UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - - -x

UNITED STATES OF AMERICA :

- against - : **OPINION**

HARVEY PEREZ, : 02 Cr. 854 (DC)

Defendant. :

- - - - - - - - - - - - - - - - - - -x

APPEARANCES: JAMES B. COMEY, Esq.
United States Attorney for the
Southern District of New York
By: Alexander Southwell, Esq.
William Craco, Esq.
Assistant United States Attorneys
One Saint Andrew's Plaza
New York, New York 10007

LEONARD F. JOY, Esq.
The Legal Aid Society
Federal Defender Division
Attorney for Defendant
By: Nicole P. Armenta, Esq.
Steven Statsinger, Esq.
52 Duane Street
New York, New York 10007

CHIN, D.J.

This case presents difficult questions concerning the Fourth Amendment and the internet. On the one hand, child pornography and the sexual abuse of children are crimes that have been fueled by the internet, as those who would exploit children have sought to take advantage of the internet's vast and largely anonymous distribution and communications network. On the other hand, when law enforcement gathers information about the activity of individuals on

the internet, the potential for unreasonable intrusions into the home -- the chief concern of the drafters of the Fourth Amendment -- is great. This case demonstrates the tension that can exist: the Government argues, in essence, that it had probable cause to search the homes and seize the computers of thousands of individuals merely because they entered their e-mail addresses into a website where images of child pornography were available, even without any proof that the individuals uploaded, downloaded or discussed the images, or otherwise participated in the website.

Defendant Harvey Perez is charged in a one-count indictment with violating 18 U.S.C. § 2252A(a)(5)(B) by unlawfully and knowingly possessing materials containing images of child pornography transmitted in interstate commerce. The Government also seeks the forfeiture of certain of Perez's computer equipment. This case arises out of Operation Candyman, an undercover FBI investigation into a group that allegedly traded pornographic images of children over the internet.

Perez moves to suppress certain evidence obtained as the result of the execution of a search warrant at his home. For the reasons that follow, the motion is granted and the evidence is suppressed.

STATEMENT OF THE CASE

A. The Warrant

On March 6, 2002, federal law enforcement agents executed a search warrant at Perez's home. They seized a computer, numerous compact discs and floppy discs, computer drives, a scanner, two cameras, and a piece of paper listing various websites. (Perez Aff. ¶ 2; Armenta Aff. Ex. C (FBI property receipts)). The agents also interviewed Perez; he "admitted to visiting child pornography sites" on the internet. (Armenta Aff. Ex. D (FBI 302); see Perez Aff. ¶ 3).

B. The Affidavit

The search warrant was issued by Magistrate Judge James C. Francis IV on the basis of a 32-page affidavit executed by Special Agent Austin P. Berglas of the FBI on March 1, 2002. (Armenta Aff. Ex. E). The affidavit requested authorization to search nine residences in Manhattan, the Bronx, Riverdale, West Point, Wappingers Falls, Tarrytown, and the village of Florida, New York. (Id. ¶¶ 2, 5). One of these residences was Perez's home. The agent represented that probable cause existed to believe that the nine residences contained evidence of violations of 18 U.S.C. §§ 2252 and 2252A, which make it a crime to knowingly transport, transmit, or receive child pornography in interstate or foreign commerce by any means, including computer. (Id. ¶ 2).

The affidavit provided a lengthy description of how the internet and computers are used -- in general terms -- to distribute

child pornography. (Id. ¶ 7). It also described an undercover investigation by the FBI into the "Candyman Egroup." (Id. ¶ 8).

The affidavit provided little detail on the Candyman Egroup. It explained that the Candyman website displayed the following message:

> This group is for People who love kids.
>
> You can post any type of messages you like too or any type of pics and vids you like too.

(Id. ¶ 8(b)). The affidavit did not represent or assert that the sole or principal purpose of the Candyman Egroup was to engage in unlawful conduct. It represented that the group had 3,397 members. (Id. ¶ 8(h)).

The affidavit explained that to become a member of the website an undercover FBI agent was required to send an e-mail message to the group's moderator requesting permission to join; no fee was required. (Id. ¶ 8(b)-(c)). The affidavit detailed how, after receiving confirmation of membership via e-mail, the undercover agent was able to download, from the Candyman website, approximately 100 images and video clips of "prepubescent minors engaged in sexual activities," "the genitalia of nude minors," and "child erotica." (Id. ¶¶ 8(a), (e)). Of these, the majority of the images and video clips fell into the first category. (Id. ¶ 8(e)). In addition, the affidavit reported that the undercover FBI agent received some 498 e-mails from the Candyman Egroup, of which approximately 105 had

attachments containing child pornography and another 183 had attachments containing "child erotica images." (Id. ¶ 8(f)).[1]

The affidavit explained that the Candyman Egroup website had several features, including a "Files" section that permitted members to post images and videos for other members to download. It also disclosed that the Candyman site offered a "Polls" feature that permitted members to answer survey questions; a "Links" feature that permitted members to post links to other websites; and a "Chat" section that permitted members to engage in "real time conversations with each other." (Id. ¶ 8(d)).

The affidavit represented that all new members were immediately added to the Candyman Egroup's mailing list, and it asserted the following:

> Every Candyman Egroup member on the Candyman Egroup e-mail list automatically received every e-mail message and file transmitted to the Candyman Egroup by any Candyman Egroup member. Therefore, when individuals transmitted child pornography to the Candyman Egroup, those images automatically were transmitted to every Candyman Egroup member.

(Id. ¶ 8(d) (emphasis added)). These representations were critical because they advised the magistrate judge that all Candyman members

---

[1] The definition of "child pornography" requires a "visual depiction" of a "minor" -- "any person under the age of eighteen years" -- "engaging in sexually explicit conduct." 18 U.S.C. § 2256(1), (8). Cf. Ashcroft v. Free Speech Coalition, 535 U.S. 234, 122 S. Ct. 1389, 1405-06 (2002).

automatically received all e-mails and that therefore all Candyman members must have received e-mails that contained images of child pornography.

The nine homes were included in the search warrant application because e-mail addresses for subscribers to the Candyman Egroup were registered to individuals who resided at those locations. (Id. ¶¶ 9, 10).

C. The Government Acknowledges Error

On August 12, 2002, the Government wrote defense counsel and advised that the above-quoted sentences from paragraph 8(d) of the affidavit were not accurate. (Id. Ex. F). The Government advised that in fact Candyman members had three e-mail delivery options: (1) receipt of all e-mails; (2) receipt of only a daily digest of e-mails; and (3) "no e-mail receipt at all." (Id. at 1). A member who selected the no e-mail option would not receive any e-mails from the Candyman Egroup, its moderator, or its members. (Id.). Hence, it was not correct that every Candyman member received every e-mail from the group.

In its letter, the Government sought to explain the error. It explained that the representation that all members received all e-mails "was based on the hands-on experience of FBI Supervisory Special Agent Geoffrey Binney as an undercover member of the Candyman Egroup." (Id.). Binney, who has since left the FBI for the private

practice of law, was the lead undercover agent in the investigation. He joined the Candyman Egroup in an undercover capacity on January 2, 2001. The Government wrote in its letter:

> In his experience as a member, SSA Binney was never given an option for how to receive e-mail. After sending an e-mail requesting to become a member of the Egroup, he began receiving all e-mail traffic automatically.

(Id. at 1-2 (footnote omitted)). The Government also represented that an employee of Yahoo! Inc. ("Yahoo"), Lauren Guarnieri, had confirmed Binney's understanding that upon joining the group members started receiving e-mail automatically. (Id. at 2).

On January 2, 2003, the Government sent Perez a second letter acknowledging further error: the Government stated that paragraph 8(c), which represented that the undercover agent "was required to send an e-mail" to join the Candyman Egroup and did so, was also inaccurate. The letter forwarded logs from Yahoo and two FBI reports.

D. The Hearing

Perez moved to suppress the physical evidence seized and statements obtained as a result of the execution of the search warrant. I conducted an evidentiary hearing on January 15, 2003 and heard additional testimony and argument on February 19, 2003. Binney and another FBI agent, Special Agent Kristen Sheldon, testified for

the Government. Based on the evidence presented, I make the following findings of fact:

1. The Candyman Egroup

The Candyman Egroup operated from December 2000 until February 6, 2001, when it was shut down. (GX 1; McGoff Stip. ¶ 5).[2] It was initially operated by a company called eGroups, Inc. ("eGroups"). Yahoo acquired eGroups in August 2000 but did not begin converting the eGroups sites to its own product, "Yahoo! Groups," until late January 2001. (McGoff Stip. ¶ 3).

The main page of the Candyman website (as it existed shortly after Binney joined the Candyman Egroup) announced that "[t]his group is for People who love kids," and it told members that they could "post any type of messages" or "any type of pics and vids." (GX 1; see 1/15/03 Tr. at 15; Armenta Aff. Ex. E 8(b)). An additional description was given in the middle of the page: "Category: Top: Adult: Image Galleries: Transgender: Members."

A number of hyperlinks appeared near the top of the left side of the page, including, as the first link, "Subscribe." The other links listed were: "Messages," "Post," "Files," "Polls,"

---

[2] "GX" and "DX" refer to the Government's and defendant's exhibits, respectively, received into evidence at the hearing. "McGoff Stip." and "Hull Stip." refer to the stipulations between the parties as to the testimony, if called as witnesses, of Cathy A. McGoff, Yahoo's compliance manager, and Mark Hull, a Yahoo director of product management, respectively.

"Links," and "Chat." In the lower half of the middle of the page, certain addresses were given, including: "Subscribe: TheCandyman-subscribe@egroups.com." At the top of the right side of the page, under "Membership," were the hyperlinks "Modify" and "Unsubscribe." In the middle of the page on the right side, under "Options," the following appeared: "Not listed in directory," "Open membership," "Unmoderated," "Anyone can post," "Archives for members only," and "Email attachments are permitted." (GX 1).

Hence, a first-time visitor to the site in January 2001 certainly would have had some idea that the site provided access to child pornography. Although the page did not refer explicitly to child pornography or child erotica, it described the category as "Adult," "Image Galleries," and "Transgender." (GX 1). It also told visitors that the group was "for People who love kids" and advised that "any type of pics or vids" could be posted.

On the other hand, the page also offered links or tabs to several features that had the appearance of being -- and actually were -- text-based, in whole or in part. The "Chat" feature permitted members to engage in on-line text-based conversation. (1/15/03 Tr. at 80-82). The "Polls" feature let members take part in polls or surveys. (Id. at 23; GX 8). These two features were exclusively text-based. Other options were text-based in part but also permitted access to images. The "Links" option provided links

to other sites, where images could be found. The "Messages" option permitted members to access messages, to which images could be attached. The "Files" option permitted members to access files for downloading. (1/15/03 Tr. at 23, 80-81; GXs 6, 7, 8). Members could actively participate in the group, or they could merely "lurk" -- they could participate "passively" by reading what others had written without "talking" or answering the polls themselves. (1/15/03 Tr. at 81). Members could read through the chat sessions and see the results of polls without actually participating in them, and this would not be illegal activity. (Id. at 81-82). The first page did not show any images.

To view the contents of the website beyond the first page, a visitor to the site would have to subscribe first. (Id. at 76, 78-79). One could subscribe merely by entering an e-mail address and no fee was charged. (Id. at 79-80).

During the time that Binney was a member, i.e., from January 2, 2001 through February 6, 2001 (when the site was shut down (id. at 27)), he received 498 e-mails, all the e-mails transmitted from the Candyman Egroup during that period. Most of the e-mails were "text based in nature." (Id. at 30). Of the 498 e-mails, only a little more than 100 had files attached. (Id. at 26). Of those, most were "child erotica" -- pictures of "naked children" -- but they were not "child pornography." (Id. at 26, 30). The remaining files

-- "a substantial number" of the 100 -- were "child pornographic" in nature. (Id. at 26). Hence, only a small portion of the 498 e-mails of the period (less than 10%) actually transmitted child pornography.[3]

The Candyman Egroup had approximately 3,400 members at one point and perhaps as many as 6,300 subscribers. (Armenta Aff. Ex. F at 2 n.2; GX 11; see also 1/15/03 Tr. at 35, 118). Some individuals subscribed and then later unsubscribed. (1/15/03 Tr. at 145).

2. E-Mail Delivery Options

A prospective member of an Egroup run by eGroups (including the Candyman Egroup) could subscribe in one of three ways: (1) via the website by clicking on the "subscribe" button on the particular group's website; (2) via e-mail by sending an e-mail to the "subscribe address" listed on the front page of the particular group's website; or (3) via e-mail by sending an e-mail to the moderator at an address listed on the group's website. (Hull Stip. ¶¶ 3, 4, 5).

---

[3] Binney's testimony at the hearing is inconsistent with the information in the Berglas search warrant affidavit, which represented that of the 498 e-mails, approximately 287 had computer files attached, of which 105 contained "child pornography" while 183 contained "child erotica images." (Armenta Aff. Ex. E ¶ 8(f)). Of course, there is an error in the arithmetic, and Berglas did not base his statements on personal knowledge. Accordingly, I accept Binney's hearing testimony in this respect.

A subscriber who joined via the website was automatically presented with three options for the delivery of e-mail. By clicking on the "subscribe" button, he would be sent to a page that gave him three options: (1) he could have individual e-mail messages sent to his personal e-mail address (selected as the default choice); (2) he could have a daily digest of messages (described on the site's text as "many e-mails in one message") sent to his personal e-mail address; or (3) he could receive no e-mail messages at all (described as "Don't send me email, I'll read the messages at the Web site"). At the bottom of the page was a "join" button. (Id. ¶ 3 & Ex. A).

A subscriber who joined via e-mail to the "subscribe" address would be automatically "signed up" after responding to a confirmation request, if the group was an "open group" (as was the Candyman group (GX 1)). A subscriber who joined via e-mail to the moderator was not automatically signed up; rather, the moderator could choose to subscribe the individual, deny or ignore the request, or send a further invitation. For both e-mail subscription methods, no e-mail delivery options were provided; rather, the default setting was that the new member would start receiving all e-mails. A member could change to a different e-mail option by clicking on the "modify" button on the first page of the website. (Hull Stip. ¶¶ 3, 4, 5, 6).

3. Binney Joins

When he joined the Candyman Egroup on January 2, 2001, Binney had been with the FBI for eight years, all in the Houston division. He had spent two years on the "Innocent Images" project, primarily working undercover on-line to investigate individuals who were seeking to meet children for unlawful purposes. (1/15/03 Tr. at 2-6). Binney believed that the FBI was spending "an awful lot of time on-line," and that the effort was not "as productive" as it could have been. (Id. at 8-9). In addition, he wanted to target individuals who were seeking to exploit younger children, i.e., children who were too young to go on-line themselves. (Id. at 9). In the fall of 2000, Binney began to look for an opportunity for an on-line, undercover child pornography investigation, and this effort eventually led to Candyman. (Id. at 11).

Binney learned of the Candyman Egroup through a link in an on-line newsletter called "Lolitanews.com." Subscribers to the Lolitanews on-line newsletter apparently did not trade images but only engaged in "chatting" and posting of links, and Binney believed this was "constitutionally protected" activity. (Id. at 12, 82, 85).

After subscribing, Binney began exploring the Candyman site. He found that the site "contained a place where child pornography pictures and videos[] could be stored and for the users to download [them]." (Id. at 21). At some point, Binney clicked on the "modify" button, but nothing happened. (Id. at 26-27).

As the Yahoo logs show, Binney subscribed to Candyman via the website. The logs show:

> gobannon@usa.net, Jan 02 2001 12:53 PM, Subscribed,gobannon@usa.net, via web from 24.162.50.185.

The parties agree that this log entry related to the Candyman website and "gobannon@usa.net" was Binney's undercover e-mail address. (McGoff Stip. ¶ 4 & Ex. A; Hull Stip. ¶¶ 7, 8). Hence, Binney must have been presented with the three delivery options, and I find that, in fact, he was presented with the delivery options. (See 1/15/03 Tr. at 48 (Binney conceding that "it's at least probable that I joined via the web instead of the e-mail"); id. at 49).

Two other facts support this conclusion. First, Binney does not have a record of sending an e-mail to join. He testified that he normally would have printed and saved any e-mails he sent in an undercover operation such as this. Yet, he did not have a copy of any e-mail that he sent to subscribe to the Candyman Egroup. Likewise, he did not prepare a 302 or other written record of sending such an e-mail. (1/15/03 Tr. at 64-65).

Second, the FBI itself reached the same conclusion. The Cyber Division of the FBI conducted an investigation, reviewed the Yahoo/eGroups records and other materials, and issued two reports, both dated December 12, 2002, on the issue of how Binney joined the Candyman Egroup. In one report, the FBI concluded: "[W]e have no

information to dispute [Yahoo's] claim that . . . Binney must have subscribed via the website, and that he must have been presented with email delivery options." (DX B at 6).

The other report detailed how the FBI, with the assistance of Yahoo personnel, reviewed the source code for the eGroups.com website -- the version that was, according to Yahoo, in effect at the time Binney joined. The agents were shown "a more detailed version of the log data than what was previously provided." (DX A at 3). The report continued:

> Specifically, the log data was shown with one additional piece of information: the filename of the source code file that generated the log entry. This pointed specifically to a file "subscribe.c," which was used by the web site to present email delivery options to the user, and then to confirm the user's selection. . . . The log entry is generated only as a result of clicking on a button (the text of the button can vary, based on context) on the subscribe page, and the subscribe page always provides email options.

(Id. (emphasis added)). The report found that "it must be concluded based on the log data that Mr. Binney must have been presented with email delivery options." (Id. at 4).

4. Indications of the Existence of Delivery Options

Binney and FBI Special Agent Kristen Sheldon, who took over the case from Binney, knew or should have known, before the search warrant affidavit was executed in this case on March 1, 2002, that Candyman members had e-mail delivery options. At a minimum,

they knew that it was an open question. I make these findings based on the following:

First, as discussed above, Binney actually joined via the website and thus he was actually presented with the page that gave him the three e-mail delivery options.

Second, between January 2, 2001 and March 6, 2001, Binney joined, in addition to Candyman, seven other groups operated by eGroups or Yahoo. In six of the seven, the Yahoo logs show that Binney joined "via web." No entry is given for the last of the seven. (2/18/03 Stip. ¶¶ 2, 3 & Ex. B). For each of these six websites, which he joined long before the search warrant affidavit was executed in this case, Binney was also presented with e-mail delivery options. (Id. ¶¶ 2, 3; 1/15/03 Tr. at 50).

Third, Binney testified that he explored the site after he joined. It is hard to imagine that he would not have clicked on the "subscribe" button at some point, as he testified he did with the "modify" button and certain hyperlinks. (1/15/03 Tr. at 27). One would expect that an FBI agent acting in an undercover capacity would have clicked on the "subscribe" button as well, and that he would have explored thoroughly the process by which members came to receive e-mails, given the significance of the issue of whether members

received e-mails.[4] If he had clicked on the "subscribe" button, he would have been sent to the page that set out the three e-mail delivery options -- one of which was no e-mail.[5]

Fourth, on February 9, 2001, Yahoo produced certain documents in response to a subpoena. (GXs 10, 11). These included a sheet, labeled "View/Edit User Attributes," that provided information about the user Mark Bates, the moderator of the Candyman Egroup. One of the items listed was: "Email preference: None." (GX 11). Although he testified that he could not recall seeing the document, Binney acknowledged that he did receive it, as part of a 58-page fax, in February 2001. (1/15/03 Tr. at 51-52). In fact, the document was the second and third page of the fax, and it was significant -- it concerned the group's moderator. The document should have raised a question as to whether there were e-mail delivery options.

Fifth, on January 18, 2002, Yahoo wrote Sheldon and produced additional information, including a computer disc, as well

---

[4] Binney also left "largely unexplored" certain other buttons and hyperlinks on the group's main page, including "Home," "Help," "MyGroups," "MyProfile," and "About Egroups." (Armenta Aff. Ex. F at 2 n.1).

[5] Common sense also suggest the existence of e-mail preferences in light of the widely-known problem of unsolicited e-mail, or spam. (See, e.g., United States v. Froman, Case No. CR H-02-0142, 3/22/02 Tr. at 46 (GX 3501-A) ("These are not unsolicited e-mails that everybody gets every day and we receive complaints about.")). At the bottom of the main page are links to eGroup's "Privacy Policy" and a link called "No Spam!" (GX 1).

as certain documents. Yahoo's letter and its four attached pages were received into evidence as GX 18. (Id. at 120, 149). The pages were printouts reflecting Yahoo "Group Administration Profiles" for Candyman and two other groups under investigation. (GX 18). The one-page group profile for the Candyman group showed that e-mail options existed. In a category for "Number of Subs[cribers]," the document reports: "3213 Normal (Single: 413 Digest: 60 NoMail: 2740)." (Id.). Hence, the document reported that there were 3,213 subscribers, of which 413 elected to receive single e-mails, i.e., all individual e-mails; 60 elected to receive a digest of e-mails; and 2,740 -- the vast majority -- elected to receive no e-mails. Similar group profiles were provided for two other groups, "shangri_la" and "girls12-16," and these pages contained the same information, showing the number of subscribers who were "NoMail." (Id.). These three group profiles did not contain a great deal of other information, and the mail preference breakdown was part of text that was important, including the total number of subscribers. The documents should have raised an issue as to the existence of e-mail delivery options.

Sixth, on January 24, 2002, a few days later, Sheldon met with Yahoo representatives, in a day-long meeting, to discuss the documents. Sheldon did not inquire about the entries in the documents regarding the e-mail delivery preferences. (1/15/03 Tr. at

102, 122, 125-26, 136). At some point, however, she and the Yahoo representatives discussed whether Yahoo groups provided members with e-mail delivery options; the Yahoo representatives told her that the Yahoo groups did have delivery options. (Id. at 126, 150-51). Sheldon testified this "caused us to ask him to kind of back up" because the "concept" of e-mail delivery options was "foreign at that time." (Id. at 151). Sheldon specifically asked whether options had been available for the eGroups groups as well, but the representatives were unsure and stated that they would get back to her. (Id. at 126, 150-51). Hence, as Sheldon agreed during her hearing testimony, the issue of whether there were e-mail delivery options under eGroups was an "open question." (Id. at 138, 150-51; see also 2/19/03 Tr. at 14-17).

5. The Draft Affidavit

In March of 2001, Binney started drafting an affidavit to be used in connection with an application for a search warrant. The concept was that the Houston division of the FBI would send the draft affidavit to other FBI field offices. (1/15/03 Tr. at 40-41, 127). Eventually Sheldon did so. (Id. at 127). Even though she did not hear back from the Yahoo representatives after the January 24, 2002 meeting, and even though she knew this was an "open question," she sent out the draft search warrant with the representation that all members automatically received all e-mails. (Id. at 138). The draft

was sent to FBI field offices around the country -- about 700 in the "first batch." (Id. at 146).

6. More Information Emerges As the Warrants Are Executed

On March 18, 2002, Sheldon interviewed Mark Bates, the former moderator of the Candyman Egroup. Bates told her that Candyman members could elect not to receive e-mail. She apparently did not believe him. (Id. at 139-40).[6]

In May 2002, Sheldon learned from an FBI agent in St. Louis that Yahoo had submitted an affidavit in a Candyman case stating that there had been e-mail delivery options. (Id. at 128).

At some point in mid-2002, the Government started to acknowledge in the various Candyman cases that the search warrant affidavits had contained an error: it was not correct that all members automatically received all e-mails. As a consequence, defendants in different Candyman cases moved to suppress evidence obtained as a result of the search warrants.

---

[6] This information from Bates -- that Candyman members could elect not to receive e-mails -- did not stop Sheldon from testifying at a suppression hearing two days later that, in substance, all members received e-mails. (1/15/03 Tr. at 141-42). Sheldon apparently did not believe Bates, at least in part because Bates's information was inconsistent with what Binney had told her and because she felt Bates, who was in custody and was facing charges, was untrustworthy. (Id. at 142-44). Likewise, Binney testified that when this information was relayed to him, he also rejected it because he did not believe Bates was trustworthy. (Id. at 72-73).

E. Binney's Explanation

Not surprisingly, Binney has had to explain his representation that all Candyman members received all e-mails. In an affidavit submitted in opposition to a motion to suppress in another Candyman case in July 2002, Binney gave the following explanation:

> First, I went to the Candyman website and copied the E-mail address of the moderator, which was listed on the web page. I then left the website, went to my web mail provider, and sent an E-mail to the Candyman moderator asking to join the group. During this entire process, I was never given any opportunity to select any mail delivery options. Nor was there any mention of such options during the joining phase.

(DX C ¶ 4).[7] Binney has testified several times in other Candyman cases and provided a similar explanation of subscribing via e-mail and not being presented with e-mail delivery options. (1/15/03 Tr. at 52-53). He also included a similar explanation in the search warrant affidavit itself. (Armenta Aff. Ex. E ¶ 8(c)). In this case, Binney testified:

> I recall seeing the subscribe e-mail address on the bottom, and copying and pasting that e-mail address, and then going to my web based e-mail provider, which was usa.net as it's indicated on the top there, and then sending an e [--],

---

[7] When Binney executed the affidavit, he knew that motions to suppress had been filed attacking the validity of the searches and he knew also that Yahoo was claiming that members of the groups did have e-mail delivery options. (1/15/03 Tr. at 54). He knew the issue of the availability of e-mail delivery options was an important one. (Id. at 55).

> pasting the e-mail address in the "to" column, and then saying something to the effect of sign me up, and then hitting "send."

(1/15/03 Tr. at 17). This is also essentially the explanation that the Government gave to defense counsel when it first gave notice of the error. (Armenta Aff. Ex. F).

F. Binney's Explanation of His Explanation

It is now clear that Binney's explanation for his erroneous belief that all Candyman members received all e-mails is wrong, for the recently-produced Yahoo logs show that Binney did not join via e-mail, but that he did so via the website and that he was presented with the e-mail options.

Hence, Binney has now had to explain not only why he made the initial error but also why his explanation for that initial error is also wrong.[8] When asked to explain the basis for his "belief" that all members received the same e-mails he received, he testified:

> It was almost entirely based on my experience in the site, very little bit based on a conversation that I had with Ms. Guarnieri, and also based on the logs, the first set of logs

[8] In fact, the record includes a four-page, single-spaced "analysis" that Binney prepared discussing the question of the existence of e-mail delivery options and the conflict between his testimony and that of a Yahoo representative who explained that there were e-mail delivery options. Binney wrote: "I feel as though we are probably looking at all the evidence we are ever going to get with respect to the Email options." He goes on to discuss "four possible explanations as to how this discrepancy could have occurred. They are that Yahoo is lying, Yahoo is mistaken, I am mistaken, or I am lying." (DX D; see 1/15/03 Tr. at 56-57).

> that we got in August or so of 2001. . . . There was nothing in the logs to indicate that any member was any different than any of the other members except for dates that they had subscribed and unsubscribed.

(1/15/03 Tr. at 44-45). When asked whether he had assumed that all members received all e-mails automatically, he responded: "That was my recollection as -- that was entirely based on my experience in the group." (Id. at 60). Later, he reiterated that "I assumed everybody had the same joining process as I did" and later again that "my belief that . . . all members got all e-mails was almost entirely based on my experience." (Id. at 69, 87).

When asked whether the "easiest way to know whether there were [e-mail delivery] options" would have been to look at the site, Binney responded: "Or to send subpoenas and court orders to the provider." (Id. at 60). He added: "I think you're presupposing that I thought there was something to find. I didn't feel like there was anything to look for so I was subpoenaing Yahoo and sending court orders . . . ." (Id. at 61).

Notwithstanding the evidence that his explanation for how he came up with his erroneous belief that all members received all e-mails is wrong, Binney testified: "I don't know that I will ever, short of Yahoo producing some sort of video of me entering into the site, I don't know that I will ever believe a hundred percent that I didn't enter the way I believe I entered." (Id. at 48). Despite the

evidence that he must have been presented with e-mail delivery options not only for the Candyman site but for six other groups, Binney testified that "the first time I even heard the word[s] e-mail delivery options or something to that nature was after the interview of Mark Bates, the Candyman himself," referring to the March 18, 2002 interview of Bates conducted by Sheldon. (Id. at 43; see also id. at 87 (Binney testifying that "it wasn't until the conversation I had with Special Agent Sheldon about her interview of Mr. Bates" that he learned of the existence of delivery options)). He continued to assert that he does not recall seeing anything about e-mail delivery options when he subscribed to Candyman or when he initially explored the site after joining. (Id. at 42).

Sheldon gave conflicting testimony as to what Binney told her. She testified in March 2002 at a hearing in another case in Texas that she was told by Binney that he had joined by visiting the website and typing in his e-mail address at the website:

> Q. You said [Agent Binney] became a member around January 2nd of 2001; is that correct?
>
> A. Yes, it is.
>
> Q. How did he become a member?
>
> A. He simply visited the Egroup's website and typed in his email address and gained access to the group.

(GX 3502-C at 27). In this case, although she was initially less precise in her testimony, she eventually acknowledged that Binney

told her he joined by typing in his e-mail address at the website. (1/15/03 Tr. at 134-35).

Later, however, on the second day of the hearing, she testified that Binney told her he joined via e-mail:

> THE COURT: And when you say he joined, meaning he joined via e-mail?
>
> THE WITNESS: He joined the -- the logs indicate that he joined web, via web.
>
> THE COURT: He joined via web but was he telling you that, that he had joined via the web or via e-mail?
>
> THE WITNESS: E-mail.
>
> THE COURT: He was telling you that he joined via e-mail and now it appears he joined via the web?
>
> THE WITNESS: That's correct.

(2/19/03 Tr. at 18).

Finally, I discount Binney's reference to the conversation with Lauren Guarnieri of Yahoo as a basis for his mistaken belief. As he acknowledged, his belief was based "almost entirely" on his experience in joining and "very little" on the conversation. Binney testified that Guarnieri "couldn't have been really any more unhelpful than she was." (1/15/03 Tr. at 32). Moreover, the conversation was focused on a different subject -- the dates when individuals were members, "start dates and end dates and things like

that" -- and it was in that context that he asked her a question. (Id. at 37). Binney testified as follows:

> Not having any start dates for any of these people, I asked her, I said, Well, are these people like me? I have e-mails that I thought at that point went to every member of the group and since I couldn't tell when they started, if I had an e-mail from Joe at AOL.com on January 10, was it safe to say that they received the same e-mails I did between the 10th and the day it shut down? And she said yes.

(Id.). The question to Guarnieri was an ambiguous one and I conclude that Guarnieri did not say that all members automatically started receiving all e-mails upon joining -- a statement that would have been wrong. She was not asked whether new members were offered e-mail delivery options.

G. The Evidence as to Perez

The search warrant contained only three paragraphs specifically about Perez. It reported that information obtained from Yahoo and AOL (an internet service provider) as well as from the Department of Motor Vehicles, the Postal Service, and other public records showed: (1) the e-mail address "navajablade@ aol.com" belonged to an individual who joined the Candyman Egroup; (2) "navajablade@aol.com" was registered in the name of "Harvey Perez," and (3) "Harvey Perez" resided at one of the premises listed in the search warrant. (Armenta Aff. Ex. E ¶¶ 8(i), 9(e), 10(e)).

Yahoo logs and documents indicate that the user with the e-mail address "navajablade@aol.com" -- Perez -- subscribed via the website on January 29, 2001. (McGoff Stip. ¶ 8; Armenta Aff. ¶ 9 & Ex. H). He elected the "No Email" option. (Armenta Aff. Ex. H). The Yahoo logs do not contain any entries showing that the user "navajablade@aol.com" posted any messages, uploaded any files, or unsubscribed. (McGoff Stip. ¶ 8). Hence, Perez was a member for some nine days, as the site shut down on February 6, 2001.

Perez states in his affidavit that he never downloaded any material from the Candyman website. Yahoo did not keep a record of this kind of activity. (Perez Aff. ¶ 5; see Armenta Aff. ¶ 11 & Ex. G ¶ 13).

As the Government acknowledged at oral argument, there is nothing in the record to indicate that Perez did anything more with respect to the Candyman site than subscribe. (2/19/03 Tr. at 30).

DISCUSSION

A. Applicable Law

To protect the "right of the people to be secure in their persons, houses, papers, and effects," the Fourth Amendment prohibits "unreasonable searches and seizures" and mandates that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. amend. IV. In Franks v. Delaware, 438 U.S. 154 (1978), the Supreme Court ruled that a defendant may

challenge the validity of a search warrant issued on the basis of an affidavit that contained false information. The Court held that if a defendant shows, by a preponderance of the evidence, that the affidavit contained deliberately or recklessly false or misleading material, and that the "affidavit's remaining content" is insufficient to establish probable cause when the false material is set aside, the search warrant must be voided and the evidence suppressed. Id. at 155-56; accord United States v. Canfield, 212 F.3d 713, 717-18 (2d Cir. 2000). In certain circumstances, an affidavit may also be misleading if material information is omitted. Canfield, 212 F.2d at 718; Rivera v. United States, 928 F.2d 592, 604 (2d Cir. 1992).

Here, as the Government concedes, the search warrant affidavit contained false information: it was not true, as the affidavit alleged, that all Candyman members automatically received all e-mails and therefore it was not true that all Candyman members automatically received the e-mails that contained child pornography. In fact, as the Government now concedes, Candyman members had three delivery options, including a no e-mail option. Hence, two principal issues are presented: (1) whether the false statements or omissions in the affidavit were made deliberately or with reckless disregard for the truth, and (2) if so and the false statements are set aside,

whether the "corrected" affidavit would support a finding of probable cause.

In discussing the applicable legal principles, first I address the scienter requirement and in particular what constitutes "recklessness" for these purposes; second, I discuss the concept of probable cause; and third, I set forth some additional Fourth Amendment principles that are relevant to the inquiry at hand.

1. Scienter

The Fourth Amendment does not require that "[e]very statement in a warrant affidavit . . . be true." United States v. Trzaska, 111 F.3d 1019, 1027 (2d Cir. 1997). That is, of course, because law enforcement officers often must rely on hearsay information, tips from informants, and information sometimes "garnered hastily." Franks, 438 U.S. at 164 (citing United States v. Halsey, 257 F. Supp. 1002, 1005 (S.D.N.Y. 1966)). Rather, as the Supreme Court explained in Franks, the affidavit must be:

> "truthful" in the sense that the information put forth is believed or appropriately accepted by the affiant as true. It is established law, that a warrant affidavit must set forth particular facts and circumstances underlying the existence of probable cause, so as to allow the magistrate to make an independent evaluation of the matter.

438 U.S. at 164 (citations omitted). Consequently, a defendant may challenge a search warrant affidavit on this basis only if the "inaccuracies or omissions are the result of the affiant's deliberate

falsehood or reckless disregard for the truth." Canfield, 212 F.3d at 717-18 (quoting United States v. Salameh, 152 F.3d 88, 113 (2d Cir. 1998)). An inaccuracy that is the result of negligence or innocent mistake is insufficient. Franks, 438 U.S. at 171; see 2 Wayne R. LaFave, Search & Seizure § 4.4 (3d ed. 1996).

As for omissions, they are less likely to present "'a question of impermissible official conduct'" because allegations of omissions may result in "'endless conjecture about investigative leads, fragments of information, or other matters that might . . . have redounded to defendant's benefit" had they been included. United States v. Lopez, No. 96 Cr. 105 (RSP), 1997 WL 567937, at *2 (N.D.N.Y. Sept. 11, 1997) (quoting United States v. Atkin, 107 F.3d 1213, 1217 (6th Cir. 1997)). Nonetheless, the Fourth Amendment requires that a neutral and detached magistrate must review the facts to determine the existence of probable cause, and "[i]t follows that a police officer cannot make unilateral decisions about the materiality of information." Wilson v. Russo, 212 F.3d 781, 787 (3d Cir. 2000). Hence, material omissions made with an intent to mislead or with a reckless disregard for the truth also must be corrected before the court considers the sufficiency of a search warrant affidavit. Id. at 787-88; see also Canfield, 212 F.3d at 718.

Little precedent exists to define "reckless disregard" in the search warrant context. The Franks Court refers to information

that is not "appropriately accepted by the affiant as true," Franks, 438 U.S. at 165, but "[u]nfortunately" it gives "no guidance" beyond observing that "'negligence or innocent mistake [is] insufficient.'" United States v. Davis, 617 F.2d 677, 694 (D.C. Cir. 1979) (quoting Franks, 438 U.S. at 171). Courts in this circuit have made the same observation. See, e.g., Rivera v. United States, 728 F. Supp. 250, 258 (S.D.N.Y. 1990) (Mukasey, J.) ("Judicial precedent has established this standard of deliberate falsehood and reckless disregard to support a Franks challenge, but research has disclosed no case defining 'reckless disregard' in this setting."), aff'd in relevant part, 928 F.2d 592, 604 (2d Cir. 1991).

In Rivera, Judge Mukasey applied a "serious doubt" standard:

> The words themselves . . . suggest that "reckless disregard for the truth" means failure to heed or to pay attention to facts as [the DEA investigator affiant] knew them to be. If [the affiant] made statements which failed to take account of the facts as he knew them, or which he seriously doubted were true, that would show reckless disregard for the truth.

Rivera, 728 F. Supp. at 258 (emphasis added). Variations of the "serious doubt" standard, imported from the First Amendment context, St. Amant v. Thompson, 390 U.S. 727, 731-32 (1968), have been widely adopted by federal courts. That is, "[t]o prove reckless disregard for the truth, the defendants had to prove that the affiant 'in fact entertained serious doubts' as to the truth of his allegations."

United States v. Whitley, 249 F.3d 614, 621 (7th Cir. 2001) (citation omitted); United States v. Williams, 737 F.2d 594, 602 (7th Cir. 1984) (agreeing with United States v. Davis, 617 F.2d at 694, holding that the First Amendment definition should be applied by analogy in the Franks context).

There is a corollary to the "serious doubt" standard: "Because states of mind must be proved circumstantially, a fact finder may infer reckless disregard from circumstances evincing 'obvious reasons to doubt the veracity of the allegations.'" Whitley, 249 F.3d at 620; see, e.g., United States v. Schmitz, 181 F.3d 981, 986-87 (8th Cir. 1999) ("[T]he test for determining whether an affiant's statements were made with reckless disregard for the truth is not simply whether the affiant acknowledged that what he [or she] reported was true, but whether, viewing all the evidence, the affiant must have entertained serious doubts as to the truth of his [or her] statements or had obvious reasons to doubt the accuracy of the information he [or she] reported."); United States v. Ranney, 298 F.3d 74, 78 (1st Cir. 2002) (same); Beard v. City of Northglenn, 24 F.3d 110, 116 (10th Cir. 1994) (same); Wilson, 212 F.3d at 787-88 (distinguishing between assertions and omissions, and in defining the former, "we have borrowed from the free speech arena and equated reckless disregard for the truth with a 'high degree of awareness of [the statements'] probable falsity'" and noting "reckless disregard

for the truth is exhibited when expressing that which was not 'believed or appropriately accepted' as true" (citations omitted)); United States v. Senchenko, 133 F.3d 1153, 1158 (9th Cir. 1998) ("high degree of awareness of probable falsity").

As to omissions, as the Third Circuit has explained, they "are made with reckless disregard if an officer withholds a fact in his ken that 'any reasonable person would have known that this was the kind of thing the judge would wish to know.'" Wilson, 212 F.3d at 788 (quoting United States v. Jacobs, 986 F.2d 1231, 1235 (8th Cir. 1993)); see also Rivera, 928 F.2d at 604 ("[R]ecklessness may be inferred where the omitted information was 'clearly critical' to the probable cause determination." (citations omitted)). In Jacobs, for example, the Eighth Circuit concluded that the officer acted with reckless disregard when he told the magistrate that a drug-sniffing dog showed "interest" in the defendant's bag, but omitted the information that the dog had not gone into "alert," as it was trained to do if drugs were present. 986 F.2d at 1234. In Wilson, the Third Circuit held that an officer's failure to disclose the differential in height between the defendant (5'11") and the description of the assailant as reported by the two victims (between 6'3" and 6'5") was reckless, for, as the court concluded, any reasonable person would have wanted to know this fact. 212 F.3d at 788.

Hence, to prevail on the first prong of the Franks test, Perez must prove by a preponderance of the evidence that (1) the drafters of the affidavit made the statement that all Candyman members automatically received all e-mails with knowledge that the statement was false, (2) they had a serious doubt as to the truth of the statement when they made it, or (3) they had obvious reason to doubt the veracity of the statement. As to the omitted information that Candyman members had e-mail delivery options, including the choice of receiving no e-mail, Perez must prove by a preponderance of the evidence that any reasonable person would have known that this was the kind of information that the magistrate judge would have wanted to know.

2. Probable Cause

If a court decides that false statements or material omissions in a search warrant affidavit were made knowingly or recklessly, the court must then "correct" the affidavit by "disregard[ing] the allegedly false statements" or filling in the omitted information and then proceed to "determine whether the remaining portions of the affidavit would support probable cause to issue the warrant." Canfield, 212 F.3d at 718 (citations and internal quotations omitted). If, upon a de novo review, the court determines that the "corrected" affidavit provides a sufficient basis to find probable cause, the court must uphold the warrant and deny

suppression. Id. "The ultimate inquiry is whether, after putting aside erroneous information and material omissions, 'there remains a residue of independent and lawful information sufficient to support probable cause.'" Id. (quoting United States v. Ferguson, 758 F.2d 843, 849 (2d Cir. 1985)).

A search warrant may issue only "upon probable cause," U.S. Const. amend. IV, and probable cause exists only where the known facts and circumstances are sufficient to support a "reasonable belief" that "contraband or evidence of a crime will be found." Ornelas v. United States, 517 U.S. 690, 696 (1996). A magistrate presented with a search warrant application must make "a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). The affidavit must provide sufficient facts to permit the magistrate to draw the inferences necessary to a finding of probable cause, and the magistrate must not merely rely without question on the assertions in the affidavit but must make an independent evaluation. Giordenello v. United States, 357 U.S. 480, 485-86 (1958); see Gates, 462 U.S. at 239 ("Sufficient information must be presented to the magistrate to

allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others.").

In practice, the probable cause standard, however rendered, is as familiar as it is unhelpful. The Supreme Court has called it "a fluid concept -- turning on the assessment of probabilities in particular factual contexts -- not readily, or even usefully, reduced to a neat set of legal rules." Gates, 462 U.S. at 232. The Court has also cautioned that "the evidence thus collected must be seen and weighed not in terms of library analysis by scholars, but as understood by those versed in the field of law enforcement." Id. (quoting United States v. Cortez, 449 U.S. 411, 418 (1981)).

Indeed, although probable cause is a "mosaic" that is "multifaceted" and a "fluid concept," the standard takes its "substantive content" from the particular context in which the standard is being assessed. Ornelas, 517 U.S. at 696-98 (citing, inter alia, Brinegar v. United States, 338 U.S. 160, 175 (1945) ("The standard of proof [for probable cause] is . . . correlative to what must be proved.") and Ker v. California, 374 U.S. 23, 33 (1963) ("This Court[] [has a] long-established recognition that standards of reasonableness under the Fourth Amendment are not susceptible of Procrustean application"; "[e]ach case is to be decided on its own facts and circumstances." (internal quotations omitted))). In other

words, in the balancing that every Fourth Amendment challenge requires, "to safeguard citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime" and still "give fair leeway for enforcing the law in the community's protection," the particular context -- that is, "what must be proved" -- must be kept in mind. Brinegar, 338 U.S. at 176.

3. Additional Fourth Amendment Considerations

I set forth some additional Fourth Amendment principles that are of particular importance to this case.

a) Reasonableness

The "central requirement" of the Fourth Amendment is "reasonableness." Koch v. Town of Brattleboro, Vt., 287 F.3d 162, 166 (2d Cir. 2002) (quoting Illinois v. McArthur, 531 U.S. 326, 330 (2001)). The "touchstone" of reasonableness is "measured in objective terms by examining the totality of the circumstances." Ohio v. Robinette, 519 U.S. 33, 39 (1996). Generally, a Fourth Amendment examination "requires a contextualized reasonableness analysis that seeks to balance the intrusion on privacy caused by law enforcement against the justification asserted for it by the state." Lauro v. Charles, 219 F.3d 202, 209 (2d Cir. 2000) (citing Graham v. Connor, 490 U.S. 386, 396 (1989)). Though reasonableness is most often considered in the context of warrantless searches or seizures, reasonableness is nonetheless required even when a warrant is

procured. Cf. United States v. Ramirez, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant." (citation omitted)).

The Fourth Amendment requires reasonableness not only as to whether a search should be "conducted at all, but also to ensure reasonableness in the manner and scope of searches and seizures that are carried out." Lauro, 219 F.3d at 211. In addition, "the reasonableness of the police's actions in conducting a search or seizure must be judged, in part, through an assessment of the degree to which those actions further the legitimate law enforcement purposes behind the search or seizure." Id.

b) Presumption of Validity

While "[i]t is a basic principle of Fourth Amendment law that searches and seizures inside a home without a warrant are presumptively unreasonable," Payton, 445 U.S. at 586 (internal quotations omitted), when a search is conducted pursuant to a valid warrant, the reverse is true. "There is, of course, a presumption of validity with respect to the affidavit supporting the search warrant." Franks v. Delaware, 438 U.S. 154, 171 (1978). This presumption stems from a belief in the function of the examining magistrate as a neutral gatekeeper, and it encourages law enforcement to seek warrants; "the preference for warrants is most appropriately

effectuated by according 'great deference' to a magistrate's determination." United States v. Leon, 468 U.S. 897, 914 (1984) (citation omitted).

c) The First Amendment and Child Pornography

The Supreme Court has held that no higher probable cause standard applies when the First Amendment is implicated by a Fourth Amendment search or seizure. The Supreme Court rejected this notion in New York v. P.J. Video, Inc., 475 U.S. 868, 870-71 (1986) (retreating from language in prior cases that a court must act with "scrupulous exactitude" in this context (citing Stanford v. Texas, 379 U.S. 476, 481-485 (1965); Maryland v. Macon, 472 U.S. 463 (1985))). Moreover, child pornography is not considered presumptively protected activity. "Because of the state's interest in protecting children from sexual exploitation, child pornography may be banned regardless whether it fails the test for obscenity." United States v. Jasorka, 153 F.3d 58, 60 (2d Cir. 1998).

The Supreme Court has repeatedly recognized the state's compelling interest in this area, enumerating several reasons why the government is "entitled to greater leeway in the regulation of pornographic depictions of children." New York v. Ferber, 458 U.S. 747, 756 (1982); see Sarah Sternberg, Note, The Child Pornography Prevention Act of 1996 and the First Amendment: Virtual Antitheses, 69 Fordham L. Rev. 2783, 2792 (2001). The Court has upheld laws that

ban simple possession of child pornography, citing the need "to dry up the child pornography market." Osborne v. Ohio, 495 U.S. 103, 110 (1990) ("[I]t is now difficult, if not impossible, to solve the child pornography problem by only attacking production and distribution."). The Court noted that the state's "ban on possession and viewing encourages the possessors of these materials to destroy them," helping to eliminate images that "permanently record the victim's abuse" and may be used by pedophiles to seduce other children. Id. at 111.

d) The Home

The search warrant here targeted nine different homes, including Perez's home. Courts have long observed that in Fourth Amendment jurisprudence, the home has something of a "special status" and have "emphasized the sanctity of the private home, and the particular gravity the Fourth Amendment accords to government intrusions on that privacy." Lauro, 219 F.3d at 211. The Supreme Court has repeatedly declared that "[t]he Fourth Amendment embodies [the] centuries-old principle of respect for the privacy of the home," Wilson v. Layne, 526 U.S. 603, 610 (1999), and has noted the "'overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic.'" Id. (quoting Payton v. New York, 445 U.S. 573, 601 (1980)). Indeed, "'physical entry of the home is the chief evil against which the

wording of the Fourth Amendment is directed'" and it is "the warrant procedure [that] minimizes the danger of needless intrusions of that sort." Payton, 445 U.S. at 586 (quoting United States v. United States District Court, 407 U.S. 297, 313 (1972)).

On the other hand, of course, as Justice Jackson observed for the Court in Johnson v. United States, 333 U.S. 10, 14 (1948):

> Crime, even in the privacy of one's own quarters, is . . . of grave concern to society, and the law allows [evidence of] such crime to be reached on proper showing. The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance. When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent.

(footnotes omitted).

e) The Good Faith Exception

The Government initially took the position in opposing Perez's motion that even if the search warrant was not supported by probable cause, the motion to suppress had to be denied because the officers who executed the search acted in good faith reliance on the warrant. (Gov't's Mem. in Opp. to Def.'s Mot. to Suppress at 29-31). The Government now retreats from that position (2/19/03 Tr. at 21), as it must.

In the event of a successful challenge under Franks, the good faith exception set forth in United States v. Leon, 468 U.S. 897 (1984), does not apply. This much the Court in Leon made clear: "Suppression therefore remains an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." Leon, 468 U.S. at 923 (citing Franks).[9]

Likewise, although the Government also argued initially that the motion to suppress had to be denied because the affiant, Berglas, was acting in good faith and "simply relay[ing]" the inaccurate information provided by Binney (Gov't's Mem. in Opp. to Def.'s Mot. to Suppress at 19), it has retreated from that position as well. (2/19/03 Tr. at 21).

---

[9] The Second Circuit has recognized this relationship between Leon and Franks. See United States v. Moore, 968 F.2d 216, 222 (2d Cir. 1992) (noting that "[t]he good faith exception has parameters, in particular four circumstances set out in Leon, in which it does not apply," including "where the issuing magistrate has been knowingly misled"); United States v. Reilly, 76 F.3d 1271, 1273 (2d Cir. 1996) ("It bears emphasis, however, that the good faith exception requires a sincerely held and objectively reasonable belief that the warrant is based on a valid application of the law to all the known facts. Good faith is not a blanket excuse for any police behavior. A warrant is not a general hunting license, nor is it a mantle of omnipotence, which cloaks its holders in the King's power to 'do no wrong.' And perhaps most important, it is not an excuse if the police are not frank with the magistrate in proceedings to obtain the warrant -- proceedings that are typically ex parte. See Franks v. Delaware, 438 U.S. 154, 155-56 (1978).").

There simply is no support for the Government's initial position, where the source of the information is another government agent. The Government cannot insulate one agent's deliberate or reckless misstatement in an affidavit merely by relaying it through another agent personally ignorant of its falsity. See Franks, 438 U.S. at 164 n.6; United States v. Wapnick, 60 F.3d 948, 956 (2d Cir. 1995) (noting that "when the informant is himself a government official, a deliberate or reckless omission by the informant can still serve as grounds for a Franks suppression" because "[o]therwise, the government would be able to shield itself from Franks suppression hearings by deliberately insulating affiants from information material to the determination of probable cause"); see also United States v. Whitley, 249 F.3d at 621 ("Subsequent decisions have slightly expanded the Franks principle to include the state of mind not only of the affiant, but also of those governmental agents from whom the affiant received false information incorporated into the affidavit. In other words, the validity of the search is not saved if the governmental officer swearing to the affidavit has incorporated an intentional or reckless falsehood told to him by another governmental agent."); United States v. Brown, 298 F.3d 392, 408 (5th Cir. 2002) (same).

B. Application

In applying the law to the facts, first, I address the issue whether the agents knowingly or recklessly made the false statement that all Candyman members automatically received all e-mails and omitted the information that Candyman members had e-mail delivery options; second, I consider whether, with the false information set aside and the omitted information provided, the "corrected" affidavit supports a finding of probable cause; and third, I address the decisions in other Candyman cases that have rejected challenges to the searches in question.

1. The Agents' State of Mind

I conclude that the law enforcement agents acted recklessly in submitting an affidavit that contained the false information that all Candyman members automatically received all e-mails, including e-mails that forwarded images of child pornography, for the agents had serious doubt as to the truth of the statements or, at a minimum, they had obvious reasons to doubt their veracity. Moreover, I conclude that the agents also acted recklessly in omitting the information that Candyman members in fact had e-mail delivery options, including the option of receiving no e-mail at all. I reach these conclusions for the following reasons.

First, Binney was presented with e-mail delivery options when he joined Candyman and he was presented with those options again on six other occasions when he joined other websites. Clearly, then,

he had obvious reason to doubt the veracity of the representation that all members automatically received all e-mails. Although he steadfastly clung to the explanation that his "experience" had led him to conclude that, like him, all members were sent all e-mails without any say in the matter, his "experience" was in fact the opposite -- he was offered a choice.

Second, the information as to e-mail delivery options was right there, on the website, available to Binney with the click of a mouse. It is hard to imagine, as he explored the site in his undercover capacity and clicked on various buttons (as he testified he did), that he did not also click on the "subscribe" button. He must have done so, and he must have seen the delivery options. Thus, again, he had obvious reason to doubt the veracity of the representation that members automatically received all e-mails.

Third, the Yahoo documents and representatives provided an "obvious" basis to doubt the veracity of the representation. The February 9, 2001 production included a document regarding the Candyman moderator that referred to "Email preferences: None." (GX 11). Although this document, by itself, was ambiguous, in the context of all the evidence, it provided some clue that there might be e-mail options.

More significantly, the January 18, 2002 production included a group profile document that reported: "3213 Normal

(Single: 413 Digest: 60 NoMail: 2740)." Two similar profiles were included for other websites, again reporting that many subscribers had opted for "NoMail." (GX 18). These profiles were attached to the cover letter of the production and did not contain a great deal of other information. This was a much stronger indication that there were e-mail options, including a "NoMail" option.

Even assuming these documents also were ambiguous, again there was more: Yahoo representatives specifically told Sheldon at the January 24, 2002 meeting that Yahoo group members had delivery options, Sheldon asked about the eGroups groups, and they told her they did not know. Sheldon acknowledges that it was an "open question" whether eGroups groups had e-mail delivery options. Although the agents deny that they saw the documents or understood the significance of the entries, the documents together with the discussion at the January 24th meeting surely gave them obvious reason to doubt the truth of the statement that all members automatically received all e-mails.

Fourth, as the Second Circuit has held, recklessness may be inferred where information "clearly critical" to the probable cause determination has been omitted. See Rivera, 928 F.2d at 604. In other words, although the inquiry into the agents' state of mind is distinct from the inquiry into the materiality of the false statements to probable cause, the two are related. See, e.g., United

States v. Castillo, 287 F.3d 21, 26 n.5 (1st Cir. 2002) (noting that materiality is connected to the state of mind inquiry by the "closeness of the probable cause question"). Here, the issue of whether members automatically received all e-mails was "clearly critical" to a finding of probable cause. Although the Government takes the position that probable cause exists even without the representation, at the very least the question is a much closer one and, as I hold below, no probable cause exists without it. (See 1/15/03 Tr. at 62 ("THE COURT: If someone in fact did not get e-mails, then there would be no real basis to prosecute such a person? [BINNEY]: That's correct . . . ."). At a minimum, this was information that the magistrate judge would have wanted to know.

Finally, I conclude that the agents acted recklessly also because there was absolutely no support for their assertion that all members automatically received all e-mails. There is nothing in the record that could have led the agents to reach this conclusion. Binney's assertion that he erroneously believed that all members automatically received all e-mails because that was his "experience" is belied by the evidence -- including the Yahoo logs that show that his "experience" was the opposite, the absence of a copy of the alleged e-mail by which he joined or a 302 describing such an e-mail, the conclusion in the FBI Cyber Division's reports that Binney must have been presented with e-mail delivery options, the likelihood that

Binney found the delivery options by exploring the site, and even the initial testimony of Agent Sheldon. Binney gave an elaborate explanation of his "experience," in great detail and without any hesitation or doubt, and yet it simply did not happen the way he says it did.

The Government argues that, at worst, the agents made the false statement negligently, and that Perez is merely complaining that the agents should have done a more thorough investigation, when the law is clear that a failure to fully investigate is not sufficient to show reckless disregard. (Gov't's Post-Hearing Mem. at 32 (citing United States v. Dale, 991 F.2d 819, 844 (D.C. Cir. 1993))). Although I have no quarrel with the proposition of law, here there was more than a mere failure to investigate or an innocent or negligent mistake.

Accordingly, I hold that the agents acted with reckless disregard for the truth when they erroneously represented, in paragraphs 8(c)-(d) of the affidavit, that all Candyman members automatically received every e-mail transmitted to the Candyman Egroup and that every Candyman member automatically received images of child pornography transmitted to the group. I further hold that they recklessly omitted the fact that Candyman members had e-mail delivery options, including the option not to receive any e-mails. The false representations are stricken and the omitted information is

deemed included, and I turn to the issue of whether the "corrected" affidavit would support a finding of probable cause.

2. Probable Cause

First, I determine what the affidavit contains after the inaccurate statements are stricken and the omitted information is included. Second, I consider whether the "corrected" affidavit provides "a residue of independent and lawful information" sufficient to permit a magistrate judge to reasonably conclude that there was a fair probability that contraband or evidence of a crime would be found in Perez's home.

a) What Remains?

After eliminating the false information and supplying the omitted information, the "residue" consists of the following: general information about child pornography and the use of the internet and computers to distribute it; information regarding the Candyman Egroup generally, including that the undercover agent was able to download images of child pornography from the Candyman site; information that the undercover agent received numerous e-mails, including many with images of child pornography attached; information that Candyman members had e-mail delivery options, including the option not to receive any e-mails at all; and representations that a user joined the Candyman Egroup using an e-mail address that was registered to Perez.

The "corrected" affidavit contains no representation that the user -- Perez -- received any e-mails or that he received or downloaded or viewed any images or files or that he sent or uploaded any images or files. In fact, the "corrected" affidavit reports that Candyman members could choose not to receive any e-mails, but it provides no information as to which option Perez had selected. The "corrected" affidavit contains no representation as to how long Perez was a member, whether he unsubscribed, or whether he did anything beyond subscribing. The "corrected" affidavit contains no information about what it meant to be a "member" or "subscriber."

As to the Candyman Egroup itself, the "corrected" affidavit provides scant detail about the group and its activities. It reports that images of child pornography were available for downloading and were transmitted by e-mail. It also discloses that the site offered protected activities: polls and surveys; links to other sites; and a "chat" section for real time "conversations." The "corrected" affidavit does not allege that the Candyman enterprise was wholly or even largely illegitimate.

b) Is the "Corrected" Affidavit Sufficient?

In the end, all that is left is the fact that Perez subscribed to a website where unlawful images of child pornography could be downloaded. I conclude this was not a sufficient "residue" to permit a magistrate judge to determine that a fair probability

existed that contraband or evidence of child pornography would be found in Perez's home.

With the critical allegation that all members automatically received all e-mails stricken, the only arguably incriminating fact remaining is Perez's membership in the group. Cases have held, however, that "proof of mere membership in [an organization], without a link to actual criminal activity, [is] insufficient to support a finding of probable cause." United States v. Brown, 951 F.2d 999, 1003 (9th Cir. 1992) (finding membership in corrupt police unit did not establish probable cause); see Mendocino Envtl. Ctr. v. Mendocino County, 192 F.3d 1283, 1294-95 (9th Cir. 1999) (finding assertion that environmental group "had a reputation for violence, property destruction and sabotage" did not establish probable cause). Mere membership in an organization, without any other link to actual criminal activity, will support a finding of probable cause only where the organization is engaged in criminal activity to such an extent that it must be considered "wholly illegitimate." United States v. Rubio, 727 F.2d 786, 793 (9th Cir. 1984) ("where there is no allegation that the enterprise is wholly illegitimate, . . . evidence of mere association would not necessarily aid in obtaining a conviction . . . ; otherwise, the Fourth Amendment would offer little protection for those who are innocently associated with a legitimate enterprise"); United States

v. Acosta, 110 F. Supp. 2d 918, 933 (E.D. Wis. 2000) (denying motion to suppress on grounds that mere association with Latin Kings organization was sufficient to establish probable cause because search warrant affidavit "provided probable cause to believe that such a large portion of the Latin Kings' activities were illegitimate that the enterprise could be considered in effect wholly illegitimate").[10]

Here, a magistrate judge could not reasonably conclude, from the four corners of the "corrected" affidavit, that the Candyman organization was engaged in criminal activity to such an extent that it could be considered "wholly illegitimate" in the criminal sense.[11] Although the affidavit reported that the website displayed the

---

[10] At oral argument, the Government conceded that mere membership, for example, in the Ku Klux Klan would not constitute probable cause to search an individual's home for evidence of civil rights violations. (2/19/03 Tr. at 38). See also Ybarra v. Illinois, 444 U.S. 85, 91 (1979) ("[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.").

[11] This Court reviews the corrected affidavit de novo. Of course, the reviewing court cannot consider material outside of the affidavit. See Aguilar v. Texas, 378 U.S. 108, 109 n.1 (1964) ("It is elementary that in passing on the validity of a warrant, the reviewing court may consider only information brought to the magistrate's attention.") (citation omitted); see U.S. Const. amend. IV ("no Warrants shall issue, but upon probable cause, supported by Oath or affirmation"). Thus, evidence that emerged after the warrant issued -- evidence highly relevant to the agents' state of mind -- will not be considered in the probable cause inquiry in the first instance. I do consider extrinsic evidence in the discussion of the reasonableness of the Government's position.

message "[t]his group is for People who love kids," no images appeared on the first page, the words "child pornography" did not appear, and visitors were told they could post messages or "pics and vids." (Armenta Aff. Ex. E ¶ 8(b)). The affidavit did not even reveal that the words "Adult," "Image Galleries," and "Transgender" appeared on the website. (Id. ¶ 8). The affidavit did not represent that the Candyman Egroup engaged only or even primarily in illegal activity; to the contrary, the affidavit noted that the website offered protected and legal activities: text-based messaging, answering survey questions, posting links to other sites, and "chatting" -- engaging in real time "conversations." Hence, a magistrate judge could not reasonably conclude, based on the contents of the "corrected" affidavit, that the sole or even primary purpose for joining the group was to download images of child pornography.

Binney testified at the hearing that "in my affidavit I state that the primary purpose of the website was the file section where the people can go and download. My experience as an investigator of child pornography types of violations and the training that I received and the behavioral science aspect of it, I felt very strongly that if somebody was a member for any period of time they would have downloaded images." (1/15/03 Tr. at 63). The "corrected" affidavit, however, does not identify the "primary purpose" of the website, nor does the "corrected" affidavit assert

that "if somebody was a member for any period of time they would have downloaded images." (See Armenta Aff. Ex. E ¶¶ 8(d), (e)).

Hence, a magistrate judge could not conclude, on the face of the "corrected" affidavit, that a fair probability existed that all subscribers to the site illegally downloaded or uploaded images of child pornography. The extrinsic facts confirm that was the case. As the Yahoo logs show, the vast majority of subscribers, including Perez, elected to receive no e-mails. The vast majority of the e-mails that Binney received did not have images of child pornography attached. Subscribers were not required to post or upload images, and the Yahoo logs show that Perez did not. Subscribers could have engaged in protected, non-criminal activities, such as answering survey questions or chatting. An individual could have joined simply by entering an e-mail address without paying a fee, explored the site without knowingly downloading any images, and left, without ever returning. This would not have been illegal conduct.

Three Ninth Circuit cases involving the sufficiency of search warrant affidavits in computer child pornography cases are instructive. Probable cause was found in two of the cases. In United States v. Lacy, 119 F.3d 742 (9th Cir. 1997), the affidavit reported that an individual had telephoned a Danish computer bulletin board system and downloaded at least two files containing child pornography. The telephone calls were traced, by telephone records,

to the defendant's home. Hence, there was specific information that the defendant's home telephone was used to download at least two images of child pornography. In United States v. Hay, 231 F.3d 630 (9th Cir. 2000), a known trafficker in child pornography was arrested in Canada; information found on his computer revealed that files containing images of child pornography were transmitted to a computer with a unique internet address affiliated with the University of Washington. The computer was eventually traced to the defendant, a student at the university. In both cases, the court held there was a sufficient basis for a finding of probable cause.

In contrast, in United States v. Weber, 923 F.2d 1338 (9th Cir. 1991), the court found no probable cause. The defendant placed an order for child pornography in response to a government-generated advertisement; two years earlier, the defendant had been sent apparent child pornography, but he never claimed the materials from customs. These facts were included in a search warrant affidavit, and a search warrant was issued and executed before the new materials were delivered. The court held that probable cause did not exist because these facts did not give rise to a "fair probability" that contraband would be found in the home.

The facts of this case are more similar to the facts of Weber than they are to the facts of Hay and Lacy. Perez's subscription to the Candyman website is roughly comparable to Weber's

placement of an order for materials that had not yet been delivered; in both cases at best there was a chance, but not a fair probability, that child pornography would be found. On the other hand, the search warrants were sustained in both Hay and Lacy precisely because there was concrete evidence, and not just speculation, that the defendant had downloaded images of child pornography. Here, with the false statements deleted, the affidavit contains nothing concrete to suggest that Perez had transmitted or received images of child pornography.

Again, "the Fourth Amendment's touchstone is reasonableness, and a search's reasonableness is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed to promote legitimate governmental interests." United States v. Knights, 534 U.S. 112, 118-19 (2001). The Court must evaluate the reasonableness of a search by engaging in a practical, common-sense analysis, taking into account the particular context in which probable cause is being assessed, and balancing the rights of citizens to be secure in their homes from unwarranted intrusion against the needs of law enforcement.

In the context of this case, a finding of probable cause would not be reasonable. If the Government is correct in its position that membership in the Candyman group alone was sufficient

to support a finding of probable cause, then probable cause existed to intrude into the homes of some 3,400 (or even 6,000) individuals merely because their e-mail addresses were entered into the Candyman website. Without any indication that any of these individuals downloaded or uploaded or transmitted or received any images of child pornography, without any evidence that these individuals did anything more than simply subscribe, the Government argues that it had the right to enter their homes to conduct a search and seize their computers, computer files and equipment, scanners, and digital cameras. This cannot be what the Fourth Amendment contemplated.

The context here is the internet, specifically, the use of the internet to trade child pornography. Law enforcement needs a certain amount of latitude to address those who would violate the child pornography laws and sexually exploit and abuse children. Just as there is no higher standard of probable cause when First Amendment values are implicated, however, there is no lower standard when the crimes are repugnant and the suspects frustratingly difficult to detect.

Here, the intrusion is potentially enormous: thousands of individuals would be subject to search, their homes invaded and their property seized, in one fell swoop, even though their only activity consisted of entering an e-mail address into a website from a

computer located in the confines of their own homes.[12] In fact, here the FBI sent out 700 or more draft search warrants across the country. (1/15/03 Tr. at 146). And in this case the affidavit covered nine premises. In light of the potential impact, care must be taken.

---

[12] Whether the statute reaches mere internet "browsing" is something of an open question. Here, it is a central contention in the warrant affidavit that members of the group automatically received group e-mails with illegal files attached, activity that would most likely violate the statute. Without the receipt and possession of those e-mailed files, probable cause to believe evidence of criminal activity would be found on a suspect's computer is that much more uncertain. The statute does not criminalize "viewing" the images, and there remains the issue of whether images viewed on the internet and automatically stored in a browser's temporary file cache are knowingly "possessed" or "received." The question, as the court in United States v. Zimmerman, 277 F.3d 426, 435 (3d Cir. 2002), put it while examining probable cause, is that without evidence that pornography was specifically downloaded and saved to a defendant's computer, the offending images "may well have been located in cyberspace, not in [the defendant's] home." In United States v. Tucker, 305 F.3d 1193, 1205 (10th Cir. 2002), the court upheld a conviction for possession of files automatically stored in a browser cache because the defendant's "habit of manually deleting images from the cache files established that he exercised control over them." Id. at 1198. The court clarified, however, that it offered "no opinion on whether the mere viewing of child pornography on the Internet, absent caching or otherwise saving the image, would meet the statutory definition of possession" nor whether "an individual could be found guilty of knowingly possessing child pornography if he viewed such images over the Internet but was ignorant of the fact that his Web browser cached such images." Id.; see United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002) (noting that the district court (Judge Perry) acquitted the defendant on one count and "explained that one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing the image to be automatically stored in the browser's cache, without having purposely saved or downloaded the image").

In addition, the competing interests can be accommodated. While the anonymity of the internet empowers those who would break the law, it provides law enforcement with crime-fighting tools, including the ability to go undercover with relative ease and to obtain significant information from third parties such as service providers. Here, for example, the agents either had or could have had, before they requested the warrant, all the Yahoo logs, which provided extensive information -- whether a subscriber was offered e-mail delivery options; whether he elected a delivery option; whether he uploaded or posted any images; when he subscribed; and whether he unsubscribed. In addition, although the investigating agents testified they did not understand the material they received, it is hard to believe that other FBI experts -- the Cyber Division, for example -- could not have provided assistance. The fact that the agents missed the information or did not understand it or that Yahoo was not as cooperative as it should have been is no basis for relaxing the requirements for a finding of probable cause.

In United States v. Strauser, another Candyman case on which the Government heavily relies, the district court (Perry, D.J.) observed that mere membership in the Candyman group did not give rise to probable cause:

> I do not believe . . . that subscription to such a service, without more, provides probable cause to believe that evidence of possession of child pornography will be found at the

> subscriber's home. One could subscribe, then, having seen the type of content of the site, simply never go back to the site, but also never go to the trouble of "unsubscribing." If such a member had the "no mail" option, there would not be any emails sent, and the child pornography would not be received. Without any evidence that child pornography had ever been received or that the web site had otherwise been accessed, I do not believe that probable cause would have existed.

United States v. Strauser, No. 02CR82 CDP, slip op. at 6 (E.D. Mo. Sept. 4, 2002) (annexed to Southwell 11/7/02 Aff. as Ex. B). I agree with Judge Perry's analysis in this respect.

3. Other Operation Candyman Cases

The Government relies on rulings in five other Candyman cases denying other defendants' motions to suppress based upon identical or similar search warrant affidavits. United States v. Pisarek, 02 Cr. 852 (CM), slip op. (S.D.N.Y. Dec. 10, 2002) (annexed to Southwell 2/13/03 Aff. as Ex. A); United States v. Coye, No. 02-CR-732 (FB), 2002 WL 31526542 (E.D.N.Y Nov. 14, 2002) (Block, J.); Strauser, No. 02CR82 CDP, slip op.; United States v. Froman, Criminal No. H-02-142-03, slip op. (S.D. Tex. Aug. 21, 2002) (annexed to Southwell 11/7/02 Aff. as Ex. D); United States v. Coplan, No. CR 02-319 (E.D.N.Y. Aug. 15, 2002) (Ross, J.) (bench ruling) (annexed to Southwell 11/7/02 Aff. as Ex. C). These cases are not binding on this Court, and are not persuasive for the following reasons.

First, and most significantly, these decisions were rendered without the benefit of the additional evidence presented in this case that clearly shows that Binney's explanation of how he made the error is wrong and that his actual experience was that he joined via the website and was presented with e-mail delivery options. These courts did not have the benefit of the recently obtained Yahoo logs showing that Binney subscribed not via e-mail but by the web, that he did so for six other Egroups as well, and that he was presented with e-mail delivery options each time, nor did they have the two FBI Cyber Division reports.

Second, in three of the cases, no Franks hearing was held. In Coye, the defendant did not "explicitly" raise the issue of the error in the affidavit and did not argue that the false statement was made intentionally or recklessly. Likewise, in Coplan, the defendant did not allege "recklessness or intentional lying," and the court thus held that no Franks hearing was warranted. In Pisarek, Judge McMahon of this district denied a defendant's suppression motion, as well as his request for a Franks hearing. She drew most of the factual information for her conclusions from the Strauser case -- apparently with the consent of the defendant, who did not contest any of the facts of Strauser.

Third, some of the courts relied in part on the Leon good faith exception or the fact that the affidavit was executed by an FBI

agent who relied in good faith on the information provided by Binney. See Coplan; Froman; Pisarek; Coye. The Government now concedes that this was error.

Fourth, the Court has been advised that the Strauser case has been reopened to consider additional evidence. (2/19/03 Tr. at 20). As noted, the Pisarek case relies heavily on Strauser.

Finally, Perez is not bound in any way by the findings of fact or conclusions of law in these other cases, for he was not a party and was not in privity with any party in these other cases. He is entitled to litigate these issues in his own right.

As for the issue of whether the "corrected" affidavit contains sufficient information to support a finding of probable cause, four of the courts reached the issue. The Strauser court held the affidavit was not sufficient, and the Pisarek, Froman, and Coplan courts held it was sufficient. The Coplan case is distinguishable, at least to an extent, because the search warrant affidavit there also noted that the defendant was a member of, in addition to the Candyman group, another Egroup apparently centered around distributing child pornography, entitled "girls12-16." Coplan, at 8. For the reasons set forth above, to the extent that Pisarek, Froman, and Coplan hold that mere membership in the Candyman group was a sufficient basis to find probable cause, I respectfully disagree.

CONCLUSION

For the reasons set forth above, defendant's motion is granted and the fruits of the search are suppressed. The parties shall appear for a status conference on Friday, March 14, 2003 at 2:00 p.m.

SO ORDERED.

Dated: New York, New York
March 5, 2003

DENNY CHIN
United States District Judge