

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Brook Mallak,

Civil File No. 13-CV-02119

DWF/LIB

Plaintiff,

v.

Aitkin County, *et al.*

**AFFIDAVIT OF
MARK LANTERMAN**

Defendants.

STATE OF MINNESOTA)

)

SS:

COUNTY OF HENNEPIN)

I, Mark Lanterman, being first duly sworn on oath, state and depose as follows:

1. I am the Chief Technology Officer for Computer Forensic Services, Inc. (“CFS”) in Minnetonka, Minnesota. I have previously provided expert testimony in the above-captioned matter. That report also contains an overview of my biographical information and experience. A copy of my curriculum vitae has been attached as Exhibit A for reference.

2. I have previously served as a court-appointed neutral computer forensic analyst and as an expert witness on behalf of numerous law enforcement agencies and government entities. In that capacity, I have developed protocols for computer forensic discovery that protect the interests and functions of government and law enforcement as well as the legitimate interests and needs of parties seeking information from government entities and law enforcement.

CURRENT DISPUTE AND SCOPE OF REQUEST

3. I was initially retained as a consultant in this action by counsel for the Plaintiff. I was asked to assist with electronic evidence pertaining to Plaintiff's allegations. Electronic evidence is central to this dispute given the nature of the Driver and Vehicle Service's electronic, web-based portal used to access citizen's driving records.

4. The DVS database keeps track of access information within "access logs". Access logs are simply limited in the scope of information they record. These logs include the name of the citizen being researched, the date and time, the StationID number, and the originating IP address. To illustrate these limitations, it is usually not possible to decipher how long a particular citizen's DVS profile was viewed. Such determinations, however, may be made with access to the original electronic devices, from which the DVS databases could be accessed.

5. Because of the nature of this dispute and the challenges associated with device identification, an unknown number of devices may have accessed DVS records within the relevant timeframe. These devices include, but are not limited to, personal and government-issued smartphones, laptops, tablets, desktops, as well as in-squad computers.

6. As noted in my previous reports, the DVS database may be accessed from any electronic device with an Internet connection and an Internet browser. The names and location of the devices can be difficult if not impossible to identify from the DVS access logs alone. Although the logs contain the originating IP address, the names of the devices are not. IP addresses are numerical values that represent a unique connection to the Internet.

In the case of mobile devices that use cellular networks (in-squad computers, mobile phones), this is generally not possible.

7. In order to assemble the narrative of activity and verify the veracity and accuracy of the information contained within the DVS database logs, it is my recommendation to counsel for Plaintiff's that a reasonable inspection be performed against relevant electronic devices that were used to access the DVS information in dispute. This will permit Plaintiff to determine the nature and scope of Internet activity surrounding the accesses in dispute as well as electronic data related to the accesses, including deleted emails and documents.

8. As such, CFS recommends that physical access be granted to any and all government and personal computers, and other electronic devices (smartphones, tablets, thumb drives) that were used to access Plaintiff's personal data from the DVS database on the dates and times contained in Exhibit B of the Second Amended Complaint for the purpose of forensic imaging (copying). The process of imaging creates an accurate representation of the device, regardless of file or operating system.

FORENSIC METHODOLOGY

9. The first step generally taken by a trained computer forensic examiner is to create a duplicate copy of an entire electronic storage device (often known simply as 'imaging'). The creation of a drive image is recognized by the computer forensic community as the proper way to preserve original electronic evidence. The devices can be imaged on a rolling basis. Multiple devices can be imaged at the same time. Imaging can be done in a manner that reduces the intrusiveness on government functions.

10. It is important to understand that in addition to the production of the 'hard copy' of a document or file, there may be computer-generated information (metadata) relating to the document that is not produced in the 'hard copy'. The process of creating a forensic image captures this information in its original, unmodified state. For example, there may be hidden text from earlier drafts in the computer file that does not appear in the printed-paper version. Computer files also have system information that is not disclosed on the printed version, such as dates that indicate when documents were created, accessed or modified.

11. Merely turning on a computer will change the state of the evidence by altering such critical date stamps and will potentially write over and erase existing files. For this reason, "imaging" should be done as soon as any potentially relevant electronic evidence is identified.

12. It is also important to understand that when a user "deletes" files, the files are not necessarily unrecoverable. Until the file is "overwritten" by another file, the "deleted" file is still subject to being recovered. As such, it is essential to preserve all involved computer hard drives as soon as possible because deleted, but relevant, data may be overwritten and destroyed.

13. I understand that the electronic storage devices subject to analysis in this, or any, case may contain highly personal and confidential information, possibly including proprietary information, attorney-client privileged material, and non-responsive e-mail communications. The protocol set forth below protects the interests of the producing party. It is the same protocol ordered by Judge Boylan in the Multifeeder litigation and

similar to the protocol ordered by Judge Frank in the Intoxylizer source code litigation. Those orders are attached hereto as Exhibits B and C.

14. I am familiar with the practice in litigation of requiring and using protective orders to restrict the disclosure and use of information. I have agreed to be bound by the terms of any Protective Order in force in this case. I further agree to be bound by any other instructions of the Court.

15. After the devices have been forensically preserved, I have recommended to Plaintiff's counsel that the parties adopt the following protocol:

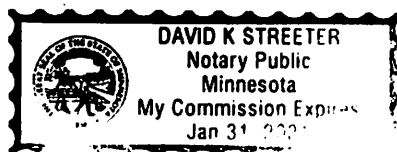
- a. CFS will be given physical access to all relevant computers and other storage devices (smartphones, tablets) for forensic imaging (copying).
- b. CFS will then prepare, from that data and the list of search terms supplied by Plaintiff's counsel, two logs to be provided to both Defendants' and Plaintiff's counsel.
- c. The first log will list each relevant document on the hard drive with the document's file name; file extension (i.e., whether the document is a Word document or PowerPoint presentation); whether the file has been deleted; the date and time when the file was created, last accessed, and last altered; the size of the file; and the location of the file (file path). This log will capture all potentially relevant documents, but will not specifically identify individual emails.
- d. The second log will provide identification of each potentially relevant email pooled from the first log and will list who sent and received the

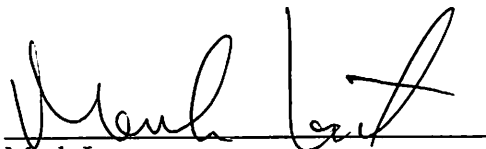
email, the date and time, the subject line and the names of any attached files.


- e. In addition to such searches, CFS will also prepare detailed Internet history reports. Given the nature of access of the DVS database systems, responsive Internet browsing information is best presented as spreadsheets. These spreadsheets would contain a summary of available Internet activity from a provided system.
- f. I will provide Defendants' counsel a copy of all search-responsive documents/files from the provided devices. In turn, Defendants' counsel could then determine which of the documents are to be produced.
- g. Defendants' counsel would then produce the documents to Plaintiff's counsel in native format accompanied by a privilege log.
- h. While all documents and file contents will first be provided to Defendants' counsel, CFS is permitted to discuss with Plaintiff's counsel any technical findings. Such findings will not include any confidential information, but will simply serve to provide context for the data, such as file deletions or altering of documents.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: May 5, 2016




Mark Lanterman


05/05/16