EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

United States of America Plaintiff, v. Michael Lacey, *et al.*, Defendants.	Case No. CR-18-422-PHX-SMB DECLARATION OF TAMI LOEHRS

I, TAMI LOEHRS, hereby declare as follows:

Qualifications and Experience

I am a digital forensics expert and owner of Loehrs Forensics, LLC (formerly Loehrs & Associates), a firm specializing in digital forensics. My offices are located at 1505 North Central Avenue, Suite 111, Phoenix, Arizona 85004. I am competent to testify and the matters contained herein are based on my own personal knowledge.

I have been working with computer technology for over 20 years and I hold a Bachelor of Science in Information Systems. I have completed hundreds of hours of forensics training including courses with Guidance Software and Access Data. I am an EnCase Certified Examiner (EnCE), an Access Data Certified Examiner (ACE), a Certified Computer Forensic Examiner (CCFE) and a Certified Hacking Forensic Investigator (CHFI). I have conducted over one-thousand forensics exams on electronic evidence including hard drives, cell phones, removable storage media, security systems, dash cams, and other electronic devices, in addition to forensically preserving and analyzing on-line data such as cloud storage and social media platforms. I have conducted seminars on Computer Forensics and Electronic Discovery throughout the United States. In addition, I hold a Private Investigator Agency

License in the State of Arizona which requires a minimum of 6,000 hours investigative experience. My Curriculum Vitae is attached as Exhibit A.

I have been hired as a digital forensics expert on over one thousand criminal and civil cases throughout the United States and internationally since the year 2000 and I have testified over one hundred and twenty-six times as a digital forensics expert in State, Federal and international Courts.

Role of Loehrs Forensics

I have been retained as a digital forensics expert by counsel for defendants for the purpose of assisting with matters related to the searching, collecting, analyzing and producing of electronic evidence in this case. Specifically, the government has alleged that Defendants facilitated the promotion of prostitution through the use of the website Backpage.com and conspired to commit money laundering. The government seized approximately one-hundred and six (106) servers associated with the operation of Backpage.com and these servers were located in Tucson, Dallas and Amsterdam. Using industry standard methodologies, techniques and tools, it is the role of Loehrs Forensics to assist defendants in accessing the Backpage.com data that resides on these servers for the purpose of corroborating or refuting the government's allegations.

I have reviewed discovery materials produced by the government including, but not limited to, evidence chain of custody forms regarding items collected from 202 S. Tucson Blvd, Tucson, AZ on May 3, 2018, 13601 Preston Road, Dallas, TX on May 10, 2018 and 1855 N. 6th Avenue, Tucson, AZ on April 6, 2018; photographs; Joint Status Reports with exhibits; and the Superseding Indictment.

On April 17, 2019, I flew to Pocatello, Idaho to review fourteen (14) of the servers in the government's possession. The servers were located on several different tables, with two to three servers stacked on top of each other. During my visit, I was restricted to a visual

inspection only and was not permitted to photograph the servers or power them up to determine the configuration of the servers or the nature of the data contained within.

On April 23, 2019, I conducted a similar visual inspection of thirty-two (32) servers and three (3) external hard drives located at the FBI in Phoenix, Arizona. Again, I was not permitted to photograph the servers or power them up to determine the configuration of the servers or the nature of the data contained within. Also during that visit, four hard drives containing digital evidence in this matter were released to me for my review and analysis to be conducted at the Loehrs Forensics lab.

On May 17. 2019, Loehrs Forensics picked up three boxes of evidence from the offices of Bruce Feder and took them to the Loehrs Forensics lab for review and analysis. Those three boxes contain fifty-six (56) hard drives produced by the government that purport to be five (5) of the one hundred and six (106) servers seized from Backpage.com.

Summary of Opinions and Conclusions

The majority of the electronic data seized from Backpage.com and produced by the government does not meet minimum industry standards and is completely unusable in its current form. The issues with the data produced by the government includes, but is not limited to, the way in which the data was acquired and preserved, the integrity of the data produced and the ability or lack thereof to access, review and analyze the data.

There are nationally and globally accepted standards for documenting, acquiring and preserving digital evidence. Some of the most recognized organizations who promote those standards include the International Organization for Standardization (www.ISO.org), the Scientific Working Group on Digital Evidence (www.SWGDE.org), and the National Institute of Standards and Technology (www.NIST.gov). In addition, law enforcement has adopted its own standards for acquiring and preserving digital evidence. Regardless of the organization or agency setting the standards, the methodologies accepted for acquiring and preserving

digital evidence are identical in their purpose, to maintain the integrity of the data being acquired and preserved and the government failed to do that in this case.

Backpage.com Operations

Based on my review of SA Robinson's Declaration, Backpage.com relied upon database servers, image servers and web servers to host the website as it would have appeared to users on the Internet. No one server contains web pages as they were presented to the user when the site was active, rather, elements would need to be pulled from multiple servers in order to generate an ad as it would have been displayed to the user. In fact, a single advertisement on the website may be constructed of multiple files spread throughout numerous servers and hundreds of hard drives. Further, any actions taken with regard to an advertisement, such as removing it, would also be located among multiple files, multiple servers and multiple hard drives all working as a cohesive unit. When any one component of the unit has been damaged or removed, the advertisement and any activity associated with that advertisement, may be lost. This includes, but is not limited to:

- whether the ad was blocked and when,
- whether the source of the ad was blocked and when,
- whether the ad was removed from the website and when,
- whether the ad was reported to law enforcement and when,
- who accessed an ad on the website and what the result was, and
- which individuals were involved in any of these activities.

In that regard, it is critical that all Backpage.com servers are acquired and preserved in such a manner so as not to destroy or remove any one of these components and maintain the data in substantially the same state it was in when it was active on the Internet.

Data Acquisition and Preservation

When electronic data becomes evidence in a case, it is up to the forensic examiner to assess the digital evidence thoroughly to determine the best course of action to take. Digital

evidence is fragile and can easily be altered or damaged. Similar to preserving a crime scene, the investigator must protect potential physical evidence from being damaged or destroyed. The investigator cannot just tread through the bloody crime scene in street shoes and pick up the murder weapon with an ungloved hand, he must assess the situation and plan accordingly. Careful considerations must also be made with regard to the tools to be used at the crime scene, the methods in which to acquire and preserve the physical evidence and careful documentation of the entire process.

Similar considerations must be made when acquiring digital evidence, especially when that digital evidence consists of a complicated, dynamic system that depends upon multiple interconnected servers to keep a website up and running. The simple act of powering down a server incorrectly may forever alter and destroy the integrity of the data that resides within. In addition to considerations on how to approach the preservation of evidence, industry standards require that digital evidence be acquired and preserved in a forensically sound manner so as not to alter, damage or destroy that data but to maintain the integrity of that data.

When seizing and preserving any electronic media, especially a server, careful documentation of its current state, running processes, physically mounted items, and damage should be thoroughly recorded and photographed. Because servers can be extremely volatile, it is imperative to follow best practices and procedures for each server type and scenario. For instance, if a server containing potential evidence is powered on, the current processes, network configuration, encryption keys and memory should be captured prior to powering off in the event it contains information crucial to properly analyzing the physical hard disks. Servers that are located powered on should also be properly powered down using the operating system shut down function prior to dismantling any of the physical disks to avoid data loss or damage. Servers that are located powered off should be carefully documented to

determine if they are connected to a power source, are warm to the touch that may indicate it was recently powered on,

The government has provided very little information, if any at all, as it relates to their process of acquiring and preserving the Backpage.com data. In that regard, it is unknown when the data was acquired, what tool or tools it was acquired with, the type of acquisition conducted, who conducted the acquisition, the name or description of the server being acquired, which specific hard drive in the server was acquired, the configuration of the server and/or the hard drive being acquired, whether the data was encrypted or otherwise formatted in such a way that the integrity of the data could be lost, what processes were running, network configurations, verification that the acquisition process was successful or that the data has been verified as an exact duplicate of the original.

Additionally, most of the data acquired by the government was not produced in an industry standard format and is not forensically sound. This is tantamount to sending someone a document that cannot be opened in Microsoft Word or Adobe, industry standards, because the document was created with an unknown program, and then not informing the person of the program used. Until the unknown program has been identified and obtained, the document remains inaccessible. Because the data produced by the government is not in industry standard formats and the government has provided little to no information regarding their process for acquiring the data, I am unable to access, identify or restore the data to its original condition and the data remains inaccessible and unusable to defendants in its current form.

Integrity of the Data

Data integrity refers to the accuracy and consistency of data. Essentially, the data should be in substantially the same condition as it was when it was taken into custody. In this case, the original condition of the Backpage.com data was a working website. That website contained millions of advertisements with images and text that could be viewed on the

Internet, but also contained internal data related to the editing, blocking, removal, payment and reporting of those advertisements. The functionality of the Backpage.com website was dependent upon numerous interrelated servers, each server containing multiple internal hard drives that also work together as a cohesive unit. If any one of these servers or any single hard drive within those servers has not been properly acquired and preserved, the Backpage.com website does not function in its original condition.

The data produced by the government bears no resemblance to the original Backpage.com website and the integrity of that data has been destroyed in a number of ways. First, the government has not produced all of the interrelated servers required for the Backpage.com website to function. Second, the government has not produced valid forensic images of the hard drives contained within each of those interrelated servers making it impossible to recreate a single server in substantially the same condition as it was when it was seized. Third, the government has provided no information regarding the configuration of the servers or the hard drives within making it further impossible to recreate a single server in substantially the same condition as it was when it was seized. The data, as it has been produced by the government, has made it impossible to identify, access or restore the data to its original condition and the data remains inaccessible and unusable to defendants in its current form.

Ability to Access the Data

An important element of having industry standards is to ensure the data acquired can be accessed by anyone with the proper tools and expertise. It does not matter how experienced or knowledgeable an expert may be, if data is produced in an unknown format that does not meet industry standards, cannot be accessed using industry standard tools, and no information about that format is provided, the data will be inaccessible and unusable.

Although the government produced some of the data using industry standard forensic formats, even that data has proven to be inaccessible and unusable. Many of the forensic

images produced by the government are incomplete, invalid and cannot be read by industry standard forensic tools. Although numerous attempts were made at accessing these forensic images, using numerous industry standard tools, none were successful and the data remains inaccessible and unusable in its current form.

Conclusions

The data seized by the government in this case is unique because Backpage.com was a working website that relied upon an extensive, complicated system of interconnected servers in order to function. However, the government did not document the system before taking it down, they did not document their processes for acquiring and preserving the evidence, they did not acquire the devices using industry standard methodologies or formats, and they did not produce all of the necessary data to restore the Backpage.com website. Rather, the government has produced only some bits and pieces of a complex integrated system, some of which are broken, with no documentation or information on how it was running when they seized it or the tools and methodologies they used to acquire it. This is tantamount 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 required to put it all together.

The data seized from Backpage.com and produced by the government is undocumented, incomplete, broken, inaccessible and unusable. In its current form, the data produced by the government does not meet industry standards and the integrity of the data has been altered and/or destroyed.

DATED August _5_, 2019.

Tami Loehrs, CCFE, CHFI, EnCE, ACE