IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF THE RESIDENCE OF DAVID PAUL HELKOWSKI LOCATED AT 8302 OAKLEIGH ROAD, PARKVILLE, MARYLAND 21234

Case No. 14-0666 TJS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jeremy Bucalo, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

- I am a Special Agent (SA) with the Federal Bureau of investigation (FBI) and have been employed since October 31, 2004. Currently, I am currently assigned to the FBI Baltimore Field Office. My experience as an FBI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of fraud and intrusion. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, intellectual property and other computer-based crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment as well as interview and interrogation of subjects in regards to cyber crimes. I have been involved in numerous criminal and national security investigations involving cyber intrusion, cyber terrorism, and counter-intelligence.
- This affidavit is made in support of an application for a warrant to search the single-family residence located at 8302 Oakleigh Road, Parkville, Maryland, described further in Attachment A (the "Subject Premises"), for evidence, instrumentalities, fruits, and contraband, described further in Attachment B, concerning violation of Title 18, United States Code, Section 1030(a)(2)(C), (fraud and related activities in connection with computers) committed by DAVID PAUL HELKOWSKI.
- The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have not however excluded any information that would tend to defeat a finding of probable cause. Instead, I have set forth facts that I believe are sufficient to establish probable cause to believe that HELKOWSKI committed a violation of Title 18, United States Code Section 1030(a)(2)(C), and evidence, instrumentalities, fruits, and contraband concerning said violation.

PROBABLE CAUSE

- Beginning on March 15, 2014 the University of Maryland security task force received an email from "theppm7@hushmail.com" at 02:12 stating the following: "Security Taskforce, There are current open holes that have been fixed. Out of politeness I'll give you a chance to respond directly about this to me, and I'll consider pulling it off the public internet. Please read http://www.reddit.com/r/news/comments/20gmfe/umd_data_breach_round_2 Your internal IDs are listed below to get your attention. This isn't spam. If you want to cooperate I would be willing to provide details (cooperate as in just let me impart useful information on things that need to be fixed immediately - at no cost or demands of any sort btw), but I would want some assurance (in legal writing) that I will not be charged with any crimes. If not, consider this your fair warning and last contact from me. -The PPM." Also within the email was a list of names, student ID numbers, email addresses and titles of employees of UMD that the writer believed are the individuals associated with the Security Task force to include: Dr. Ann G. Wylie, Kim L. Colbert, Dr. Michal Cukier, Ms Michele A. Eastman, Dr. Michael Hicks, Christian Johnson, Dr. David Maimon, Dan Navarro, Porter W. Olsen, Terry Roach, Apaar Singh, Gerry Sneeringer, Dr. Susan Taylor, Dr. Amitabh Varshney, Dr. Chuck Wilson, and Jim Zahniser.

- Further investigation revealed a pastebin.com posting of the following:

"MD Data Security

I'm a computer hacker. I've been hacking into computers since I was a kid. I've always considered computer security to be an absolute joke, and have easily broken pretty much any security that can be broken. I say easily, but it still takes a tremendous amount of work and research.

Recently I heard in the news about the 'UMD Data Breach'. I didn't care at all, because it surprised me none. Some time later I heard from a friend that there may be more to the story than was revealed by the media. I pried at the friend who mentioned it, and kept pressing. Eventually the friend related that he knew about a security report that was written by someone who works for UMD.

I asked if he could get a copy of the report to me. He balked and wanted to know why I wanted it. This friend knows I like to make waves and don't care for political niceties. I lied and told him it was simply of interest to me. I got the report.

The person who wrote the report stated in it that they knew about a security vulnerability at UMD; months before the data breach occurred. They stated that they reported the hole, and that nothing was done about it. The report went on to explain in detail about the hole itself, and how it has existed for many years, and was clearly originally planted by computer hackers.

The report seems to me to have been given to UMD at some point. (and that's how I got it...) The sequences of events described showed it was written after the UMD data breach in the news. I don't know who at UMD received or got the report initially, but I have a feeling there are few people who know about it.

I used the information in the report and used standard attacks against the UMD site to attempt to gain access in the same fashion as I assume was used by the original attacker. I found holes. I was able to replicate the original attack described in the report. This is now, after supposedly security has been enhanced greatly, the NSA has been involved, and the Secret Service has been involved.

After gaining initial access, I elevated my level of access, using the information from the report,

and was easily able to obtain full access to almost all of the websites hosted by the UM system, as well as more than 80 databases of information at UMD. I downloaded a lot of them. The information I was able to obtain far exceeds the previous UMD data breech reported in the news, and I believe shows incompetence in the security methodology of UMD employees and all those working to enhance their security.

As evidence of my replication of the attack, I give you the following:

(Affiant Note: Personally identifiable information of a UMD official (SSAN, name, title, and phone numbers) was included in the posting, but is omitted herein out of concern for his/her privacy)

I am sorry I am exposing your private information Mr. Loh, but it is necessary to prove the seriousness of the problem. Your statement to the news said that contact information was not present in the leaked data. This may be true, I don't know what the original attackers took, but I can tell you that I'm in possession of this and a whole lot more information that should not fall into the wrong hands.

I can state with certainty that the following information about people is available to myself, and is likely available to whatever hackers originally planted the holes that were found:

1. Names of all current employees and students of UM

2. Social security numbers

3. Contact information (phone numbers and home addresses)

4. Student ID numbers

5. Student issued ID barcode data (the one of the back of student IDs)

6. Student Major, GPA, etc.

7. Access levels of employees

I have detailed information across the entire systems. I have obtained org charts of all employee, contact information for everyone, and all internal procedures and policies dating back for years into the past.

As an additional example, I shall quote a portion of the policy from years ago regarding dealing with bomb threats. I am pretty sure that policy is not public, for good reasons. The policy says, as one of it's main things, that the person talking to the person making a threat should ask "Why do you want to blow up the building?"

That leads me to the point. My point. Why did I write this? Why am I publicly posting this information? What do I intend to do with the data now in my possession?

I shall first alleviate anyone's concerns for their privacy and for the safety of UMD. I have not given the information to anyone, I don't intend to sell the information to anyone, nor do I intend to do anything at all with it. I hacked the system because I didn't believe the news, and I wanted to prove that the security at UMD is still terrible. I have done so. That was and is my goal.

Is this a positive goal? What is the constructive point of this? The truth. I believe firmly in the truth. The truth is not the fairy tale that you've been told by the news and PR heads. The truth is that security is terrible everywhere, across the internet, and that if you want your information to be secure, don't ever give that information to anyone else that you can't entirely trust. Your university is not someone you can trust. Sorry.

As an aside, I'd like to mention that I am well aware of the damage this statement may cause. I am also aware that many will simply discount my statements and say I gained no access. That is fine. If you want to take the blue pill and live in a bubble; enjoy.

I believe the following people may be hurt by this report:

1. UMD Employees (specifically the people who setup their security)

It can't look good for UMD employees to have active security holes after supposedly fixing their security for over a month now.

2. Government Entities (NSA / Secret Service)

Considering I'm not sitting in a jail cell right now, apparently these guys suck more than I expected and have failed to notice my intrusion or to do anything about it. I suppose it's possible they know everything and are just waiting for me to do something bad, like write this, but I honestly believe they have no clue.

3. Anyone involved in the report that I obtained.

Considering I broke into the system using information obtained from the report I got access to, everyone who saw the report, and anyone involved in the creation of it, may likely get in trouble. Sorry guys, but you brought this one upon yourselves. If you are gonna break into stuff, the first rule of thumb is to never reveal any information about yourself.

4. Myself

I admitted I hacked into the system and copied data that I don't have official access to. I've posted personal information of the UMD president. While I don't feel particularly bad about any of this, it is quite likely that these are considered crimes. I'm a US citizen, since I admitted gaining this information from people with access to it. It's entirely possible the people who gave me the information may figure out who I am. I could very well get in a lot of trouble.

In my own defense, I will state the following as my ultimate purpose and justification: I want UMD security to actually be improved, not just for people to say it is being improved. I have in no way damaged UMD systems, nor have I explained to anyone how to replicate what I have done.

In closing, I leave you with the following:

I am using the pseudonym 'theppm7' to identify myself.

The following is an RSA key I have created for the purpose of communicating with me and/or validating that any statement is actually from me.

If you want to send me a private message, just post it somewhere public that can be found on google using my pseudonym, and I will attempt in some way to respond. Learn how to encrypt it to the key listed here.

If you are a criminal of some sort, and you are gonna beg me to give you the data; please don't bother. It's not for sale, at any price. My purposes are not for personal gain."

- On March 15, 2014, the FBI became aware that the Canton Group was working with the UMD School of Public Health to perform website migration. David Helkowski (HELKOWSKI), employee of Canton Group, identified a vulnerability within the UMD network. Canton Group provided the information to UMD on 2/27/2014.

AUSA 3/16/14

- On March 16, 2014, the FBI interviewed employee 1 of Canton Group and was informed that HELKOWSKI was "chatting" online via Steam using the moniker "livxtrm". This individual provided the following chat between HELKOWSKI and himself:

livxtrm: hey
Aykus: hey
livxtrm: I contacted the task force related to the data breach
livxtrm: and they are gonna sign a thing saying they won't press charges against me
livxtrm: and I'll tell them everything
livxtrm: told them a lot already; kind of waiting for the legal assurance now
livxtrm: they said they will though
Aykus: ok
livxtrm: I'll be glad to have it out of my hair
livxtrm: It was entertaining but un-nerved me
livxtrm: I wrote a thing describing how crappy their security is
livxtrm: and how they did basically nothing
livxtrm: and that i was able to break in again
livxtrm: (all anonymous btw)
livxtrm: and I then found the IDs of all the people in the task force
livxtrm: and emailed it to them all at once
livxtrm: along with the SSN and cell # of the president of the college
livxtrm: and said they can either work with me, or I'll just post it online and be done with it
Aykus: jesus
livxtrm: I got tired of being ignored
livxtrm: so I forced their hand
livxtrm: I posted it publicly to reddit too
livxtrm: and sent them the link
livxtrm: so the presidents info has now been leaked online
livxtrm: i fucking hate people treating me like an amateur
livxtrm: am just sick and tired of it
livxtrm: I contacted major news agencies also
livxtrm: but they just ignord me
Aykus: wow
livxtrm: after the news agencies ignored me
livxtrm: that is what made me go nuts
livxtrm: and talk to the task force
Aykus: i have a lot i'd like to say at the moment
Aykus: but i'm not sure that I can
livxtrm: oh? how is that?
livxtrm: they questioned you I guess
Aykus: you are very smart, and I know that about you at least :)
livxtrm: I worded my stuff very carefully
livxtrm: I don't think they can prove it was me
livxtrm: I'm sure they suspect it's me
livxtrm: I got sick of them fuckingaround

A.E.E. 3/16/14

livxtrm: sorry
Aykus: I didn't know about anything of this, all I knew about was the thing I gave to my teacher
livxtrm: He gave it to the task force
livxtrm: they have it
livxtrm: he cowrote their policies with the lead of their security
livxtrm: I am in direct communication now with their lead of security
Aykus: ok I know you just want the issue fixed as do I, I mean it is my freakin information
livxtrm: exactly
livxtrm: that's what I said too
livxtrm: I've asked nothing of them
livxtrm: except to not get me in legal trouble
Aykus: have you gotten to speak with them yet
Aykus: in person or just over the phone or something?
livxtrm: through hushmail; through VPN; using anoynmous alias
livxtrm: have refused to disclose my identity
livxtrm: until they guarantee no legal action
Aykus: ok ok let's not talk anymore
Aykus: for both our sakes
livxtrm: ok -shrug-
Aykus: because the less I know the better for now
livxtrm: that's fine
Aykus: it is nothing personal
livxtrm: my only reason to tell you
livxtrm: is positie
livxtrm: that they are actually improving things
livxtrm: so I am happy now
livxtrm: cause I was tired of nothing being done
Aykus: yes, i appreciate that
Aykus: really do, so thank you again
livxtrm: ok
livxtrm is now Away.

- On March 15, 2014, a UMD IT official received an email from "theppm7@hushmail.com" at 14:10:46 -0400 and contained within the email the writer stated, "The following is a SHA256 hash of my name and the last 4 digits of my social security number, surrounded by 9 letters of garbage in front of it, and 12 behind it: 4e958844a83aa6baa308c1c7528805af8fde93ce6acccd17bee2a8f547f6ec1c". The writer also wrote, "Please draft up a legal protection that says the following things:".

- On March 15, 2014, the FBI interviewed employee 2 of Canton Group and was informed that HELKOWSKI used the moniker "livxtrm" when gaming online. This individual provided the following online "chat" with HELKOWSKI:

Friday, March 14, 2014
livxtrm: I didn't say anything

livxtrm: but I took your pig
mowens3: lol fair enough
livxtrm: you want your award?
mowens3: not really
livxtrm: oh -shrug-
mowens3: haha
mowens3: maybe they will send it to me
livxtrm: maybe who knows
livxtrm: good news
mowens3: whats up
livxtrm: UMD may be willing to actually listen to me
livxtrm: and do something about their security problems
livxtrm: Danny's teacher guy is a nobody I think
livxtrm: I got in touch with the right people
mowens3: damn that's good
livxtrm is now Online.
livxtrm: they don't know it's me
livxtrm: I'm pretending to be a hacker who hacked in
livxtrm: usign the report that I actualyl did write
livxtrm: lol
livxtrm: I'm demanding they sign legal documentation that I won't get in trouble
livxtrm: before revealing my identity
mowens3: will this get me in trouble?
mowens3: what are they saying they want to do?
livxtrm is now Away.
mowens3: wonder how they will react to this
livxtrm is now Online.
mowens3: I left the company and definitely don't want to be involved in anything like that
livxtrm: sorry was writing an email to them
livxtrm: no
livxtrm: I am demanding they don't do anything bad to anyone I'm inolved with
livxtrm: and that it is fully my responsibility
livxtrm: I'll get the legal protection first
mowens3: damn
livxtrm: before I say shit about it being me
livxtrm: I sent them a sha256 salted hash of my name and information
livxtrm: to put in the signed legal docs
livxtrm: upon which, after getting it signed, I'll give them the salt
livxtrm: it's salted with 20 characters
livxtrm: so there is no way they could possibly reverse the hash until then
mowens3: lol
mowens3: I didnt even know that was possible
livxtrm: works for me
livxtrm: why wouldn't it be :)
Your state is set to Offline.
livxtrm is now Offline.
Lost connection to Steam, will rejoin chat automatically when connection

regained.

Connected again and rejoined chat.
livxtrm is now Online.
livxtrm: did you know that the public and private rsa keys can be swapped
livxtrm: and it still would work fine?
livxtrm: you could rename your pubic keyfile to private one
mowens3: haha
livxtrm: and the other way around
mowens3: WTF
livxtrm: and give out your private key
livxtrm: and hold onto your public key
livxtrm: cryptographically they are the same
mowens3: damn
livxtrm: you are just giving out one of the two
livxtrm: imagine that for a trivia question
livxtrm: on who wants to be a millionaire
livxtrm is now Offline.
Your state is set to Offline.
Lost connection to Steam, will rejoin chat automatically when connection regained.
Connected again and rejoined chat.
livxtrm is now Online.
livxtrm: going well so far
livxtrm: president, lead of task force, and lead of internal security are all agreeing to not press charges
livxtrm: so is good... I just want to describe everything I've done in detail and be done with it at this point
livxtrm: the likelyhood of being crucified in the name of justice from here on out is just too high
livxtrm is now Online.

PREMISES TO BE SEARCHED

- The Subject Premises is a single-family residence located in Parkville, Maryland that is occupied by HELKOWSKI and his wife.

- On March 16, 2014, agents conducting surveillance at the Subject Premises, identified a Green Mazda bearing Maryland license plate 3AJ3814, which is registered to DAVID PAUL HELKOWSKI, Date of Birth 02/17/1982.

- On March 16, 2014, a Real Property search conducted for 8302 Oakleigh Road, Parkville, Maryland revealed PAUL HELKOWSKI as the owner of the residence.

- Based on my training and experience, and conversation with other agents, I know that criminal cyber actors typically conduct criminal operations in the privacy of their home utilizing a laptop or desktop computer system. Criminal cyber actors typically store tools,

malware, and additional software on these computer systems. Additionally, conducting operations from home provides the actors with high speed, reliable Internet access, access to information stored on servers accessible via the Internet, and allows them to conduct these operations out of view of the general public.

- As described above and in Attachment B, this application seeks permission to search for records and materials that might be found at the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Federal Rule of Criminal Procedure 41(e)(2)(B).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

- I submit that if a computer or storage medium is found at the Subject Premises, there is probable cause to believe records that are evidence of violation of 18 United States Code Section 1030(a)(2)(C) will be stored on that computer or storage medium, for the following reasons:

  - Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
  - Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
  - Wholly apart from user-generated files, computer storage media, in particular, computers' internal hard drives, contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically possible to delete this information.
  - Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

- As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crime described in this affidavit,

but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the Subject Premises because:

- Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. I submit that if a computer or storage medium is found at the Subject Premises, there is probable cause to believe the records described in Attachment B will be stored on that computer or storage medium, for the following reasons:
    - Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- Wholly apart from user-generated files, computer storage media, in particular, computers' internal hard drives, contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

- As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the Subject Premises because:
  - Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
  - Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and lastaccessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
  - A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

- The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- I know that when an individual uses a computer to create and store fraudulent identification documents and means of identification, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

OFF SITE REVIEW

- In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:
- The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be

impractical and invasive to attempt on-site.

- Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.
- Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.
- Because several people may share the Subject Premises as a residence, it is possible that the Subject Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is probable that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.
- Due to the above, authorization is hereby sought to allow any off site search to be conducted in accordance with Attachment C.