

**UNITED STATES DISTRICT COURT  
DISTRICT OF MAINE**

<b>UNITED STATES OF AMERICA</b>	)	
	)	
<b>v.</b>	)	<b>Criminal No. 07-82-P-H</b>
	)	
<b>VICTOR HANSON,</b>	)	
	)	
<b>Defendant</b>	)	

**RECOMMENDED DECISION ON MOTION TO SUPPRESS**

Victor Hanson, charged with one count of transportation and attempted transportation of child pornography in violation of 18 U.S.C. §§ 2252A(a)(1) and (b)(1) and 2256(8)(A) and one count of possession of child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2256(8)(A), *see* Indictment (Docket No. 1), seeks to suppress any and all evidence seized pursuant to a search warrant executed at his home on or about April 22, 2004, *see* Motion To Suppress Evidence Seized as a Result of Search Warrant (“Motion”) (Docket No. 8) at 1. For the reasons that follow, I recommend that the Motion be denied.

**I. Factual Backdrop<sup>1</sup>**

On April 21, 2004 Scot A. Bradeen, a Lewiston Police Department detective and member of the Maine Computer Crimes Task Force, applied for a warrant to search the home of the defendant at 86 Gage Street in Augusta, Maine and to seize evidence (including computer hardware and storage media) of the crimes of sexual exploitation of a minor in violation of 17 M.R.S.A. § 2922,

---

<sup>1</sup> No evidentiary hearing was sought or held with respect to the instant motion, which challenges the validity of a search warrant. *See generally* Motion.

dissemination of sexually explicit materials in violation of 17 M.R.S.A. § 2923 and possession of sexually explicit materials in violation of 17 M.R.S.A. § 2923. *See* Affidavit and Request for a Search Warrant (“Affidavit”), Exh. A to Motion, at [1]-[2], [11]. In a section of the Affidavit titled “Statement of Probable Cause,” Bradeen stated, *inter alia*, that:

1. He had been a law-enforcement officer for approximately twelve years and had received specialized training in the investigation of computer-related crimes, including specific training in the investigation of dissemination of child pornography via peer-to-peer networks. Statement of Probable Cause, contained at pages [2]-[11] of Affidavit, ¶¶ 1-2.

2. On February 18, 2004 he received two investigative referrals from Special Agent Robert Leazenby of the Wyoming Division of Criminal Investigation. *Id.* ¶ 3. Leazenby advised that he was conducting undercover Internet investigations into distribution of child pornography through the use of peer-to-peer, or “P2P,” file-sharing networks. *Id.*<sup>2</sup> Leazenby also reported to Bradeen that:

A. He was first certified as a peace officer in Wyoming in 1988 and had been trained in the investigation of computer use in the exploitation of children and in methods of forensic analysis of computers used in criminal activity. *Id.* ¶ 3.1. He was assigned to operate in an undercover capacity on the Internet by the director of the Division of Criminal Investigation for the purpose of identifying and investigating persons attempting to exploit or solicit sexual acts with children. *Id.*

B. As part of his undercover investigation, he used P2P client software to access a file-sharing network via the Internet. *Id.* ¶ 3.2. He also used a software video capture program that captured the computer screen as he viewed it and saved the output to a video file. *Id.* ¶ 3.3. During his undercover sessions, he ran a software firewall whose operation was visible on the screen of his computer. *Id.*

---

<sup>2</sup> Bradeen explained that P2P file-sharing programs are a standard way of transferring files from one computer system to another while connected to a network, usually the Internet, and allow groups of computers using the same file-sharing network to connect directly with each other and to share files from one another’s computer systems. Statement of Probable Cause at [3] n.1.

¶ 3.5.<sup>3</sup> The firewall revealed the resolved name or IP address of computers connected to the undercover computers, and bytes received and sent were visible and were documented through use of the video capture program. *Id.*<sup>4</sup> During the undercover session and when possible during transfer of the image in question, he executed the MS Windows “netstat” command, the results of which were written to a file. *Id.* ¶ 3.6.<sup>5</sup>

C. On Thursday, October 16, 2003 he received an image depicting a female child approximately ten years old performing oral sex on an adult male. *Id.* ¶ 4. He saved that image. *Id.* Using the above-described technology, he determined that the image was transferred at least in part from a computer with an IP address of 65.235.252.8. The resolved name associated with that IP address was 1Cust8.tnt2.augusta.me.da.uu.net. *Id.* On Thursday, October 23, 2003, Leazenby received the same image from a computer with the IP address 65.235.252.60. *Id.* The resolved name associated with that IP address was 1Cust60.tnt2.augusta.me.da.uu.net. *Id.* In both instances, while the transfer of the image occurred, the offender identified himself with the user name [Bob@KaZaA](#). *Id.*

D. Leazenby recognized the image in question as belonging to a series of child pornographic images referred to as the “Sabban” series. *Id.* ¶ 4.1. That series is well-known to law enforcement as a series containing images of actual children and is included in the Known Child Victim Identification Program maintained by the National Center for Missing and Exploited Children as part of its initiative to identify child victims. *Id.* As part of his referral, Leazenby sent Bradeen two compact discs (“CDs”). *Id.* ¶ 5.

3. On February 19, 2004 Bradeen reviewed the CDs provided by Leazenby. *Id.* He opened the image file that was received by Leazenby, viewed it and determined that it depicted a

---

<sup>3</sup> Bradeen explained that a firewall is a hardware device or software program designed to monitor and protect a computer system and that a firewall can monitor the connections to a computer and the amount of data transmitted and received. Statement of Probable Cause at [3] n.2.

<sup>4</sup> Bradeen described an IP address as a unique number given to a specific computer at a specific time that identifies that computer while connected to a network, most often the Internet. Statement of Probable Cause at [4] n.4. He noted that the IP number generally is assigned by a customer’s Internet Service Provider (“ISP”) and that most ISPs maintain logs so they can determine the IP address assigned to a customer on a date and a specific time. *Id.* He indicated that a resolved name is a unique name that the registrant of IP addresses may associate with an IP address. *Id.* at [4] n.5. That association is maintained in the domain name services (“DNS”). *Id.*

<sup>5</sup> Bradeen explained that Netstat is a program that enables display of the connections to a computer at the time the program is run. Statement of Probable Cause at [3] n.3. Depending on the parameters given to the program, it may show the IP address of the connection in numerical or named form. *Id.* When the “netstat” command is executed during a file transfer between computers, the output will include the IP address or name of the computer(s) that transferred the file(s). *Id.*

female child performing oral sex on an adult male. *Id.* ¶ 5.1. He then viewed the video files documenting the two undercover sessions during which the image file was received, verifying Leazenby's information concerning the IP addresses, resolved names and user names associated with transfer of the file. *Id.* ¶¶ 5.3, 5.4.

4. Bradeen then conducted reverse DNS lookups of both IP addresses, which yielded the same resolved names that had appeared in the status window of the firewall on Leazenby's computer. *Id.* ¶ 6.<sup>6</sup> Bradeen then checked the American Registry for Internet Numbers, determining that the two IP addresses in question were registered to UUNET, AlterNet of Ashburn, Virginia, which he knew to be a subsidiary of MCI. *Id.* ¶ 7. Via an administrative subpoena issued by the Bureau of Immigration and Customs Enforcement, Bradeen obtained information that the IP addresses in question were assigned to [oldfart59@netzero.net](mailto:oldfart59@netzero.net), an e-mail address assigned to Victor Hanson of 86 Gage Street, Augusta, Maine. *Id.* ¶¶ 8, 8.1.

5. Bradeen confirmed through the Maine Department of Motor Vehicles that Victor Hanson, born on June 9, 1942, resided at 86 Gage Street in Augusta, Maine. *Id.* ¶ 10. He checked Augusta Police Department records, which also showed Hanson residing at that address and revealed that a concealed firearms permit had been issued to Hanson by that agency. *Id.*

6. On February 24, 2004 Bradeen obtained a warrant to search Hanson's residence. *Id.* ¶ 11. On arrival, he learned that Hanson had left for Florida and would not be returning until April 2004. *Id.* On April 21, 2004 Lt. Brann of the Augusta Police Department advised Bradeen that Hanson had returned home from Florida. *Id.*

7. Bradeen stated, *inter alia*, that he knew from his training and experience that:

---

<sup>6</sup> Bradeen stated that a reverse DNS lookup of an IP address returns the associated resolved name of that IP address if the  
(continued on next page)

A. P2P application software allows networked computer users to share many types of files with other users, generally through the Internet. *Id.* ¶ 11.1. These files typically include music, graphics, images, movies and text. *Id.* In this way, users are able to collect large numbers of files, including child pornography. *Id.* P2P networks provide ready access to child pornography. *Id.* ¶ 11.2.

B. The P2P client application software allows the user to catalogue the files he has in his collection. *Id.* ¶ 11.6. Cataloguing the files allows other users to locate them quickly for download. *Id.* Music files, for example, may be catalogued by artist and song title. *Id.* Pornographic images or videos may be catalogued by age of the child or description of the sex act. *Id.* A user searching for a file may then request the file by some search term such as “artist” or “title” and, if the file has been made available for sharing with other P2P network users, a list of computers with the file indexed in the same manner will become available from which the user may download the file. *Id.* ¶ 11.7. In order to download a file, the receiving computer must make a direct connection to the source(s) computer. *Id.* ¶ 11.10. These direct connections can be seen by using software tools such as “netstat” or firewalls. *Id.* When a user downloads a file from another P2P user, the original file remains on the P2P user’s equipment. *Id.* ¶ 11.12.

C. Those who have demonstrated an interest in collecting child pornography are likely to keep these images concealed, but accessible. *Id.* ¶ 12(1). Images may be kept as trophies, such as actual photographs or images of the suspect’s own sexual activity with children. *Id.* ¶ 12(2). An offender may also keep images as a means of seducing a child victim by arousing curiosity, attempting to normalize the desired acts, lowering the inhibitions of potential child sexual partners and demonstrating and explaining what the offender may desire to be done, a process generally referred to as “grooming.” *Id.* ¶ 12(3). Images are also maintained as a means of sexually arousing the suspect or for commercial purposes, to obtain money or other items of value, including more child pornography. *Id.* ¶ 12(4). Child pornographic images tend to be extremely important to these offenders. *Id.* ¶ 12(5). These images are likely to remain in their possession or under their control for many years. *Id.* Because of the importance of these images, offenders are unlikely to destroy them or delete them from their computers before printing or copying to other media. *Id.* Offenders who collect child pornography using the Internet often copy those images to removable media such as floppy or compact discs, which are concealed in the residence or commingled with other media. *Id.* ¶ 12(6).

D. Those who collect, trade or disseminate child pornography often hide their collections of sexually explicit materials in hard-to-find places or attempt to hide them on their computers. *Id.* at [11]. They often go to great lengths to conceal these materials from inadvertent discovery by family members, friends or law

---

resolved name has been established in the DNS of the Internet. Statement of Probable Cause at [5] n.8.

enforcement. *Id.* Those who collect child pornography rarely, if ever, dispose of such materials. *Id.*

The search warrant for which Bradeen applied was issued the same day – April 21, 2004 – by Maine District Court Judge John B. Beliveau. Exh. B to Motion. Police executed the warrant the following day, seizing items that included two computers and CDs. Exh. C to Motion.<sup>7</sup>

## II. Analysis

“A warrant application must demonstrate probable cause to believe that (1) a crime has been committed – the ‘commission’ element, and (2) enumerated evidence of the offense will be found at the place to be searched – the so-called ‘nexus’ element.” *United States v. Ribeiro*, 397 F.3d 43, 48 (1st Cir. 2005) (citation and internal quotation marks omitted). Both the issuing magistrate and a subsequent reviewing court look to “the totality of the circumstances indicated [within the four corners of] a supporting affidavit” to assess the existence *vel non* of probable cause. *United States v. Schaefer*, 87 F.3d 562, 565 (1st Cir. 1996). “Yet such review cannot start from scratch. A magistrate’s determination of probable cause should be paid great deference by reviewing courts.” *Id.* (citation and internal quotation marks omitted).

“In determining whether the nexus element is satisfied, a magistrate has to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Ribeiro*, 397 F.3d at 48-49 (citation and internal punctuation omitted). “Put differently, the

---

<sup>7</sup> The defendant objects to inclusion of information on page 4 of the government’s brief regarding a police interview of him on the ground that the information is irrelevant and immaterial. *See* Government’s Opposition to Defendant’s Motion To Suppress Evidence Seized as a Result of Search Warrant (“Opposition”) (Docket No. 10) at 4; Defendant’s Reply to Government’s Opposition to Defendant’s Motion To Suppress Evidence Seized as a Result of Search Warrant (“Reply”) (Docket No. 11) ¶ 1. The objection is sustained. I have not recited that information or considered it in my analysis.

application must give someone of reasonable caution reason to believe that evidence of a crime will be found at the place to be searched.” *Id.* at 49 (citation and internal quotation marks omitted).

The defendant contends that probable cause to issue the warrant pursuant to which items were seized from his home on April 22, 2004 was lacking inasmuch as (i) critical information presented in the Affidavit was more than six months old (and, hence, stale) as of the time of issuance of the warrant, and (ii) the Affidavit established no nexus between the alleged criminal activity and the place to be searched – namely, his home. *See* Motion ¶¶ 4-8. The government rejoins that the Affidavit supplied ample probable cause for issuance of the warrant; alternatively, it invokes the so-called *Leon* good-faith exception. *See* Opposition at 5-13; *see also United States v. Leon*, 468 U.S. 897, 922-25 (1984).

A defendant bears the burden of proving the illegality of a warrant; if he succeeds, the burden shifts to the government to prove entitlement to the *Leon* good-faith exception. *See, e.g., United States v. Longmire*, 761 F.2d 411, 417 (7th Cir.1985) (“The general federal rule on who bears the burden of proof with respect to an allegedly illegal search or seizure is based upon the warrant-no warrant dichotomy: If the search or seizure was effected pursuant to a warrant, the defendant bears the burden of proving its illegality; if the police acted without a warrant, the prosecution bears the burden of establishing legality.”); *see also, e.g., United States v. Koerth*, 312 F.3d 862, 868 (7th Cir. 2002) (“If a defendant is successful in establishing the invalidity of the search warrant, the burden then shifts to the Government to establish that the police relied in good faith on the judge’s decision to accept the affidavit and issue the warrant.”). For the reasons that follow, I conclude that (i) the defendant fails to carry his burden of proving the illegality of the search warrant he challenges, and (ii) even assuming *arguendo* the warrant was defective, the *Leon* good-faith exception applies.

Hence, I recommend that the motion to suppress be denied.

#### **A. Probable Cause: Staleness**

As the government acknowledges, *see* Opposition at 5, probable-cause analysis includes a temporal component, *see, e.g., United States v. Bizier*, 111 F.3d 214, 219 (1st Cir. 1997) (“a long delay in seeking a search warrant can create difficulties if the information is stale”) (emphasis omitted); *United States v. Dauphinee*, 538 F.2d 1, 5 (1st Cir. 1976) (“It is well established that the temporal proximity or remoteness of the events observed has a bearing on the validity of a warrant.”). There is no one-size-fits-all rule for determining staleness: “Factors to be considered in determining whether an affidavit is stale include the nature of the criminal activity under investigation and the nature of what is being sought.” *United States v. Reiner*, 500 F.3d 10, 15 (1st Cir. 2007) (citation and internal quotation marks omitted); *see also Dauphinee*, 538 F.2d at 5 (“[N]o hard and fast rule can be formulated as to what constitutes excessive remoteness, because each case must be judged in its circumstantial context.”). The First Circuit has further elaborated:

Staleness is not measured merely on the basis of the maturity of the information but in relation to (1) the nature of the suspected criminal activity (discrete crime or regenerating conspiracy), (2) the habits of the suspected criminal (nomadic or entrenched), (3) the character of the items to be seized (perishable or of enduring utility), and (4) the nature and function of the premises to be searched (mere criminal forum or secure operational base).

*United States v. Bucuvalas*, 970 F.2d 937, 940 (1st Cir. 1992) (citations and internal quotation marks omitted), *abrogated on other grounds by Cleveland v. United States*, 531 U.S. 12 (2000).

As the government suggests, a recent case from the United States District Court for the Western District of Kentucky, *United States v. Wiser-Amos*, Criminal Action No. 3:07CR-42-M, 2007 WL 2669377 (W.D. Ky. Sept. 7, 2007), is instructive. *See* Opposition at 6. Applying the same four factors discussed in *Bucuvalas*, the *Wiser-Amos* court concluded that a delay of seven months

from the time information was obtained through a P2P child-pornography investigation to the time authorities sought and executed a search warrant did not render the underlying information stale. *See Wiser-Amos*, 2007 WL 2669377, at \*1. For the following reasons, application of those factors yields the same result in regard to the approximately six-month delay in issue here:

1. Character of Charged Crime. The defendant is charged with transportation and attempted transportation of child pornography on the basis of the October 16, 2003 image transmission and possession of child pornography on the basis of seizure of various items from his home during the April 22, 2004 search. *See* Indictment. The defendant in *Wiser-Amos* faced similar charges (possession and distribution of child pornography) on the strength of law-enforcement computer interception via P2P software of a solitary electronic video file containing child-pornographic images. *See Wiser-Amos*, 2007 WL 2669377, at \*3-\*4. Nonetheless, the *Wiser-Amos* court declined to characterize the crime in issue as sporadic or isolated, observing: “Courts which have considered the character of child pornography crimes . . . reject the characterization of such sexual offenses as being isolated or sporadic in nature.” *Id.* at \*6. To the contrary, the court observed, “the widely accepted view [is] that individuals who possess and trade in child pornography tend to maintain visual depictions they have downloaded for long periods of time[.]” *Id.* at \*7 (citation and internal quotation marks omitted); *see also, e.g., United States v. Ricciardelli*, 998 F.2d 8, 12 n.4 (1st Cir. 1993) (“[E]xigent circumstances will rarely, if ever, be present in child pornography cases, as history teaches that collectors prefer not to dispose of their dross, typically retaining obscene materials for years.”); *United States v. Miller*, 450 F. Supp.2d 1321, 1335 (M.D. Fla. 2006) (same).

The *Wiser-Amos* court reasoned that the underlying facts also negated any inference that the

crime detected was an isolated incident, noting that the defendant had gone to the trouble of installing P2P software “specifically designed to permit peer-to-peer sharing of electronic image files such as the Babyshivid child pornography video.” *Wiser-Amos*, 2007 WL 2669377, at \*7. The court stated: “This conduct would cause a reasonably objective law enforcement officer or a magistrate judge to conclude that [the defendant] had a longstanding, serious interest in obtaining and distributing images of child pornography.” *Id.* In this case, as well, Leazenby intercepted the images in question using P2P software, and Bradeen averred, based on his training and experience, that P2P file-sharing software permits ready access to child pornography and that those who collect such images rarely destroy them.

For these reasons, the crimes with which the defendant is charged properly can be characterized as crimes of an ongoing, rather than sporadic or isolated, nature.

2. Habits of Suspect. “Obviously, if a criminal defendant moves frequently with the hope of avoiding detection or capture, the probability that evidence of his or her criminal conduct will be found in a given location diminishes rapidly with the passage of time.” *Id.* The *Wiser-Amos* court found no evidence the defendant was nomadic. *See id.* He had opened a high-speed internet access account at his home address in spring 2004 and had the same IP address through the time of the search on February 24, 2006. *See id.* The court added:

Commonsense also suggests that individuals who have a continuing interest in child pornography have extremely limited options that preclude them from being nomadic. Their conduct is extremely forbidden. It carries severe social stigma. As a result, such individuals can only pursue their criminal sexual interests involving children in extremely private settings where they feel safe and secure from public scrutiny. A nomadic lifestyle would be extremely disruptive to their efforts to engage regularly in such criminal conduct at their leisure.

*Id.* at \*8.<sup>8</sup>

Although, in this case, Bradeen discovered upon attempting to execute a search warrant at the defendant's Augusta, Maine residence in February 2004 that the defendant had gone to Florida and was not expected to return until April, I agree with the government that nothing in the Affidavit suggested that the defendant "move[d] frequently with the hope of avoiding detection or capture." Opposition at 9 (quoting *Wiser-Amos*, 2007 WL 2669377, at \*7). Leazenby intercepted images that Bradeen was able to trace to an e-mail address assigned to the defendant, of 86 Gage Street, Augusta, Maine. Bradeen confirmed from two sources that the defendant did indeed reside at that address. He learned that the defendant was expected to return there in the spring of 2004. In these circumstances, a reasonable inference could be drawn that the defendant's residence in Augusta, Maine was and remained his primary residence or home base.

3. Nature of Items To Be Seized. After canvassing the caselaw, the *Wiser-Amos* court deemed child-pornography images non-perishable in nature, both because technology permits their retention for years and because collectors of such materials tend to hoard them. *See Wiser-Amos*, 2007 WL 2669377, at \*8-\*9. The court concluded: "This additional factor weighs heavily against finding staleness even months after the images have been obtained by defendants charged with child pornography offenses." *Id.* at \*9; *see also, e.g., United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) ("Based on her training and experience as a Customs agent, the affiant explained that collectors and distributors of child pornography value their sexually explicit materials highly, rarely

---

<sup>8</sup> The First Circuit, like the *Wiser-Amos* court, has not shied from drawing common-sense conclusions in staleness analyses. *See, e.g., Dauphinee*, 538 F.2d at 5 ("We think that, especially because of the nature of the item sought (hand grenades), the affidavit in this case was not fatally flawed because of staleness. Unlike many other items of contraband, hand grenades are not, to the best of our knowledge, in great demand even by the criminal element in our society; and they do not lend themselves to rapid disposition in the marketplace.").

if ever dispose of such material, and store it for long periods in a secure place, typically in their homes. We are unwilling to assume that collectors of child pornography keep their materials indefinitely, but the nature of the crime, as set forth in this affidavit, provided good reason to believe the computerized visual depictions downloaded by Lacy would be present in his apartment when the search was conducted ten months later.”) (citations, footnote and internal punctuation omitted).

There is no reason to reach a contrary conclusion in this case. Bradeen averred, based on his training and experience, that use of P2P programs facilitates collection of child pornography and that offenders rarely destroy pornographic images that they have taken pains to collect.

4. Place To Be Searched. In *Wiser-Amos*, as here, the place to be searched was the defendant’s home. *See Wiser-Amos*, 2007 WL 2669377, at \*9. The court found: “The home of a defendant cannot be fairly characterized to be merely a criminal forum of convenience. Rather, it is more in the nature of a secure operational base for a defendant charged with child pornography possession or distribution.” *Id.* The court reasoned:

As noted, the options available to defendants with a deviant interest in child pornography are extremely limited. Because such individuals’ behavior tends to be addictive and longstanding, they must have ready access to their pornography collections at any given moment. Further, their collections must be kept secure and away from the prying eyes of members of the public and law enforcement officials. The location ideal for them to pursue their forbidden interest is clearly the home, where defendants feel most secure and have constant access to internet connectivity through their personal computers. As a result, the probability that any given defendant being investigated for offenses related to child pornography will have secreted pornographic images in his home is far greater than other nonsexual criminal offenses.

*Id.* In this case, while the defendant evidently wintered in Florida in early 2004, one reasonably could have inferred from the available information that his Augusta, Maine address – the address he had provided in setting up Internet service – was his primary residence, or home base. Nothing in

the Affidavit indicated that address was a mere criminal forum of convenience.

In short, the four *Bucuvalas* factors point in one direction: a finding that, in the circumstances presented, the delay of approximately six months from the time of Leazenby's undercover investigation to the time of application for the instant search warrant did not render the underlying information stale.

### **B. Probable Cause: Nexus Element**

The defendant also challenges the probable-cause underpinnings for issuance of the instant warrant on the ground that the Affidavit failed to disclose a nexus between the items sought and the place to be searched apart from Bradeen's general opinions, which the defendant argues are insufficient as a matter of law. *See* Motion ¶¶ 7-8. The government counters, and I agree, that the Affidavit sufficed to demonstrate the requisite "fair probability that contraband or evidence of a crime" would be found in the defendant's home. *Ribeiro*, 397 F.3d at 49 (citation and internal punctuation omitted); *see also* Opposition at 12-13.

Bradeen was able to verify that the pornographic image twice intercepted by Leazenby emanated from IP addresses assigned to [oldfart59@netzero.net](mailto:oldfart59@netzero.net), an e-mail address that, in turn, was assigned to Victor Hanson of 86 Gage Street, Augusta, Maine. Bradeen confirmed from two sources that an individual named Victor Hanson did in fact reside at that address. From all that appears, Bradeen had no direct knowledge whether any computer hardware, software or related paraphernalia was physically located at the Gage Street address. Yet, as discussed above, he reasonably could have concluded that the Gage Street address was the defendant's primary residence. He then reasonably could have inferred, based on his knowledge of the habits of collectors of child pornography, that the defendant kept computers at that location and secreted pornographic materials

within those computers and/or elsewhere within the privacy of his home (as opposed to at a workplace, at a friend's home or even at a seasonal Florida address) – an inference strengthened by the fact that the defendant gave his Gage Street address in registering his e-mail address. In the circumstances, direct evidence that the defendant transmitted the offending image from a computer housed at the Gage Street residence, or even that the Gage Street residence contained a computer, was not essential. *See, e.g., United States v. Feliz*, 182 F.3d 82, 88 (1st Cir. 1999) (“[I]nterpreting a search warrant affidavit in the proper commonsense and realistic fashion may result in the inference of probable cause to believe that criminal objects are located in a particular place, such as a suspect’s residence, to which they have not been tied by direct evidence.”) (citation and internal quotation marks omitted); *United States v. Charest*, 602 F.2d 1015, 1017 (1st Cir. 1979) (“[T]he nexus between the objects to be seized and the premises searched do[es] not have to rest on direct observation, but can be inferred from the type of crime, the nature of the items sought, the extent of an opportunity for concealment and normal inferences as to where a criminal would hide [evidence of a crime].”)

For the foregoing reasons, the defendant falls short of demonstrating that the challenged warrant was issued in the absence of probable cause.

### **C. *Leon* Good-Faith Exception**

The above analysis is dispositive of the instant motion to suppress. However, in the event the court should disagree and deem the warrant defective for lack of probable cause, I recommend that it nonetheless deny the motion to suppress on the basis of the *Leon* good-faith exception alternatively invoked by the government. Pursuant to that doctrine, “[e]vidence seized in violation of the Fourth Amendment is admissible in court if the government placed an objectively reasonable

reliance on a neutral and detached magistrate judge’s incorrect probable cause determination.”

*United States v. Crosby*, 106 F. Supp.2d 53, 58 (D. Me. 2000), *aff’d*, 24 Fed. Appx. 7 (1st Cir. 2001)

(citation and internal quotation marks omitted). The *Leon* exception is itself subject to exceptions:

There are four exclusions to the *Leon* good-faith exception: (1) when the magistrate was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard for the truth; (2) where the issuing magistrate wholly abandoned his detached and neutral judicial role; (3) where the affidavit is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) where a warrant is so facially deficient – i.e. in failing to particularize the place to be searched or the things to be seized – that the executing officers cannot reasonably presume it to be valid.

*United States v. Owens*, 167 F.3d 739, 745 (1st Cir. 1999) (citation and internal punctuation omitted). Tellingly, in the face of the government’s invocation of *Leon*, the defendant points to no evidence and offers no argument tending to show the doctrine is inapplicable. *See generally* Reply. Nor is it otherwise apparent that it is. Therefore, assuming *arguendo* that the instant warrant was defective, suppression of the items seized is unwarranted.

### **III. Conclusion**

For the foregoing reasons, I recommend that the defendant’s motion to suppress evidence be **DENIED.**

### **NOTICE**

*A party may file objections to those specified portions of a magistrate judge’s report or proposed findings or recommended decisions entered pursuant to 28 U.S.C. § 636(b)(1)(B) for which de novo review by the district court is sought, together with a supporting memorandum and request for oral argument before the district judge, if any is sought, within ten (10) days after being served with a copy thereof. A responsive memorandum and any request for oral argument before the district judge shall be filed within ten (10) days after the filing of the objection.*

*Failure to file a timely objection shall constitute a waiver of the right to de novo review by the district court and to appeal the district court’s order.*

Dated this 5th day of December, 2007.

/s/ David M. Cohen  
David M. Cohen  
United States Magistrate Judge

**Defendant (1)**

**VICTOR HANSON**

represented by **WALTER F. MCKEE**  
LIPMAN, KATZ & MCKEE  
P.O. BOX 1051  
AUGUSTA, ME 04332-1051  
207-622-3711  
Email:  
wmckee@lipmankatzmckee.com  
*ATTORNEY TO BE NOTICED*  
*Designation: Retained*

**Plaintiff**

**USA**

represented by **CRAIG M. WOLFF**  
U.S. ATTORNEY'S OFFICE  
DISTRICT OF MAINE  
100 MIDDLE STREET PLAZA  
PORTLAND, ME 04101  
(207) 780-3257  
Email: Craig.Wolff@usdoj.gov  
*LEAD ATTORNEY*  
*ATTORNEY TO BE NOTICED*