging to U.S. residents, prosecutors said. Buyers could search the site by price, operating system or by the geographic region from where it was stolen, prosecutors said. The method of access was usually through credentials for Remote Desktop Protocol (RDP) servers.

The DOJ didn't name any victims, but said they included major metropolitan transit organizations, emergency services, government agencies, pension funds, universities and others.

The site was shut down in 2016, only to re-emerge soon after on the dark web with the new stipulation that members pay $50 to enter.

"The xDedic marketplace operated across a widely distributed network and utilized bitcoin in order to hide the locations of its underlying servers and the identities of its administrators, buyers, and sellers," the DOJ said in a statement.

No arrests were reported as part of the operation. U.S. authorities worked closely with law enforcement in Belgium, Ukraine and the European police agency Europol to orchestrate the takedown.

The xDedic site first entered the public consciousness in 2016 when security researchers from Kaspersky Lab showed that the site offered access to hacked servers from well known sites including Target and PayPal. By promising to let its users into such known websites via an easy-to-understand search function, xDedic lowered the barrier to entry for wannabe cybercriminals, Kaspersky said. For example, purchasing access to a European country's network would have cost a buyer $6 at the time.

"The one-time cost gives a malicious buyer access to all the data on the server and the possibility to use this access to launch further attacks," reported SecureList, Kaspersky's blog. "It is a hacker's dream, simplifying access to victims, making it cheaper and faster, and opening up new possibilities for both cybercriminals and advanced threat actors."

-In this Story-

EXHIBIT B

INVENTORY OF COMPUTERS REMOVED FROM THE HOUSE

Quantity	Description
5	IBM Thinkpad Laptops
*1	Lenovo Thinkpad Tablet
*4	Lenovo ThinkStation desktop
*1	Lenovo ThinkCentre desktop
1	VXT2000 Terminal
4	Compaq Alphaserver DS10L
3	Compaq Alphaserver DS10
11	DECpc 433
3	VAXstation 4000
2	Compaq Alpha Server DS20
3	Clone PC
2	Digital VT LAN 40 Terminal
1	IBM Terminal
1	Compaq Professional workstation
6	DEC 3000
1	Apple iMac
1	Digital VAX 4000
1	Clone Server
1	Compaq Alphaserver ES40
*1	HP Proliant Server
1	Compaq Alphaserver DS20E
1	Compaq Alphaserver ES45
1	Digital Laptop
1	Compaq Laptop
*1	Apple Macbook Pro
*1	iPhone XS Max
*1	iPad Mini 5

NON Computers

*1	Drobo B1200i Storage Array
*1	HP D2700 Storage Array
4	HP SAN Switches

* Items purchased after home seized April 25, 2018

EXHIBIT C

Overview

As a complete business system and network were merged into a home location, many things were set up in a way that would not be typical of a home network.

Verizon Router

All communication from internal systems except for the OpenVMS cluster routed to the Internet through a Verizon/Frontier provided router. This router managed the last 4 of the 5 static IP addresses from the business class Internet service. All internal systems would NAT through this device so that any outgoing or return traffic would show one of the static IP addresses as being the source or destination IP address for all Internet traffic, including the traffic observed during the investigation. Any static PAT rules, including external access to a remote connection, P2P software using uPnP, and all dynamic PAT rules would be configured on this router, which was also acting as the external firewall for all systems using it as a default gateway. Static PAT rules (if any) would be stored in local flash memory on the router, and dynamic rules would be in memory on the router.

All connections, including all internal computers that might have been running P2P software could be identified on this router. All dynamic entries would be maintained as long as the router was powered on, and static entries would be stored in local flash. This information is critical in understanding and documenting which computers were open to remote access and control, and which computers were running

P2P software. This router was also configured to forward its log files via syslog to the OpenVMS cluster (described later). These logs would include information about unsuccessful attempts to access the network or router, any changes to entries in the static NAT and PAT entries, and uPnP entries created by software that wanted to open outside ports for connection back into systems on the internal network.

When the agents executed the search warrant, they disconnected and powered off the router to isolate systems in the house from the Internet. When this was done, all data on active systems or controls in memory on the router were irrevocably lost. This would be critical evidence to establishing what computers were compromised and accessing the Internet with unknown software or protocols, including remote access and P2P. Additionally, this router was not collected as evidence by the agents, breaking chain of custody for required evidence to understand who was connecting to what system from where.

After systems were seized, the Internet service was changed from business class service to residential service, as there was no longer a business as all assets had been seized. Frontier collected the router and replaced it with a residential model. As such, there is no longer a way to recover the static NAT and PAT entries stored on the router.

The agents did not collect the running configuration of the router before powering it off, nor did they collect the router as a part of the overall systems that were seized, even though they indicated they were collecting everything that was “plugged in”. The password to this

router was printed on a sticker on the side of it as it was provided by Verizon, so it would have been extremely easy to have collected and saved this evidence.

OpenVMS cluster

The OpenVMS cluster was comprised of two Digital/Compaq/HP AlphaServer Systems, these systems had no local storage but connected to a shared SAN for shared storage, and they also booted from the SAN. The cluster received security logs and authentication data from other internal systems as well as storing and processing its own security logs. The cluster connected to the internet via a dedicated Cisco ASA firewall and had multiple services open to the internet including a webserver, email servers, and FTP server. The cluster also ran ssh for secure remote access into the system. Out of band logs from other systems into the internal network were collected using a software package called Console works. Any unsuccessful attempts to log into the systems, denial of service attacks, etc. would be captured and logged by these systems. The cluster also ran an older microsoft windows server function called PathWorks. The software also allowed the cluster to participate as a member of a windows workgroup, because of this, most of the internal windows computers were configured to run an older less secured method of authentication, which is NTLM version 1.

When the agents seized the equipment, they only took the AlphaServer DS20 system, not the DS10 system. The configuration of the srm console on these systems

which show which one LUN and Path would have booted from.

SAN

The SAN switch that connected systems to storage was an EMC branded Brocade switch, this switch contained the zoning configuration for the SAN which managed which systems to connect to which storage. This switch was not seized by the agents.

The storage array is a Compaq/HP RA8000 with an HSG80 controller. The controller stores its configuration, metadata and LUN mappings in NVRAM, which is backed up by an alkaline coin cell battery. This battery is good for 3-5 years of shelf life when new, and many more years when the controller remains powered on. This controller was between 15 and 20 years old when it was seized. If it was not connected back to power within a short time after it was unplugged and relocated, it is likely that the battery will have not been able to maintain the array configuration. Without the array configuration it is not possible to map the LUNs to the LBNs on the disk drives, making it impossible to recover the data. Also, the battery maintains the license of the controller. If the license is lost, it is not possible to reconfigure the controller even if a backup was made of the original configuration. HP has not supported this controller in over 10 years, and does not have the systems in place any more to regenerate or recover the license for the controller to operate.

The HSG80 controllers were configured with write back cache for the LUNs and disk drives attached to improve

the performance of the array. The write back cache was protected by lead acid batteries attached to the controller. These batteries will maintain the data for up to 2 days if the array is unplugged without being shut down properly. The agents who seized the systems just pulled power from the equipment, improperly shutting it down and starting the run down of the cache batteries. As these batteries were not new, the array would need to have been reconnected to power within hours of being disconnected. As this was not done, the write back cache was corrupted on the array. This causes a loss of data, meaning that powering up the array and entering this command: