IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, xxxxxxx xxxxxxx, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

INTRODUCTION

1. I have been employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) for over xxxx years. I have investigated matters involving the criminal infringement of a copyright, particularly in relation to violations of Title 18, United States Code, Section 2319, which criminalizes, in part, the reproduction or distribution of copyrighted works.

2. The location to be searched is known as **xxxx xxxxxx xxxxxxxx xxxxxxxxx, xxx x. xxxx xxxxxx, xxxxxx, Missouri 64730**, and this affidavit is submitted in support of a warrant to search the entire premises, including any business records and any computer and computer media located therein where the instrumentalities, fruits, and/or evidence of violations of Title 18, United States Code, Section 2319, as specified further in Attachment A, might be found.

3. The statements contained in this affidavit are based on information provided by the Butler Missouri Police Department (BPD), as well as my experience and background as an Agent with the FBI. Set forth in this affidavit are the facts I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, Unites States Code, Section 2319, are located at the above address.

DEFINITIONS

4. The term "computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

5. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings and drawings), photographic form (including, but not limited to, microfilm and photocopies), mechanical form (including, but not limited to, records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-

ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), memory sticks, optical disks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

SPECIFICS OF SEARCHES AND SEIZURES OF COMPUTER SYSTEMS

6. I have consulted with an expert in computer searches, **Computer Specialist/Forensic Examiner xxxxx xxxxxxx xx**. According to **CS/FE xxxxxxx** searching and seizing information from computers often requires agents to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, CD-ROMs, aand DVDs) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and might store criminal evidence in random order or with deceptive file names or deceptive file extensions. This requires searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes imbedded in the system, such as "booby traps"), a controlled environment is essential to its complete and accurate analysis.

7. Based upon your affiant’s consultation with experts in computer searches, data retrieval from computers and related media, and consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all of a computer

system's input/output (I/O) peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

a. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular I/O devices in order to read the data on the system. It is important the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence contained therein. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, and data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them within a reasonable time.

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as the central processing unit (CPU). Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

THE INVESTIGATION

CONCLUSION

FURTHER AFFIANT SAYETH NOT.

xxxxxx xxxxxxxxxxx, Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me
this ___ day of xxx 2005.

xxxxxxx xxxxxxxx
CHIEF UNITED STATES MAGISTRATE JUDGE