10-477

ORIGINAL

STATE OF VERMONT
CHITTENDEN COUNTY, ss.

SEARCH WARRANT

TO: Det. Michael D. Warren and any Vermont Law Enforcement Officer:

You are hereby commanded to search:

- 145 Pleasant Avenue Burlington, Vermont. 145 Pleasant Avenue is described as a one level single family residence with crème color siding, red shutters, a red garage door and the number 145 displayed to the right of the front main door. 145 Pleasant Avenue is located by taking the second, most westerly entrance to Pleasant Avenue and traveling all the way to the end. The house is the last house on the east side of the street prior to the street looping around back to Starr Farm Road (see pic below)

For the following described property or objects:

- SEE ATTACHMENT "A"

See also attached Order.

Serving this warrant and making the search of the PREMISES between the hours of **6AM and 10PM** within **ten (10)** days from the date hereof, and if the property or object be found there, to seize it, prepare a written inventory of it, and bring such property or object before the District Court of Vermont, Unit No. III.

Continuing, under the authority of this warrant, to conduct a search/analysis of the items seized for the evidence described, for as long as reasonably necessary at an off-site facility or facilities determined by law enforcement.

This warrant is issued upon the basis of an affidavit and the finding of probable cause by me, filed with the clerk of the court.

Dated at Burlington, County of Chittenden, on the 22nd day of December 2010

Judge @ 1:50 pm.

STATE OF VERMONT

SUPERIOR COURT
Chittenden Unit

CRIMINAL DIVISION

In re: Application for Search Warrant
Eric Gulfield Computer

AMENDED ORDER

The application to search the computer belonging to Eric Gulfield is *granted* subject to the conditions listed herein. In setting these conditions, the Court has been guided by *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 9th Cir. 2009).

1. As a condition for receiving a search warrant to search the subject computer, the State cannot rely upon the "plain view doctrine" to seize any electronic records other than those authorized by this warrant. That is, any digital evidence relating to criminal matters other than the identity theft offenses, may not be seized, copied, or used in any criminal investigation or prosecution of any person.

2. Inspection and investigation of the subject computer must be done by either an independent third party or specially trained computer personnel who are not involved in the investigation while staying behind a firewall, that is, in the absence of other agents of the State, and subject to a ban on copying or communicating to any person or the State any information found on the subject computer other than digital evidence relating to identity theft offenses.
3. Any digital evidence relating to the ~~threats~~ offenses being investigated must be segregated and redacted before it is provided to the State, no matter how intermingled it is.

4. If the segregation is performed by State computer personnel, it is a condition of this warrant that the computer personnel will not disclose to the State investigators or prosecutors any information other than that which is the target of the warrant, that is, digital evidence of the identity theft offenses.

5. The search protocol employed must be designed to uncover only the information for which the State has probable cause, that is the aforesaid alleged offenses, and only that digital evidence may be provided to the State. Techniques to focus the search should include but are not limited to, specific time periods relevant to the alleged criminal activity, key word searches, and limiting the search to specific file types.

6. The government has at its disposal sophisticated hashing tools that allow identification of well-known illegal files (such as child pornography) that are not

at issue in this case. These and similar search tools may not be used without specific authorization by the court.

7. Information relevant to the targeted alleged activities may be copied to other media to provide to State agents. No other digital evidence may be so copied.

8. The government must return non-responsive data, keeping the court informed about when it has done so and what it has kept.

9. Any remaining copies of the electronic data must be destroyed absent specific judicial authorization to do otherwise.

10. Within the time specified in the warrant, the State must provide the issuing officer with a return disclosing precisely what data it has obtained as a consequence of the search, and what data it has returned to the party from whom it was seized. The return must include a sworn certificate that the government has destroyed or returned all copies of data that it is not entitled to keep.

Dated at Burlington, Vt., December 22, 2010

Michael S. Kupersmith
Superior Judge