WO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

United States of America, Plaintiff, v. Michael Lacey, et al., Defendants.	No. CR-18-00422-PHX-SMB **ORDER**

Pending before Court is Defendants Motion to Compel Discovery. (Doc. 643., "Mot.") The Government filed a Response, (Doc. 696, "Resp."), and Defendants filed a Reply, (Doc. 717, "Reply"). Oral argument concerning the manner and usability of the Government's discovery disclosures was held on October 3, 2019, (Doc. 789), October 25, 2019, (Doc. 800), and December 2, 2019 (Doc. 832). At the hearings, the Court heard testimony from Special Agent J. Patrick Cullen, William Gerken, Special Agent Matthew Frost, Agent Richard Robingson, and Tami Loehrs. The Court will deny the Motion because, as explained below, the Court finds that the disclosure of electronic data in this case was made in a reasonably useable format.

I. BACKGROUND

Defendants are former executives and employees of a classified ad website charged with conspiracy and facilitation of an unlawful activity under the Travel Act, Backpage.com ("Backpage"). The charges are outlined in a 100-count superseding indictment. (Doc. 231, "SI".) At issue in this discovery dispute is the form and functionality

of the disclosure of Backpage server data previously seized by the Government.[1]

a. The Backpage Website

The viewing of Backpage ads on the Website involved cooperation among various types of servers running on FreeBSD Unix operating systems.[2] (*See generally* Doc. 789 at 61-73; 82:5-8.) In a nutshell, *web servers* facilitated Backpage users' viewing requests by connecting *database server* information with *image server* information and displaying it in users' web browsers. (*Id.* at 63:24-64:17.) These web servers comprised a majority of Backpage's overall servers and evenly distributed requests by *helper servers* to ensure no particular server was overloaded by user traffic. (*Id.* at 63:19-22; 64:22-25; 65:1-5.)

Backpage used four database servers–one "master" and three "replicates"–containing identical information to store its website data. (*Id.* at 62:1-4, 22-25.) Images associated with ads were separately stored on three image servers[3] because it was not as "efficient to store them in a database." (*Id.* at 63:5-6.) The "master" database was "where data would get written to," while "the other [three databases] would replicate that information." (*Id.* at 62: 6-10.) "For example, "if somebody [were] posting an ad, . . . the data that they're posting gets saved to that master server [and] [i]f somebody is viewing an ad, the data that is being retrieved to view that ad comes from the replicated [server]." (*Id.* at 62:11-15.) By virtue of this replication, "[a]ll four servers would have the same information on them." (*Id.* at 62:6.)

In addition to holding identical information, each database server contained (1) market databases and (2) a central database. (*Id.* at 70:2-14.) Each central database "stores a subset of [an] ad across all of those market databases," (*id.* at 70:10-12) and permits an individual to "find a subset of ads or . . . where a user had posted different ads among the different geographical regions," (*id.* at 70:5-9). After looking in the central database, an individual "could go to the market databases for the particular [geographical] region and

[1] The scope of the Government's disclosures expands far beyond the narrow, but technical question before the Court here. Defendants do not challenge the Governments already extensive production of discovery. (*See* Resp. at 4-5.)
[2] An operating system manages a server's various hardware and software functions.
[3] There is a "record of those images in the master database server." (*Id.* at 67:15-16.)

find all the information about the ads posted[.]" (*Id.* at 71:10-13.)

With access to both the database and image servers, a party can use SQL "to access the information that was contained on [Backpage] before it was seized," (*id.* at 83:13-17), and "[a]ll of the content related to the ad," (*id.* at 69:6-7). *See id.* at 79:8-9 ("With just the database server and an image server, all of the data for an ad is there. So it is possible to query those databases, to pull up the information you need for an ad and to also retrieve the images that you need for that ad.")). In other words, even "if you got [Backpage] totally back[] [sic] up and running, . . . it might be more convenient to look at the data, but there wouldn't be any additional data than just what you could obtain from the manual queries[.]" (*Id.* at 80:15-24.)

Aside from what the Backpage servers contained, how the server data is also relevant. That is, the language and software Backpage utilized to operate bears on an assessment of the Government's current disclosure. The Backpage servers themselves employed an operating system ran a UNIX operating system called FreeBSD. (*Id.* at 18:1-5.) As its name suggests, FreeBSD is an open-source operating system available for download free of charge. (*Id.* at 170:1-3.) Operating systems manage the various hardware and software functions of a server, coordinates the servers' needs and allows it to function. An individual Backpage server, in turn, housed multiple physical hard drives that contained Backpage databases. The Backpage system also used "virtual machines" called "jails." (*Id.* at 82:5-14.) "Jails" virtually group databases together and allowed an administrator to easily move a group from server to server if required. (*Id.*) The Backpage databases used a ZFS file system. (*Id.* at 173:17-22.) This open source program controls how the data is stored within the database and allows the FreeBSD operating system to interact with that data. (*Id.* at 82:15-17.) As with the jails system, the ZFS file system similarly allowed data on hard drives to be grouped into something called "Z pools." (*Id.* at 174:14-22.)

b. Seizing Backpage's Servers

The Government seized Backpage's servers from three locations—thirty-two in Tucson, Arizona, nine in Amsterdam, Netherlands, and five in Dallas, Texas. (Doc. 643-5

at 2-3.) The Amsterdam and Phoenix servers contained almost identical information.[4] If the Phoenix servers failed, then the Amsterdam servers would act as a failsafe and ensure Backpage remained operational. FBI Special Agent J. Patrick Cullen assisted with seizing the Tucson servers on April 6, 2018 at Login Data Center ("Login") pursuant to an authorized seizure warrant. Although the servers were housed at Login, DesertNet operated them. Upon arriving at Login, Special Agent Cullen was informed DesertNet's assistance was required to conduct an orderly shutdown of the Backpage servers. (Doc 789 at 17:1-19, 24:3-6.) Will Gerken and a DesertNet system administrator arrived to assist. (*Id.* at 17:1-2.) As DesertNet's founder, Chief Technology Officer, and the lead software developer who created Backpage, Gerken is intimately familiar with Backpage's servers and the software they employed. Gerken conducted a "soft shutdown"[5] of both the Tucson and Amsterdam servers, safeguarding the integrity of the data they contained. (*Id.* at 25:1-12, 75:17-20, 76:13-19.) After properly identifying and documenting Backpage's servers and Gerken's "soft shutdown," the Government transported the Tucson servers to a controlled facility in Phoenix. (*Id.* at 25:3-8.) Although the Government did not document how the Backpage servers interacted with one another before seizure, there is no indication that any Backpage data was altered or damaged in any way.[6] (*See id.* at 27:1-3, 76:13-19.) Additionally, Gerken testified that he did not have a schematic drawing for the servers.

[4] The primary distinction being the Amsterdam servers also hosted the Payment Processing Island ("PPI") governing credit card transactions of Backpage users. The PPI was not controlled or designed by DesertNet. (Doc. 789 at 66:18-25.) Thus, specific information regarding a payment, "like the ad price or date and timestamps or transactional approval data" was not stored on databases controlled by DesertNet, but on the PPI. (*Id.* at 68:12-20.) "Some very basic rudimentary information, such as a real generic invoice just for statistic purposes that would be on the DesertNet managed Backpage database, but the accounting information would be on the PPI." (*Id.*)

[5] In distinguishing between the two primary options for a system shutdown, Special Agent Cullen described a soft shutdown as a normal shutdown of a computer where running programs gradually close, files being written can finish, and data is unharmed. (Doc. 789 at 22:25-23:1 ("it does that as the best way to preserve the file system from being corrupted.")). On the other hand, he likened a hard shutdown to "yanking the power cord out." (*Id.* at 23:2-3.)

[6] Special Agent Cullen's testimony demonstrates that the manner of seizure was motivated by a prioritization of data integrity over all else. (Doc. 789 at 28:10-15) ("it's kind of like a continuum of maximum evidence preservation on this side versus, in your example, convenience on this side. They are really at odds with each other and you have to try to balance the needs of everyone involved in preserving the evidence and getting the evidence out of those systems.")).

(*Id*. at 86:24-25, 87:1-4.)

Since seizing the Tucson servers, the Government has also seized Backpage's Dallas and Amsterdam servers.[7] The FBI transferred servers from these locations to various Special Agents for forensic examination—including Special Agent Matthew Frost—for processing, analysis, and production of discovery [production] pertinent to this case. (*Id.* at 158:12-18.) Special Agent Frost was called in because he has experience working with Linux/Unix systems. Frost made forensic images—exact, verified copies used for investigation—of Backpage's hard drives and databases, and provided them to Defendants. (*Id.* at 159: 10-11.) Special Agent Frost constantly engaged Gerken throughout this process to improve his understanding of Backpage's servers. (*Id*. at 219:14-16.)

c. Procedural Background

At a September 13, 2019 hearing set to address a variety of discovery disputes, Defendants argued the Government's discovery was not reasonably usable by comparing Exhibit J—raw Backpage ad data organized in a large spreadsheet—with Exhibit K—the administrator view of a Backpage ad from the fully-functional website referred to as an "object editor"—to demonstrate the inadequacy of the Government's discovery. (Doc. 761 at 32:1-19.) Repeating an argument from their Motion, Defendants proffered Exhibit J demonstrated the manifest issues with the Government's disclosure. Represented as the Government's disclosure of imaged data for a single Backpage ad, Defendants showed the Court a "series of spreadsheets, containing more than 500 data fields and cross-references to information and images contained in other files." (Mot. at 6.) Given the divergent, intransigent positions of both parties,[8] the Court ordered an evidentiary hearing to determine the form and functionality of the Governments disclosure. (*See* Doc. 761 at 32-47.)

---

[7] Transferring the Amsterdam servers from Dutch authorities to the FBI through the Mutual Legal Assistance Treaty ("MLAT") process is ongoing. (Doc. 643-5 at 3.)

[8] *Compare* Doc. 761 at 35:19-25 (characterizing the Government's disclosure as "just completely useless. It's incomplete. It's broken. There is nothing we can do with it.") *with id.* at 39:7-10 ("The bottom line is if that information was available at the time the website was seized and shut down, we've given that information to [Defendants in] the exact same format that we have it.").

Three days of evidentiary hearings followed. (*See* Doc. 789, "Oct. 3 Hearing"; Doc. 800, "Oct. 25th Hearing"; Doc. 832, "Dec. 2 Hearing.") Both parties' witnesses broadly testified concerning the seizures of the Backpage servers, how they operated, the Government's form of disclosure, and alternative forms of disclosure.

II. LEGAL STANDARD

Federal Rule of Criminal Procedure 16(a) governs discovery in criminal cases. Fed. R. Crim. P. 16; *see also United States v. Armstrong*, 517 U.S. 456, 461 (1996). Upon a defendant's request, the Rule requires the government to make available documents and other materials "within the government's possession, custody, or control" that are either "material to preparing the defense," or that the government intends to use in its case-in-chief. Fed. R. Crim. P. 16(a)(1)(E)(i); *see also United States v. Clegg*, 740 F.2d 16, 18 (9th Cir. 1984). "A defendant needn't spell out his theory of the case" to obtain discovery under Rule 16. *United States v. Hernandez-Meza*, 720 F.3d 760, 768 (9th Cir. 2013). "The test is not whether the discovery is admissible at trial, but whether the discovery may assist [the defendant] in formulating a defense." *United States v. Soto-Zuniga*, 837 F.3d 992, 1003 (9th Cir. 1992). Admittedly, "materiality is a low threshold," *Hernandez-Meza*, 720 F.3d 768, but requires more than conclusory statements attesting to materiality or general descriptions of the materials sought. *United States v. Cadet*, 727 F.2d 1453, 1468 (9th Cir. 1984) (holding a district court abused its discretion by granting discovery due to defendants "wholly conclusory showing and the great breadth of the discovery request"); *see also United States v. Marshall*, 532 F.2d 1279, 1285 (9th Cir. 1976) ("Such 'general descriptions of the materials sought and conclusory arguments as to their materiality have been *rejected repeatedly* as insufficient under Rule 16(b).'") (quoting *United States v. Ross*, 511 F.2d 757, 763 (5th Cir. 1975) (emphasis added).

Rule 16's disclosure requirements are broad, not limitless. Rule 16 confines the Government's duty to disclosure of information "material to the preparation of the defendant's defense or . . . intended for use by the government as evidence in chief at the trial, or were obtained from or belong to the defendant." Fed. R. Crim. P. 16(a)(1)(C). In

the context of Rule 16, "the defendants defense means the defendant's response to the Government's case in chief," limiting the Government's duties to disclose only that information "which refute[s] the Government's arguments that the defendant committed the crime charged." *See Armstrong*, 517 U.S. at 462 (rejecting that "the concept of a 'defense' includes any claim that is a 'sword,' challenging the prosecution's conduct of the case" applies to Rule 16) (citing Fed. R. Crim. P. 16(a)(1)(C)).

Additionally, the government has a duty to disclose exculpatory and impeachment evidence, including evidence "known only to police investigators and not to the prosecutor."; *Strickler v. Greene*, 527 U.S. 263, 281 (1999); *see also Brady v. Maryland*, 373 U.S. 83, 87 (1963); *Giglio v. United States*, 405 U.S. 150, 154 (1972). But *Brady* does not require the government to create exculpatory evidence that does not exist. *United States v. Monroe*, 943 F.2d 1007, 1011-12 n.2 (9th Cir. 1991) (citing *United States v. Sukumolachan*, 610 F.2d 685, 687 (9th Cir. 1980). "While the prosecution must disclose any [*Brady*] information within the possession or control of law enforcement personnel, it has not duty to volunteer information that it does not possess or of which it is unaware." *United States v. Hsieh Hui Mei Chen*, 754 F.2d 817, 824 (9th Cir.), *cert. denied*, 471 U.S. 1139, 105 S.Ct. 2684, 86 L.Ed.2d 701 (1985); *see also United States v. Gray*, 648 F.3d 562, 567 (7th Cir. 2011) (considering defendant's argument that "the government should . . . create and run programs to extract data from its database that would be useful to the defense" as a "non-starter" because "[i]t implies that the state has a duty not merely to disclose but also create truthful exculpatory evidence.") (internal quotation marks and citations omitted).

Regarding electronically stored information ("ESI"), the 2012 Administrative Office of the U.S. Courts report entitled "Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases" ("ESI Protocol") provides guidance. In relevant part, the ESI protocol recommends that (1) after conferral, "any format selected for producing discovery should maintain the ESI's integrity, allow for reasonable usability, and reasonably limit costs, and, if possible, conform to industry

standards for the format; and that (2) "[w]hen producing ESI discovery, a party should not be required to take on substantial additional processing or formatting conversion costs and burdens beyond what the party has already done or would do for its own case preparation or discovery production." ESI Protocol, Introduction at 1-2 (summarizing Principles 4 and 5). "ESI discovery should be done in a manner to facilitate electronic search, retrieval, sorting, and management of discovery information," ESI Protocol, Recommendations at 4, and, relevant here, "for complex ESI productions, each party should involve individuals with sufficient technical knowledge and experience to understand, communicate about, and plan for the orderly exchange of ESI discovery." ESI Protocol, Recommendations at 2.

III. DISCUSSION

At core, Defendants demand the Government revive Backpage.com, albeit in "read-only" form. (Doc. 643-13 at 2.) Defendants "ask the Court to compel the government to provide . . . access to Backpage's systems, servers, databases, and data, functioning as they did at the time of their seizure, or, alternatively, to recreate the databases and systems to allow functional access to the data and information as it existed at the time of the government's seizures." (Mot. at 7.) Defendants characterize the Government's disclosures to date as little more than "just a pile of disconnected data." (Mot. at 6.) Their expert, Tami Loehrs, likens the Government's discovery to "buying a large piece of unassembled furniture but realizing you don't have all the parts, or the instructions on how to build it, or pictures of the final product, or the specialty tools required for the proprietary hardware to put it all together." (Reply, Exh. A at 8.) Defendants characterizations are unsupported by the nearly fourteen hours of testimony from the fact and expert witnesses of both parties. That testimony established the Government's discovery is sufficient in scope and satisfies Defendants request for Backpage.com data in a "functional and operation format," just not the format they prefer. As explained below, given the demonstrable functionality of the Government's discovery at this point, Defendants fail to establish the need for a "read-only" version of Backpage.com, much less justify the significant cost and delay fulfilling their request would incur.

a. Evidentiary Hearing Findings

i. Data Integrity and Functionality

At the outset, the evidentiary hearings establish the Government has provided discovery in a reasonably usable format. DesertNet CTO Will Gerken described three primary options for disclosure of Backpage data: (1) disclosure of raw data for manual querying; (2) a "read-only" version of Backpage.com; and (3) a fully-functioning Backpage.com. (Doc. 789 at 79-80.) As Gerken himself attested, a fully-functioning Backpage.com may be impossible to reconstitute at this point. (*See id.* at 119:17-20) Creating a read-only Backpage.com, as discussed below, is costly, time-consuming, and of questionable functional value compared with a manual query system. (*Id.* at 120-124.)

Thus, the Government inadvertently ended up with option one and furnished Defendants with forensic images of the Backpage hard drives, specifically the drives that comprised Backpage's master database server and image servers. Using these servers, Defendants undeniably have access to all the data on Backpage.com at the time of seizure.[9] Recognizing that accessing the data from the forensic images takes some specific knowledge—familiarity with FreeBSD, the jails system, and the ZFS file system—the Government offered Defendants a shortcut and provided copies of each specific database in the Backpage servers. (*Id.* at 80-81.) Thus, to present the data in a readily digestible format, an expert retained by Defendants need only have familiarity with the ZFS file system and be conversant in SQL, the language used to query the databases. (*Id.* at 81-82.) Crucially, the data is identical in all three options.[10] (*Id.* at 80:4-14.)

The Government's disclosure is manifestly functional. Agent Frost demonstrated the effectiveness of the manual query format using multiple databases to search for terms relevant to the SI's charges during the evidentiary hearings. The examined databases

[9] This does not include all historical versions of an individual Backpage ad. Because Backpage did not use "versioning" and only saved the most updated version of an ad, the data only shows ads in the state they were seized. (Doc. 789 at 72:10-19 (Gerken), 87:20-25 (Frost)).

[10] Gerkin agreed with the Government identification of convenience as the main difference between a read-only and manual query format. (Doc. 789 at 80.)

contained the universe of Backpage data in a searchable spreadsheet. (*Id.* at 193-196.)[11] Among other things, Frost could search the data table by user identification number and type of ad. He filtered the data for ads subject to moderation and ads Backpage flagged as reported to the National Center for Missing and Exploited Children ("NCMEC"). Frost demonstrated a search for total number of ads in a marketplace of any type. Specifically, he determined that 88 percent of advertisements in the D.C. marketplace were adult-related. (Doc. 800 at 43:8-10.) The Government assisted Defendants in understanding and analyzing the provided server data. Using these lessons, Defendants can easily access and analyze all the data on Backpage.com at the time of the seizure. (*See* Doc 789 at 200:3-10.) The tools required are open source, publicly available and free to download. (*Id.*)

ii. Additional Findings

In some regards, Defendants appear to preference form over function. As an investigatory tool, the Government's current format of discovery, relying on manual querying of the databases themselves, seems superior to the "read-only" version of Backpage Defendants request. Although the "read-only" version, admittedly, "looks prettier," a manual query of the databases offers functional benefits that increase Defendant's ability to rebut the SI's allegations. For instance, unlike a "read-only" version of Backpage where a search is restricted to a single marketplace database, the Government's current form of discovery allows Defendants to search across all marketplace databases in a single query. (Doc. 800 at 42-43.) So, when searching for ads reported to NCMEC, Defendants could "create a script" to search across all Backpage while the a read-only or fully-functioning version of Backpage.com was not programmed with a specific query to compile and tally each Backpage ad reported to NCMEC, such a search can be conducted with relative ease when manually querying the databases. (*See id.* at 42:12-25.) Although the user interface "wouldn't look like a Web page," it presents more information, allows for more effective investigation and more flexible searches presented

[11] Among over 91 searchable data fields, the spreadsheet included phone numbers, white list, header, title, ad, ad body, associated images, region, price, IP address, email address, user identification number and invoice information. (Doc 800 at 193-96.)

in a digestible form. (Doc. 789 at 79:13.)

Further, the additional cost and necessary delay required to create a "read-only" version of Backpage.com weighs against granting the Motion. In outlining the numerous challenges of creating a "read-only" version of Backpage at this point,[12] Will Gerken estimated that returning Backpage.com to read-only function would take "a couple of months" minimum, "at least a couple of people during that time", and cost "somewhere between $30,000 and $50,000." (Doc 789 at 123:5-10.) Especially when, as here, the functional gains of a "read-only" version are marginal (at best), costly, and substantially slow the progress of litigation, Defendants justification stands on shaky ground.

Lastly, the ESI Protocol also supports denying the Motion. "[A]ny format selected for producing discovery should maintain the ESI's integrity, allow for reasonable usability, and reasonably limit costs, and, if possible, conform to industry standards for the format." *See* ESI Protocol, Introduction at 1-2. Testifying experts clearly established that while the form of the Government's disclosure is changed, the data is identical. (*See* Doc. 789 at 80:4-11 (Gerken), 225:5-8 (Frost)). The usability of the disclosures was manifestly reasonable as Agent Frost's demonstration of manual queries using SQL proved. Not only was Agent Frost able to locate the underlying data from ads that supported specific counts in the SI, he was also able to filter for specific data points—like ads reported to NCMEC—that Defendants represent as important to their defense. (*See* Doc. 800 at 307:12-18, 320-28.) As discussed above, the current form of disclosure offers some investigative capabilities beyond what even a fully-functional Backpage.com allowed. The Government's current form of disclosure limits costs significantly. All the software needed to interpret and analyze the disclosed Backpage databases and forensic images is open source and readily available for free download. Although Defendants will likely incur some cost to retain a competent expert conversant in SQL, this cost is minimal and pales

[12] Amongst others, Gerken highlighted the lack of a schematic drawing of the original Backpage system, (Doc. 789 at 87:1-4), and setting up GYRO, an additional programming application language that allows the "same design templates [to] function as they did before." (*Id.* at 84:20-23.)

comparison to the alternative.[13] Further, the Government's disclosures comply with industry standards. The Government used industry-standard, open-source forensic tools to create forensic images, reproduce databases and provide the imaged hard drives to Defendants in industry-standard E01 format.[14] While Defendants may believe the "read-only" form benefits the presentation of their case to a jury, that form is available to neither party. *See* ESI Protocol, Introduction at 2 ("[w]hen producing ESI discovery, a party should not be required to take on substantial additional processing or formatting conversion costs and burdens beyond what the party has already done or would do for its own case preparation or discovery preparation."). Without more, the Court will not order the Government to provide discovery at significant expense merely to suit Defendants preference.

iii. Defendants Expert Tami Loehrs

Ms. Tami Loehrs testified as computer forensics expert on Defendants behalf. Loehrs testimony at the second evidentiary hearing, if credible, placed the Government's disclosures in a highly-suspect light. Loehrs painted a picture of an incompetent Government operation where key evidence was handed over in paper sacks and access to discovery was severely restricted. (Doc. 800 at 390, 388-89.) She insisted the Government's forensic tools were non-standard and much of the discovery produced was unverifiable "garbage." (Doc. 800 at 434:22-23.) The veracity of these representations, and Loehrs credibility, did not survive the third evidentiary hearing.

After Loehrs initial testimony at the October 2nd hearing, the Government offered to advise and assist Defendants with any technical difficulties. Agent Frost then met with Loehrs and select defense counsel in a recorded tutorial on November 19, 2019 to address

[13] Retaining an adequate expert in place of Ms. Loehrs who lacks expertise in many requisite areas pertinent to this case may have no net cost increase.

[14] E01 is a format called EnCase format, a standard forensic copy format. (Doc. 789 at 30 (Agent Cullen); Doc. 800 at 140 (Loehrs)). Despite conceding E01 was an industry standard format and later acknowledging the Government-provided drives in E01, Ms. Loehrs maintained the Government did not provide data in industry standard format during the hearing. Ms. Loehrs initially failed to figure out how to access the data and then testified the imaged drives held no data, only to be clearly disproven by the Government. In light of these blatant errors, the Court accords Ms. Loehrs representations little credibility.

the technological issues informing Loehrs initial testimony. (Doc. 815-1.) At the third hearing, the Government questioned Loehrs and recounted for the Court the steps required to examine the Backpage server data. The Government identified three steps: (1) whether the drive was readable; (2) whether the readable drive contained E01 forensic files that could be pulled into forensic software; and (3) accessing the Backpage server data. Despite previously testifying that the very same Backpage drives the Government provided "just show as garbage," (Doc. 800 at 139:21-23), Loehrs conceded that, after Agent Frosts November 19 tutorial, the answer at each stage was "yes." (Doc. 832 at 16-17.) The contradictions continued. Loehrs admitted the forensic images were readable, (c*ontra* Doc. 800 at 424.) She conceded her previous testimony that the Government's E01 files were "not a valid file" and something "that no forensic tool will open no matter how hard you try" was incorrect. (*Compare* Doc. 800 at 141:16-17 *with* Doc. 832 at 20:4-20.)

The Government exposed that Loehrs difficulties in accessing the Backpage drives were largely self-inflicted. Instead of a Linux-based system, Loehrs used a Windows operating system incapable of interpreting the Backpage drives correctly. Only when Agent Frost conducted a step-by-step tutorial[15] for Defendants did Loehrs acknowledge that "I totally understand that Windows doesn't interpret these [drives] correctly." (Doc. 832 at 16:15-18.) The Government downloaded Paladin 7, a free, Linux-based forensic tool, to allow her to access the drives on her Windows computer. Loehrs was unaware Paladin 7 existed. (*Id.*) As discussed in detail above, the Backpage servers used a ZFS file system and configured into ZPools. Loehrs has no experience with either. (*Id.* at 17.) The software employed by the Backpage servers—a FreeBSD operating system, jails, a ZFS file system—was readily available and known by Defendants as of February of 2018[16] at the latest. Loehrs herself met Agent Frost and viewed the Backpage servers during an on-site visit at the FBI facility in Pocatello, Idaho in April. (*See* Doc. 800 at 424:1-2.) Yet, Loehrs

[15] The Declaration of Special Agent Matthew Frost, (Doc. 815-1), outlines the history of this meeting in detail.

[16] In a February 2019 call, Agent Frost advised Defendants of the specific expertise required to properly analyze the Backpage servers, specifically commenting that because he "also already extracted the databases" familiarity with the ZFS file system was required. (Doc. 789 at 160-61).

lacked basic knowledge about the Backpage systems until the first evidentiary hearing on October 2, 2019. (*Id.* at 382:10-12.) The Court is perplexed by Loehrs failure to even attempt to apprise herself of basic information directly bearing on her testimony despite ample opportunity. (*See id.* at 421, 423-24.) Whether a product of poor communication between Loehrs and Defendants' counsels or Loehrs own willful ignorance or incompetence, her testimony worked to Defendants disadvantage. Loehrs representations were internally inconsistent and contradicted by both Will Gerken and Government demonstrations before the Court and in a recorded tutorial the Government conducted for Defendants benefit. This Court agrees with many prior courts that Ms. Loehrs "provided little, if any, credible or reliable testimony to support her expert opinions in this case." *U.S. v. Thomas*, 5:12-cr-37, 44, 97, 2013 WL 6000484 at *16 (D. Vt. Nov. 8, 2013); *see also United States v. Pirosko*, 787 F.3d 358, 367 (6th Cir. 2015) (agreeing with the *Thomas* court and noting Loehrs retractions of testimony on cross-examination); *United States v. Certantes-Perez*, EP-12-CR-217-KC, 2012 WL 6155914 at *6 (W.D. Tex. Dec. 11, 2012) (finding Loehrs conclusions "imprecise, misleading, and similar to expert testimony . . . properly excluded" in prior cases).

b. Defendants Remaining Arguments

More specifically, Defendants present five independent grounds justifying their request for a fully-functional Backpage.com. (*See generally* Motion.) That is, Backpage.com must be necessarily reconstituted to: (1) adequately defend against Backpage's alleged moderation practices; (2) fully investigate and respond to the fifty alleged victim ads referenced in the Superseding Indictment; (3) defend against the Government's general characterization of Backpage.com; (4) identify ads posted through aggregation; and lastly, (5), to rebut allegations that Backpage ads show a "reciprocal link agreement" with TheExoticReview.com ("TER"), a prostitution website where "johns" could rate escorts. As discussed previously, a flawed premise underlies each justification—that the Government's current discovery is not reasonably usable *and* restoring Backpage.com to "read-only" form is required to allow Defendants to meaningfully

address the SI's allegations. Satisfied by the reasonable usability of the Government's discovery, the Court briefly addresses Defendants specific justifications in turn.

First, Defendants believe access to Backpage's actual databases will reveal exculpatory moderations practices[17] at odds with the Government's allegations. That is, restoring Backpage.com to full-functioning will show Defendants moderation practices impeded rather than facilitated, the advertisement of prostitution on Backpage. (*See* Mot. at 10.) Fortunately for Defendants, the Governments current manner of disclosure facilitates their search for exculpatory moderation practices. As discussed above, Agent Frost demonstrated step-by-step how Defendants can manually query all Backpage ads categorized as "adult" and filter for any moderation flags, edits, or changes. (Doc 800 at 329-31.) Combined with the earlier hot document production, (*See* Resp. at 11), the Government's disclosures meet their Rule 16 obligations. Second, Defendants believe access to a functioning Backpage is necessary to fully investigate and defend against the fifty ads referenced by the SI. Defendants concerns here are unfounded. The Government disclosures demonstrably allow for the investigative functionality they desire. (*See* Mot. at 11-12.) Third, Defendants request a functioning Backpage to "show comparative and analytic information about the Backpage.com website and its practices as a whole." (Mot. at 13.) The manual query format demonstrated multiple times in detail clearly provides Defendants requested capabilities. Defendants remaining justifications—to identify ads posted using Backpage aggregation practices and ads demonstrating a reciprocal link agreement with TER—are moot. Defendants possess all the ad data held on Backpage servers at the time of seizure. They are further aware of cost-free, effective tools to analyze that data for evidence of aggregation or links to TER. And, as mentioned previously, Backpage did not use versioning. Thus, Defendants cannot expect to find all historical versions of an ad modified with Backpage aggregation practices that "occurred only in the

[17] The moderation practices at issue refer to Backpage policies theoretically designed to flag and, at times, remove inappropriate content from Backpage ads. The SI alleges that, rather than filtering out prostitution-related content, the moderation strategies assisted Defendants in concealing the true nature of the ads. (*See* SI at ¶¶11, 68, 100-01.) Specifically, the SI points to emails and internal documents already provided to Defendants in discovery to support these allegations. (*See* Resp. at 11-14.)

early years of Backpage.com" if later deleted, even on a fully-functional Backpage.

IV. CONCLUSION

Accordingly,

IT IS ORDERED Defendants Motion to Compel Discovery is **DENIED**. (Doc. 643.)

Dated this 7th day of January, 2020.

Honorable Susan M. Brnovich
United States District Judge