United States v. Wilbert

United States District Court for the Western District of New York

March 28, 2017, Decided; March 28, 2017, Filed

16-CR-6084-DGL-JWF

Reporter
2017 U.S. Dist. LEXIS 77818 *

UNITED STATES OF AMERICA, v. ***SCOTT T. WILBERT***, Defendant.

Subsequent History: Adopted by, Motion denied by *United States v. Wilbert, 2017 U.S. Dist. LEXIS 77141 (W.D.N.Y., May 22, 2017)*

Magistrate's recommendation at *United States v. Wilbert, 2018 U.S. Dist. LEXIS 187515 (W.D.N.Y., Aug. 20, 2018)*

Core Terms

pornography, upload, upstairs, Recommendation, staleness

Counsel: For ***Scott T. Wilbert***, Defendant: Robert A. Napier, LEAD ATTORNEY, Napier & Napier, Rochester, NY; Jeffrey L. Ciccone **[*1]** , Federal Public Defender, Rochester, NY.

For USA, Plaintiff: Kyle P. Rossi, Melissa M. Marangola, LEAD ATTORNEYS, U.S. Attorney's Office, Rochester, NY.

Judges: JONATHAN W. FELDMAN, United States Magistrate Judge.

Opinion by: JONATHAN W. FELDMAN

Opinion

REPORT AND RECOMMENDATION

Preliminary Statement

STEVEN FELDMAN

On August 23, 2016, the Federal Grand Jury returned an Indictment, charging Defendant ***Scott T. Wilbert*** ("defendant" or "Wilbert") with receipt of child pornography. See Docket # 11. The defendant's court-appointed attorney filed omnibus motions on November 14, 2016 (Docket # 17). The government responded on November 23, 2016 (Docket # 18) . The Court held a motion hearing on December 8, 2016, and, with one exception, resolved the motions on the record. See Docket # 22.

The exception concerned the defendant's motions to suppress evidence and motion for a Franks hearing. The Court reserved decision and asked for supplemental briefing. The defendant filed his supplemental brief on January 12, 2017 (Docket # 27), and the government filed its supplemental brief on January 27, 2017 (Docket # 29). This Report and **[*2]** Recommendation[1] resolves the defendant's remaining suppression motion.

Relevant Facts

The remaining issue for this Court to decide concerns the defendant's motion to suppress physical evidence seized from the upstairs apartment at 634 Garson Avenue in the City of Rochester pursuant to a search warrant signed by Monroe County Court Judge Victoria M. Argento on February 17, 2016. See Docket # 18-1. The search Warrant was based on an affidavit signed by New York State Police Investigator David A. Cerretto. In his affidavit, Cerretto stated that on December 22, 2015, he received information from the National Center for Missing and Exploited Children that an image containing child pornography had been uploaded to a computer using a specific Internet Protocol (IP) address. The upload took place during the early morning hours of October 22, 2015. The IP address was controlled by Frontier Communications. Frontier told Inv. Cerretto that during the date and time of the upload, the IP address was assigned to ***Scott T. Wilbert***, 634 Garson Avenue, Rochester, New York 14609. According to Frontier, that IP address also had an email address in the name of ***Scott T. Wilbert*** and a local **[*3]** phone number assigned as well. Inv. Cerretto also averred in his supporting affidavit that a record check of ***Scott T. Wilbert*** revealed that Wilbert was a registered "level 2" sex offender and in 2004 was investigated for uploading child pornography files, although no charges were ever filed. Docket # 18-2, at 6.

Based on the information set forth in the Cerretto affidavit, Judge Argento found probable cause to search 634 Garson Avenue. The primary issue raised by the defendant concerns the description of the place to be searched. In his affidavit, Inv. Cerretto described the premises as

> being a green and white colored, multi-level residential building. The building is identified by the numbers "634" above a maroon colored entrance door. Mentioned entrance door is on the north side of Garson Avenue, which is located in the City of Rochester, County of Monroe, State of New York. Leading to mentioned entrance door are fixed metal hand rails on both sides of a concrete stairway. 634 Garson Avenue is attached to the left of 636 Garson Avenue, which is utilized commercially as a hair salon. This search is to include the upstairs apartment of 634 Garson Avenue, the subject of this investigation **[*4]** (***SCOTT T. WILBERT*** (08/21/1974)), and any out buildings, real property, vehicle(s), and curtilage utilized by the subject at the mentioned location. See attached photos of described building.

Id. at 1 (emphasis added).

The defendant argues that the affidavit in support of the search warrant failed to establish a nexus between the alleged crime and the premises sought to be searched. The affidavit describes 634 Garson Avenue as a "multi-level residential building." Id. In fact, the defendant argues, 634 Garson Avenue is a multiple unit residence, in which Wilbert - the target of the investigation - occupies only one unit, the upstairs apartment. In other words, although the affidavit linked the defendant to 634 Garson Avenue, it did not specify the specific portion of that building he occupied. The defendant claims that Cerretto's use of the word "multi-level" was intended to "obfuscate rather than illuminate its true occupancy." Aff. of Robert Napier, Docket # 17-1, at ¶ 11. According to defense counsel, this

---

[1] By Order of Hon. David G. Larimer, United States District Judge, dated August 24, 2016, all pretrial matters in the above-captioned case have been referred to this Court pursuant to *28 U.S.C. §§ 636(b)(1)(A)-(B)*. See Docket # 12.

"obfuscation" rendered the search warrant overbroad and lacking probable cause to believe "that contraband or evidence of crime would be found in the place searched." Id. at ¶ 8.

The defendant **[*5]** also seeks a so-Called Franks hearing, arguing that Inv. Cerretto's description of the place to be searched was so imprecise and misleading that it amounted to a deliberate and "reckless disregard of the truth." *Franks v. Delaware, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978)*. Finally, the defendant contends that the evidence Inv. Cerretto relied on in his warrant was too "stale" to establish probable cause to search the upstairs apartment where he resided.

Law enforcement officers executed the search warrant on February 24, 2016. There is no dispute that the only apartment in 634 Garson Avenue that was searched was the upstairs apartment.

Discussion

Particularity of the Place to Be Searched: The *Fourth Amendment* requires a search warrant to describe with particularity both the place to be searched and the items to be seized. This particularity requirement is not a mere formality. *United States v. Voustianiouk, 685 F.3d 206, 210 (2d Cir. 2012)*. To meet the particularity requirement, "[i]t is enough if the description is such that the officer with a search warrant can, with reasonable effort ascertain and identify the place intended." *Steele v. United States, 267 U.S. 498, 503, 45 S. Ct. 414, 69 L. Ed. 757 (1925)*.

In the usual course of business, law enforcement drafts and submits both the warrant application and a proposed search warrant to the issuing judge. Although both documents may have been drafted by **[*6]** the government, it is only the application for a search warrant that "belongs" to the government. The search warrant itself is a document belonging to the judge, regardless of who may have drafted it. While a judge can reject a warrant, it is also not uncommon for a judge to change, modify or delete portions a search warrant proposed and drafted by law enforcement. "The mere fact that the Magistrate issued a warrant does not necessarily establish that he agreed that the scope of the search should be as broad as the affiant's request." *Groh v. Ramirez, 540 U.S. 551, 561, 124 S. Ct. 1284, 157 L. Ed. 2d 1068 (2004)*. Thus, "[i]n determining the permissible scope of a search that has been authorized by a search warrant . . . we must look to the place that the magistrate judge who issued the warrant intended to be searched, not to the place that the police intended to search when they applied for the warrant." *Voustianiouk, 685 F.3d at 211*.

The foregoing is important because, contrary to the defendant's argument, the *Fourth Amendment's* particularity requirement is measured by the terms of the warrant and not the warrant application. And here, there is an important difference between the two. Inv. Cerretto's application describes the dwelling sought to be searched as "634 Garson Avenue, Rochester, New York 14609." Docket **[*7]** # 18-2, at 1. The warrant issued by Judge Argento, on the other hand, describes the dwelling to be searched as "634 Garson Avenue, Apartment Up, Rochester, New York 14609." Docket # 18-1, at 1 (emphasis added). The probable cause set forth in the application is limited to the apartment occupied by the defendant and not any other apartments in 634 Garson Avenue. By adding the words "Apartment Up" to the warrant, Judge Argento explicitly limited the scope of the place to be searched to the dwelling where probable cause had been established and prevented the police from using the warrant to justify searching any other apartment in 634 Garson Avenue. Since there is no dispute that the only apartment searched pursuant to the warrant was the upstairs apartment and the contraband found during the search came from the upstairs apartment, there is no *Fourth Amendment* violation. Any imprecision in the warrant application was cured by the precise language included in the search warrant itself.[2]

---

[2] It would be a closer question had the search warrant not included the limiting description of "Apartment Up." It is true that paragraph A(1) of the warrant stated that "[t]his search is to include the upstairs apartment of 634 Garson Avenue," but that language is imprecise. Does a warrant that "includes" one apartment in a building described by the warrant necessarily "exclude" the other apartments in the described building? I need not resolve that issue since the "Apartment Up" language was clearly set forth in the warrant itself.

Stale Evidence: The defendant next argues that the single upload of child pornography to Wilbert's IP address on October 25, 2015, was too stale to font the basis of probable cause for the warrant issued four months later **[*8]** on February 17, 2016. See Docket # 17-1, at 12. I do not find this argument persuasive.

The Second Circuit has recognized that staleness determinations in child pornography investigations are "unique" because "it is well known that 'images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes.'" *United States v. Irving, 452 F.3d 110, 125 (2d Cir. 2006)* (quoting another source). Therefore, "evidence that such persons possessed child pornography in the past supports a reasonable inference that they retain those images — or have obtained new ones — in the present." *United States v. Raymonda, 780 F.3d 105, 114 (2d Cir. 2015)*, cert. denied, *136 S. Ct. 433, 193 L. Ed. 2d 337 (2015)*. Defendant correctly cites to Raymonda for the proposition that this inference requires more than one single upload of child pornography. See *Raymonda, 780 F.3d at 117* ("[A]bsent any indicia that the suspect was a collector of child pornography likely to hoard pornographic files, we hold that a single incident of access does not create a fair probability that child pornography will still be found on a suspect's computer months after all temporary traces of that incident have likely cleared.").

But the defendant is mistaken that the probable cause finding here was based exclusively on one upload of child pornography. The Second Circuit **[*9]** has recognized that "suspect's admission or other evidence identifying him as a 'pedophile'" together with the upload of child pornography will supply probable cause. *Raymonda, 780 F.3d at 114*; see *Irving, 452 F.3d at 115, 125* (finding no staleness where suspect "admitted he was a convicted pedophile"); *United States v. Harvey, 2 F.3d 1318, 1323 (3d Cir. 1993)* (finding no staleness where affidavit "provided ample information that [suspect] was a pedophile"). Unlike *Raymonda*, the defendant here was previously convicted for felony criminal sexual acts, was a registered sex offender and had been suspected of uploading child pornography in the past. These facts, alleged in the affidavit and coupled with the new upload of child pornography, were sufficient to form the basis for probable cause to search the upstairs apartment for evidence of child pornography.

"Franks Hearing": Having determined that the search warrant satisfies the particularity requirement of the *Fourth Amendment*, and because the search was only conducted on the upstairs apartment, there is no basis for the Court to hold a hearing pursuant to *Franks v. Delaware, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978)*. Any "erroneous information" in the warrant affidavit was not material to the issuing judge because the search warrant itself limited the search to the apartment where probable cause had Clearly been established. **[*10]**

Conclusion

For the foregoing reasons, it is my Report and Recommendation that defendant's motion to suppress evidence and for a Franks hearing (Docket # 17) be **denied**.

SO ORDERED.

/s/ [Signature]

JONATHAN W. FELDMAN

United States Magistrate Judge

Dated: March 28, 2016

Rochester, New York

Pursuant to *28 U.S.C. § 636(b)(1)*, it is hereby

ORDERED, that this Report and Recommendation be filed with the Clerk of the Court.

ANY OBJECTIONS to this Report and Recommendation must be filed with the Clerk of this Court within fourteen (14) days after receipt of a copy of this Report and Recommendation in accordance with the above statute and Rule 59(b)(2) of the Local Rules of Criminal Procedure for the Western District of New York.[1]

The district court will ordinarily refuse to consider on *de novo* review arguments, case law and/or evidentiary material which could have been, but was not, presented to the magistrate judge in the first instance. See, e.g., *Paterson-Leitch Co., Inc. v. Mass. Mun. Wholesale Elec. Co., 840 F.2d 985 (1st Cir. 1988)*.

Failure to file objections within the specified time or to request an extension of such time waives the right to appeal the *District Court's Order*. *Thomas v. Arn, 474 U.S. 140, 106 S. Ct. 466, 88 L. Ed. 2d 435 (1985)*; *Wesolek v. Canadair Ltd., 838 F.2d 55 (2d Cir. 1988)*.

The parties are reminded that, pursuant to Rule 59(b)(2) of the Local Rules of Criminal Procedure for the Western District of New York, "[w]ritten objections . . . shall specifically identify the portions of the **[*11]** proposed findings and recommendations to which objection is Made and the basis for each objection, and shall be supported by legal authority." **Failure to comply with the provisions of Rule 59(b)(2) may result in the District Court's refusal to consider the objection**.

Let the Clerk send a copy of this Order and a copy of the Report and Recommendation to the attorneys for the Plaintiff and the Defendant.

SO ORDERED.

/s/ [Signature]

JONATHAN W. FELDMAN

United States Magistrate Judge

Dated: March 28, 2017

Rochester, New York

End of Document

---

[1] Counsel is advised that a new period of excludable time pursuant to *18 U.S.C. § 3161(h)(1)(D)* commences with the filing of this Report and Recommendation. Such period of excludable delay lasts only until objections to this Report and Recommendation are filed or until the fourteen days allowed for filing objections has elapsed. *United States v. Andress, 943 F.2d 622 (6th Cir. 1991)*, cert. denied, ***502 U.S. 1103, 112 S. Ct. 1192, 117 L. Ed. 2d 433 (1992)***; *United States v. Long, 900 F.2d 1270 (8th Cir. 1990)*.

United States v. Wilbert

United States District Court for the Western District of New York

August 20, 2018, Decided; August 20, 2018, Filed

16-CR-6084-DGL-JWF

Reporter
2018 U.S. Dist. LEXIS 187515 *

UNITED STATES OF AMERICA, v. ***SCOTT T. WILBERT***, Defendant.

Subsequent History: Adopted by, Motion denied by *United States v. Wilbert, 343 F. Supp. 3d 117, 2018 U.S. Dist. LEXIS 187024 (W.D.N.Y., Nov. 1, 2018)*

Prior History: *United States v. Wilbert, 2017 U.S. Dist. LEXIS 77818 (W.D.N.Y., Mar. 28, 2017)*

Core Terms

chat, privacy, users, video, suppression, moderator, uploaded, pornography, monitoring, Recommendation, flagged, website, software, site, staff, electronic, snapshots, entity, Indictment, sex, omissions, captures, depicted, unwanted, screen

Counsel: **[*1]** For ***Scott T. Wilbert***, Defendant: Robert A. Napier, LEAD ATTORNEY, Napier & Napier, Rochester, NY.

For USA, Plaintiff: Kyle P. Rossi, Melissa M. Marangola, LEAD ATTORNEYS, U.S. Attorney's Office, Rochester, NY.

Judges: Jonathan W. Feldman, United States Magistrate Judge.

Opinion by: Jonathan W. Feldman

Opinion

STEVEN FELDMAN

REPORT AND RECOMMENDATION

Procedural Background

In August 2016, the Federal Grand Jury returned ah Indictment, charging ***Scott T. Wilbert*** ("Wilbert" or "the defendant") with receipt of child pornography. See Docket # 11. The defendant filed omnibus motions in November 2016 (Docket # 17), which included a challenge to the search of his residence. The Court resolved Most of the defendant's motions on the record (Docket # 22), but reserved decision on the defendant's motion to suppress the search of his home. On May 22, 2017, the Court recommended that the defendant's motions to suppress and for a Franks hearing be denied. Docket # 32. The defendant filed objections to the Court's Report and Recommendation (Docket # 36) and on May 22, 2017, Judge Larimer denied the objections and denied the motion to suppress. Docket # 37.

On August 16, 2017, after the government had made a motion to set a trial date, the defendant **[*2]** filed the instant motion to suppress and motion to dismiss on grounds not previously raised in his omnibus motions. Docket # 42. The government responded on September 5, 2017 (Docket 4 44) and the defendant replied on September 19, 2017 (Docket # 48), prompting another response from the government (Docket # 49). The Court scheduled an evidentiary hearing, which the government moved to cancel, arguing that there was no factual basis for such a hearing. Docket # 52. The Court denied the government's request (Docket # 57) and proceeded with the evidentiary hearing on January 17, 2018, at which three witnesses testified. Docket # 58. The Court ordered post-hearing briefing, which the defendant filed on March 26, 2018 (Docket # 65) and the government filed on April 23, 2018 (Docket # 69). Wilbert replied on April 30, 2018 (Docket 4 69). The Court requested additional briefing on several issues. Docket # 70. After an extension, the parties filed their Supplemental briefs on June 1, 2018. Docket ## 72, 73.

Relevant Facts

In this motion, the defendant argues that two screenshots of a video chat uploaded from his IP address[1] to a chat site and forwarded to the National Center for Missing and Exploited **[*3]** Children ("NCMEC") and then to law enforcement must be suppressed as the result of an illegal warrantless search of his computer. He also argues that other evidence subsequently obtained as a result of that illegal search Should be suppressed as fruit of the poisonous tree. Finally, the defendant asserts that the indictment itself must be dismissed for failure to preserve evidence. Three witnesses testified at the evidentiary hearing: (1) Leif K-Brooks ("K-Brooks"), owner and founder of Omegle; (2) John Shehan ("Shehan"), Vice President of the Exploited Child Division at NCMEC; and (3) Investigator Cerretto ("Cerretto") of the New York State Police ("NYSP").

Leif K-Brooks: K-Brooks testified that he is the owner and founder of Omegle, a chat website that connects users randomly and anonymously to other users. Jan. 17, 2018 Hr'g Tr., Docket # 61, ("Tr.") at 21. K-Brooks founded the Omegle site in 2009 and described his invention as follows:

> So most instant messaging or chat sites are for talking to people you already know. So you would say I want to talk to Bob and you would enter Bob's user name and you'd have a conversation with Bob. Omegle is for meeting new people so the site connects **[*4]** you to someone random, someone you don't select and it's anonymous, meaning there are no names associated with it. You don't know the other person's name and they don't know your name.

---

[1] The defendant maintains that he did not use the Omegle website to upload any images and that the offending conduct must have been committed by a roommate who used the defendant's computer. Docket # 60. The government, obviously, disagrees and intends to prove it was the defendant who was participating in the video chat en the Omegle website. Regardless, there is no dispute that it was an IP address subscribed to and paid for by Wilbert that was utilized in the relevant video chat.

Tr. at 21. If the user does not want to chat to the person they are randomly connected with, they simply press a "button" to disconnect and connect to a different random user. Omegle supports both video chats and text chats. Tr. at 27. Unlike text chats, video chats do not pass over Omegle's servers. Tr. at 27-28. Rather, video chats are conducted peer-to-peer or computer-to-computer, i.e. directly between the two users. Tr. at 27-28. Although Omegle does not possess or retain any of the chat itself, it does log "chat history metadata," including the time when the chat began and the IP addresses associated with the chat. Tr. at 29. Today, the Omegle cite averages one million distinct users per day. Tr. at 47.

Omegle is free and users need not register before using the site. Omegle does not collect or share users' identifying information. Tr. at 21-22. Upon entering the site, but before engaging in a chat, the platform displays a link to Omegle's privacy policy. Tr. at 22-23. There is "also a warning in **[*5]** large text about the video chat moderation" policy utilized by Omegle. Tr. at 22-23, 60. At the bottom of the initial Omegle screen, users are notified that they agree to Omegle's terms of service ("TOS") by casing the site. Tr. at 87. However, users are not required to read the TOS or affirmatively agree to them before engaging in a video or text chat and Omegle does not track whether users actually accessed the privacy policy. Tr. at 33.

K-Brooks explained the moderation system Omegle uses to monitor video chats. In order to discourage nudity, sexual behavior and otherwise illegal conduct during video chats, Omegle uses proprietary software that automatically captures snapshot images from the user's computer and instantly uploads those images to Omegle's servers "for moderation purposes." Tr. at 39. The software randomly captures four frames of the video chat during the first few seconds of the chat. No other images are monitored except for these initial still frame captures. Tr. at 62. After the images are uploaded to Omegle's servers they are immediately "screened" with an automated software program called "Computer Vision." Tr. at 36-37. According to K-Brooks, the program uses **[*6]** an algorithm that looks "at an image in sort of the same way a human would" by trying to recognize "shapes, colors and trying to detect features in images that 'S never seen before." Tr. at 35. If the software detects that the snapshots contain "good things," like a face or a person's Upper body, then the image will not be screened further by the software. Tr. at 36. However, if the program detects "bad things" — "things that are more likely to be something other than just a person sitting in front of a webcam talking to someone else while fully clothed," then the software will flag the images for "review by human moderators." Tr. at 36-37.

Images that the program determines may contain nudity, sexual conduct or other unknown or unwanted content are flagged to be inspected by a human moderator contracted by Omegle through Gracall, a third party company that staffs a moderator review force 24 hours a day, seven days a week. Tr. at 36-37, 40-41. Gracall staffs monitoring centers in various countries around the world and K-Brooks estimated that three to four moderators are actively viewing Omegle's screenshots at any time. Tr. at 75. K-Brooks designed a system where the snapshots are displayed **[*7]** in a "big grid" and the human moderators constantly scan the grid for offensive images. Tr. at 75. If a snapshot appears to be illegal or require further review, the human moderator "can just press buttons to flag them." Tr. at. 75. K-Brooks testified that hundreds of thousands - if not millions - of screenshots are flagged for review every day. Tr. at 46-47. Omegle bans IP addresses in the "tens of thousands" daily due to unwanted conduct. Tr. at 47.

If a moderator determines that the image contains suspected child pornography, a program developed by K-Brooks automatically compiles information in Omegle's system into a report and electronically submits it to NCMEC. Tr. at 47. The NCMEC report, known as a "cyber-tip," is generated and transmitted "[w]ithin a few minutes" after human review. Tr. at 55. The snapshots themselves typically only remain on Omegle's system for a few hours. Tr. at 64. However, if the image requires generation of a cyber tip report, Omegle preserves the images for 90 days. Tr. at 71.

K-Brooks testified that on October 25, 2015, Omegle's automated software flagged as suspicious two images from IP address 50.49.31.78. Tr. at 38. For purposes of this hearing, the **[*8]** defendant has admitted that IP address 50.49.31.78 was assigned to his computer. Docket # 60, at ¶ 6. The first image was uploaded at 2:30:21 UTC[2] and is a jpeg file whose name ended in "a9e7" ("image a9e7"). Hr'g Ex. 6. The second image was uploaded at 2:26:12

---

[2] Also known as Uniform Coordinated Time, Coordinated Universal Time, or Greenwich Mean Time. Tr. at 78.

UTC and is a jpeg file whose name ended in "c6d0" ("image c6d0"). Hr'g Ex. 6. K-Brooks testified that he is certain a third party moderator viewed image c6d0 because it was flagged as unwanted content, but he is not certain whether the Moderator viewed image a9e7.[3] Tr. at 48-49. This is so because, by looking at the records, K-Brooks could tell that the moderator had flagged image c6d0 as containing unwanted material, but did not flag image a9e7. That could mean that image a9e7 was viewed but did not contain unwanted material or that it was not reviewed at all. Tr, at 48-49, 53. However, because the two images came from the same chat session at around the same time, both were grouped together and sent on to NCMEC even though K-Brooks can only confirm that one was reviewed by a moderator and flagged as containing apparent child pornography. Tr. at 53-54.

Consistent with K-Brooks's testimony, a report[4] was automatically generated **[*9]** by Omegle's software and sent to NCMEC's "CyberTipline" at 2:38:58 UTC, indicating that two files were uploaded from IP address 50.49.31.78 and confirming that image c6d0 was reviewed by Omegle. Hr'g Ex 7, at 2-3; Tr. at 57-58. As part of that report, Omegle attached both images, even though the report is silent with respect to whether Omegle reviewed image a9e7. Tr. at 59. In accordance with Offiegle's image preservation policy, because law enforcement did not request the Snapshots within 90 days, Omegle deleted them. Tr. at 71. K-Brooks did not interview the Gracall employee who performed the review at issue here. Tr. at 73.

John Shehan: Shehan testified that he is the Vice President of the Exploited Child Division at NCMEC. Tr. at 97-98. According to Shehan, NCMEC's "mission is to help reunite families with missing children, reduce child sexual exploitation and prevent child victimization." Tr. at 99. NCMEC is a private not,-for-profit organization that receives significant funding from the federal government, as well as from various other sources. Tr, at 101. As part of his duties as Vice President, Shehan is responsible for NCMEC's CyberTipline, to which members of the public or **[*10]** internet service providers ("ISPs") can submit tips on suspected child pornography activity. Tr. at 98-103. Shehan testified that he understands *18 U.S.C. § 2258A* to require ISPs to report apparent child pornography on their systems to the CyberTipline. Tr. at 104. In doing so, ISPs must indicate - either manually or through automated software, like Omegle's - what conduct they are reporting and select the date and time of the incident; all other information they provide is voluntary. Tr. at 106. In turn, the law requires NCMEC to provide the collected information to law enforcement. Tr. at 106. NCMEC makes available CyberTipline reports to law enforcement from relevant jurisdictions via a virtual private network ("VPN"). Tr. at 109. In other words, NCMEC does not transmit the CyberTipline reports; rather, the appropriate law enforcement Members may access the database of tips through the VPN. Tr. at 109. In 2017, NCMEC received 10 million reports into the CyberTipline. Tr. at 105.

Shehan testified that NCMEC received the tip report at issue here on October 25, 2015 at approximately 2:38:58 UTC. Tr. at 111. The information reported by Omegle appears as Section A in NCMEC's CyberTipline Report 6928493 **[*11]** ("the Report"), which was ultimately provided to law enforcement. Tr. at 111-112; Hr'g Ex. 7. That section indicates that two images were uploaded from IP address 50.49.31.78 on October 25, and that image c6d0 was viewed by a moderator; the Report is silent with respect to whether image a9e7 was viewed by a moderator. Tr. at 114. However, based on the omission of any notation regarding Omegle's viewing of image a9e7, Shehan "would assume it was not" viewed. Tr. at 114. NCMEC's software blocks its staff from viewing any image that the ISP does not expressly state it viewed, but images viewed by the ISP are available to NCMEC staff to inspect. Tr. at 120. In other words, because Omegle did not specify that it viewed image a9e7, that image was not available for NCMEC staff to view.[5] Shehan testified that NCMEC engages in this practice so that it cannot be said to expand the scope of a previous search conducted by a private entity. Tr. at 122-23. Rather, the image resided on Omegle's servers in a locked file so that it could be passed on to law enforcement. Tr. at 122-23; see Hr'g Ex. 9. A NCMEC

---

[3] On cross examination, K-Brooks clarified that first in time images are not always reviewed before other images captured later, or at all. He explained, "[t]here's a lot of complexity to the logic of how queues work, so things can drain from the end of the queue if it gets too big, and so on and so on." Tr. at 77-78. He admitted that "not all images end up getting viewed. We try to review most of them, but sometimes they don't." Tr. at 78.

[4] What Omegle sent to NCMEC appears as Section A in Hearing Exhibit 7.

[5] A staff member could obtain supervisor override authorization to view the image but that did not happen here. Shehan testified that image a9e7 was not viewed by NCMEC staff. Tr. at 122.

staff member, however, was also able to view image c6d0, which Shehan testified appeared to **[*12]** be a series of four screenshots of an animal performing oral sex on a young girl. Tr. at 130-31. NCMEC classified this image as "child pornography unconfirmed" because the NCMEC employee was not able to determine the age of the child depicted in image c6d0. Tr. at 133, 156.

Shehan testified that sections B and C of the Report include information added by NCMEC. Once NCMEC received the Report, a NCMEC staff member used a publicly available search tool called MaxMind to pinpoint the geographical location of the IP address so that it could send the Report to the appropriate law enforcement agencies. Tr. at 116. Using that tool, the NCMEC employee determined that the IP address came from Rochester, New York and that the ISP was Frontier Communications. Tr. at 116.

Section D of the Report is a list of law enforcement to whom the Report was made available. All of the images — even those not viewable by NCMEC — were made available to law enforcement. Tr. at 152. The Report also documents which images, if any, were viewed by the original reporting ISP. Tr. at 148-49. Based on the geographic location of the IP address from which the images were uploaded, NCMEC made the Report available to the **[*13]** New York State Police Internet Crimes Against Children ("ICAC") task force. Tr. at 133. NCMEC's involvement ends once the report is made available to law enforcement; each agency decides whether to the review the report and what to do with the information contained in it. Tr. at 136.

Investigator David Cerretto: Cerretto, an investigator with the NYSP, testified that once NCMEC makes a report available to ICAC, members of the NYSP are able to retrieve it and review its contents. Tr. at 164. After being reviewed by ICAC, the Report here was forwarded to Keith Becker at the Computer Crimes Unit and then eventually[6] to Cerretto on December 22, 2015. Tr. at 165-66.

Cerretto testified that he accessed and viewed the Report and both images associated with the Report, even though he was aware that only image c6d0 had been viewed by Omegle and NCMEC.[7] Tr. at 168-69, 18 0. According to Cerretto, it is the NYSP's practice to open every image they obtain regardless of whether the image had been previously opened by a private entity. Tr. at 190. Cerretto determined that image c6d0 (Hr'g Ex. 1) was of an unclothed female child and a dog who was performing oral sex on the child. Tr. at 170. He was unable **[*14]** to tell whether image a9e7 (Hr'g Ex. 11) — which had not previously been viewed by Omegle or NCMEC — contained child pornography. Tr. at 170. Based on these two images and further investigation, Cerretto sought and obtained a search warrant for 634 Garson Avenue, the physical location where his investigation indicated was associated with the IP address included in the Report. Tr. at 171.

Cerretto testified that because he could not tell what was happening in image a9e7, the search warrant application was based on the image of the girl and the canine, i.e. image c6d0. Tr. at 170. In a section of the warrant application entitled "Facts Providing Reasonable Cause," Cerretto indicated that "at approximately 02:30:21, username 'WCP5MVIA3' uploaded an image of a prepubescent female (between four (4) years of age and seven (7) years of age) , who was engaged in oral sex with a K9, to the Internet through the website identified as Omegle.com." Docket # 17-2, at 5. Cerretto testified that in the search warrant application he indicated incorrectly that the image with the girl and the canine was uploaded at 2:30:21 UTC - instead of at 2:36 UTC - because he believed both images derived from one **[*15]** continuous incident that began at 2:30:21 UTC. Tr. at 173, 192-93.

Discussion

Motion to Suppress: The defendant argues that all evidence seized from the search of 634 Garson Avenue must be suppressed because the warrant for that residence was based on law enforcement viewing image a9e7, which

---

[6] Investigator T. Northrup — who did not testify — viewed both images before Cerretto viewed the images. Cerretto was aware that Northrup had viewed both images before viewing them himself. Tr. at 175-83.

[7] Cerretto stated that he makes his own assessment of whether an image contains child pornography rather than relying on any assessment made by a non-law enforcement officer. Tr. at 166-67.

Omegle had not previously reviewed. Wilbert insists that law enforcement significantly and illegally expanded Omegle's private search by conducting a warrantless search of image a9e7, for which the remedy is suppression of the fruits of the resulting search warrant.

Standing in the way of the relief Wilbert seeks is the difficulty the Court and the parties face in applying well established *Fourth Amendment* principles to processes and forms of evidence that did not even exist until fairly recently. This Court is not alone in struggling with how to apply *Fourth Amendment* formulas developed and grounded in physical places and objects to a virtual world in which evidence, objects and locations exist only as electronic impulses momentarily displayed on a computer screen. The *Fourth Amendment* issues implicated in Wilbert's suppression motion are hot new in the sense that they raise novel constitutional concepts, but rather pay tribute to the difficulty **[*16]** in fitting the square peg of the *Fourth Amendment* into the rounded hole of ESI - electronically stored information.

To prevail in this suppression motion, Wilbert has to overcome, inter alia, issues of standing and reasonable expectations of privacy, as well as navigate application of the third party doctrine, the consent to search doctrine and the private search doctrine. Complicating his challenge is the fact that all of these issues originate in the bewildering "new world" of ESI. After careful consideration of the arguments of counsel, I conclude that resolution of Wilbert's suppression motion does not require the Court to untangle most of these difficult *Fourth Amendment* issues. For, as discussed below, even if the defendant were able to "run the gauntlet" and have each issue decided in his favor, suppression of the evidence he seeks would not' result.

While it may not be necessary to resolve many of the *Fourth Amendment* issues Wilbert's motion raises, it is helpful for the Court's analysis to at least identify them. An initial issue is whether Wilbert had a reasonable expectation of privacy in the place searched sufficient to afford him standing to contest the search in the first place. "The party moving to suppress bears the **[*17]** burden of establishing that his own *Fourth Amendment* rights were violated by the challenged search or seizure." *United States v. Osorio, 949 F.2d 38, 40 (2d Cir. 1991)* (citing *Rakas v. Illinois, 439 U.S. 128, 131 n.1, 99 S. Ct. 421, 58 L. Ed. 2d 387 (1978)*). Here, the parties disagree as to exactly what the constitutionally protected space at issue is. The defendant asserts that he had a reasonable expectation of privacy in the contents of his personal computer. See *United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004)* ("Individuals generally possess a reasonable expectation of privacy in their home computers."). The government responds by arguing that Wilbert is not entitled to any expectation of privacy without first admitting that he had an expectation of privacy in the images in question. See Gov't Reply, Docket # 55, at 2 (to obtain standing, the defendant must assert that he had "a subjective expectation of privacy in transmitting child pornography through the video chat"). While the Court is skeptical of the government's position that Wilbert may not challenge the search of his computer without first admitting he was using Omegle at the time the offending images were found, it raises another expectation of privacy argument that might be more problematic for Wilbert. K-Brooks testified that Omegle's video chat component "is actually a peer-to-peer system" where the video stream **[*18]** goes directly from one user to the other. Tr. at 27-28. There is support in the case law for a diminished expectation of privacy for information an individual chooses to "share" on a peer-to-peer network, even if the sharing is not public, but limited to "friends". See, e.g., *United States v. Brooks, No. 12-cr-166, 2012 U.S. Dist. LEXIS 178453, 2012 WL 6562947, at *2 (B.D.N.Y. Dec. 17, 2012)* (discussing expectation of privacy in private peer-to-peer sharing networks)(citing cases).

The government also points out that Wilbert, like all users of the Omegle website, was advised that video chats are subject to monitoring for offensive content.[8] According to the government, such a warning (1) eliminates Wilbert's

---

[8] The relevant parts of Omegle's privacy policy provide:

> Chat messages are **[*19]** screened by an automated system for spam. In general, messages are not stored, but messages which are flagged by a as [sic] suspicious may be stored indefinitely, and select messages may be read by a human being to improve Omegle's anti-spam software, or for other quality control purposes.

expectation of privacy in the content of his chats and (2) constitutes a "binding" consent by Wilbert to allow Omegle to search and reveal the content of his video communications. See Gov't Suppl. Br., Docket 72, at 13-18. K-Brooks testified that upon entering the site, but before engaging in a chat, the platform displays a link to the privacy policy. Tr. at 22-23. At the bottom of the login screen, users are notified that they agree to Omegle's terms of service by Using the site. Tr. at 87.

The issue of how one's privacy rights are impacted by website "warnings" or by specific agreement to a posted TOS is a difficult one. Wilbert relies on *United States v. DiTomasso, 56 F. Supp. 3d 584 (S.D.N.Y. 2014)*, a Southern District of New York case involving Omegle in which the court expressly rejected the argument **[*20]** the government makes now. While that case dealt with a text chat rather than a video chat, the court analyzed the language of Omegle's privacy policy and concluded that

> it would subvert the purpose of the *Fourth Amendment* to understand its privacy guarantee as "waivable" in the sense urged by the government. In today's world, meaningful participation in social and professional life requires using electronic devices—and the use of electronic devices almost always requires acquiescence to some manner of consent-to-search terms. If this acquiescence were enough to waive one's expectation of privacy, the result would either be (1) the chilling of social interaction or (2) the evisceration of the *Fourth Amendment*. Neither result is acceptable.

DiTomasso, 56 F. Supp. 3d at 592. The court in DiTomasso held that the language contained in Omegle's privacy policy was not so clear and explicit as to completely destroy the defendant's expectation of privacy:

> Omegle took snapshots of DiTomasso's chats and parsed them for content. Although that form of monitoring is referenced in the policy, it is mentioned exclusively as a means of "monitoring for misbehavior"—by which the policy clearly means violations of Omegle's rules, not criminal activity—and of improving **[*21]** Omegle's internal monitoring system.
>
> A reasonable person, having read carefully through the policy, would certainly understand that by using Omegle's chat service, he was running the risk that another party—including Omegle—might divulge his Sensitive information to law enforcement. But this does not mean that a reasonable person would also think that he was consenting to let Omegle freely monitor his chats if Omegle was working as an agent of law enforcement. When Omegle's policy refers to the "law enforcement [purpose]" behind maintaining IP address records, it is unclear whether this "purpose" is motivated (1) by Omegle's independent desire to aid criminal investigations, or (2) by Omegle'S obligations under state or federal law. In other words, it is plausible to interpret the policy as implying that OMegle is required to keep IP address records. So construing the policy, a reasonable user would be unlikely to conclude that Omegle intended to act as an agent of law enforcement. And such a user would be even less likely to conclude that he had agreed to permit such conduct.

Id. at 596-97 (emphasis supplied) (footnotes omitted).

The government obviously disagrees with the DiTomasso holding that **[*22]** Omegle users have privacy rights in their online chats. See Docket # 72, at 11-12. The government points the Court to the so-called "third-party doctrine" which provides that "[p]eople who share information with third parties assume the risk that their information would be shared with law enforcement." Docket # 72, at 12; see *Smith v. Maryland, 442 U.S. 735, 743-*

> At the beginning of every chat, a record is made of the fact that a chat has occurred between you and your chat partner. These records may be used for the purpose of tracking spammers, hackers, and others who pose harm to the site; and may also be Used for law enforcement purposes . . . .
>
> Webcam images may be captured from Omegle video chats, uploaded to Omegle's servers, and monitored for misbehavior as part of Omegle's moderation process. . . .
>
> The records Omegle keeps may be shared with third parties for the purpose of law enforcement, to monitor and enforce compliance with Omegle's rules, or to improve Omegle's monitoring and enforcement process.

Hr'g Ex. 3.

44, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). But, as with other Fourth Amendment principles, courts are now grappling with whether the downloading of an "app" or the use of a website in today's world of ESI reflects the same relinquishment of privacy rights in which the third party doctrine was grounded. Indeed, in Carpenter v. United States, U.S. , 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018), Chief Justice Roberts referred to "the seismic shifts in digital technology" as a basis for rejecting the government's argument that the third party doctrine allows law enforcement access to cell phone records created and stored by the phone carrier. 138 S. Ct. at 2219. "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." Id. at 2217. The vast amount and personal nature **[*23]** of information stored on our electronic devices through websites and apps expands every day and includes not only location information, but our pulse rates, blood pressure, calorie consumption, credit card numbers, prescription and medical information, music and podcast choices, child monitoring cameras, thermostat controls, travel plans and airline tickets, shopping interests and purchases, diary entries and new year resolutions, prayer books, photographs and real time conversations with friends and family members. The list goes on and on and continues to exponentially explode with new technology and applications. Do we automatically relinquish Fourth Amendment protections to this highly personal data because the information is no longer physically stored in a file cabinet or a bookshelf or a desk drawer, but instead is digitally captured On an "app" we downloaded On our phone or other internet-Connected device from a "third party"? Obviously, this case involves Only Omegle, a Website inviting users to privately and anonymously communicate with another person. But whether simply posting a "warning banner" on a Website that refers a user to the website's privacy statement unequivocally "binds" the **[*24]** user to anything and everything, contained in the third party's terms of service may be not be as Cut and dry as the government asserts.

As it turns out, what matters most in deciding the defendant's suppression motion is the "private search doctrine." The "Fourth Amendment's guarantee to be free from unreasonable search and seizure is directed at [g]overnment activity." United States v. Heleniak, No. 14-cr-42A, 2015 U.S. Dist. LEXIS 15354, 2015 WL 521287, at *4 (W.D.N.Y. Feb. 5, 2015). The Fourth Amendment's protections are "wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the [g]overnment or with the participation or knowledge of any governmental official.'" United States v. Jacobsen, 466 U.S. 109, 113-114, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984) (quoting Walter v. United States, 447 U.S. 649, 662, 100 S. Ct. 2395, 65 L. Ed. 2d 410 (1980) (Blackmun, J., dissenting)).

Omegle is obviously a private company and Wilbert does not claim otherwise. Thus, the flagging of the offending images by Omegle's surveillance algorithm and the viewing of the images by the private moderators employed by Omegas by themselves raise no Fourth Amendment concerns. Where Wilbert's motion gets tricky, however, is the transmittal of the images by Omegle to NCMEC and NCMEC's subsequent transmittal to law enforcement. In Jacobsen the Supreme Court held that where a governmental search expands the scope of a private one "[t]he **[*25]** additional invasions of [a person's] privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search." Id. at 115. "A private party acting as a government agent also may not expand upon a previously private search without running afoul of the Fourth Amendment." United States v. Knoll, 16 F.3d 1313, 1320 (2d Cir. 1994). Here, the two image files captured by Omegle (c6d0 and a9e7) were passed on to NCMEC and then to the NYSP. The latter is obviously a law enforcement agency subject to the Fourth Amendment. But what about NCMEC?

In United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016), the Tenth Circuit held that NCMEC acts as a government entity, or at least an agent of the government, when it creates and maintains CyberTipline reports for Congress and reports suspected illegal content to law enforcement. In an opinion written by now Supreme Court Justice Gorsuch, the court analyzed the statutory structure governing NCMEC and its obligations to collaborate with law enforcement agencies. See 42 U.S.C. § 5773(b); 18 U.S.C. § 2258A. The Court held that because Congress statutorily required Electronic Service Providers ("ESPs") to report content containing suspected child pornography to NCMEC, required NCMEC to maintain the CyberTipline to receive illegal content, permitted NCMEC to review suspected child pornography, and **[*26]** statutorily requited NCMEC to forward CyberTipline reports to any

appropriate law enforcement agency, "NCMEC qualifies as a governmental entity" for purposes of the *Fourth Amendment*. *Ackerman, 831 F.3d at 1297*.[9]

For purposes of this Report and Recommendation, the Court will assume without deciding that the Tenth Circuit's decision in *Ackerman* is correct and NCMEC is a governmental entity, or at least an agent of the government. Even with that assumption, however, the hearing testimony does not support a finding that NCMEC, as a governmental entity, expanded the scope of the private search conducted by either Omegle or its private video chat monitors. K-Brooks testified that although he could not be certain, as far as he could tell it appears only image c6d0 was definitely flagged as containing suspected child pornography and reviewed by a monitor. Tr. at 53-54. The report uploaded by Omegle to the CyperTipline website (Hr'g Ex. 7) also supports a finding that only image c6d0 was viewed by the monitor. And finally, Shehan testified that based on his review of the CyberTipline report received from Omegle, he believes only image c6d0 was viewed by NCMEC staff and image a9e7 was never even made available for viewing. **[*27]** Tr. at 120-22.

Nevertheless, there is no question that both images were attached to the CyberTipline Report that was uploaded and submitted to the NYSP by NCMEC. Thus, the next question is: Even if NCMEC did not expand the private search of Wilbert's video chat, did the NYSP? As to this issue, the evidence was unequivocal. NYSP Investigator David Cerretto confirmed that he accessed and viewed both images in connection with his investigation of Wilbert and he was aware that only image c6d0 had been viewed by Omegle and NCMEC. Indeed, according to Cerretto, it was the policy of the NYSP to open and view every image submitted to them through the CyberTipline regardless of whether the image or its content had been previously viewed by a private party or entity. Tr. at 168-69, 190. Thus, it appears certain that the NYSP did expand the scope of the Omegle's private search of Wilbert's video chat by opening image a9e7.

Of course, to even get to this point in the analysis Wilbert would have had to run the gauntlet of various *Fourth Amendment* issues' the Court has briefly touched upon. Assuming Wilbert was able to overcome issues of standing and reasonable expectations of privacy, as well as successfully navigate **[*28]** application of the consent to search doctrine and the private search doctrine, he would appear to have a strong argument that law enforcement violated the *Fourth Amendment* by exceeding the scope of the private search. And Investigator Cerretto testified that based on the images and further investigation, he applied for and obtained a state search warrant (Hr'g Ex. 12) for the upstairs apartment at 634 Garson Avenue in Rochester, New York and discovered what we know was Wilbert's laptop computer. If the NYSP did improperly expand the scope of the Omegle's private search of Wilbert's video chat by opening image a9e7 and then relied on that image as part of their factual justification to obtain a search warrant to search 634 Garson Avenue for computers containing child pornography, does the inclusion of tainted evidence lead Wilbert to achieving suppression of the evidence obtained from his computer?

Unfortunately for Wilbert, it is at this juncture where his suppression motion arguments falls apart.

> [T]he inclusion in an affidavit of indisputably tainted allegations does not necessarily render the resulting warrant invalid. The ultimate inquiry on a motion to suppress evidence seized pursuant to a warrant **[*29]** is not whether the underlying affidavit contained allegations based on illegally obtained evidence, but whether, putting aside all tainted allegations, the independent and lawful information stated in the affidavit suffices to show probable cause.

United States v. Giordano, 416 U.S. 505, 555, 94 S. Ct. 1820, 40 L. Ed. 2d 341 (1974) (Powell, J. concurring) (emphasis added); see *United States v. Trzaska, 111 F.3d 1019, 1026 (2d Cir. 1997)* ("[A] reviewing court Should excise the tainted evidence and determine Whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant.")(quoting *United States v. Vasey, 834 F.2d 782, 788 (9th Cir.*

---

[9] In fact, according to NCMEC's John Shehan, and probably in response to the Ackerman decision, NCMEC has a policy to not open electronic files containing suspected child pornography that have not been previously opened or viewed by the private party submitting the materials through NCMEC's CyberTipline. Shehan testified that this policy is followed to foreclose any claim that NCMEC expanded the scope of a search initially conducted by a private entity.

1987)). Investigator Cerretto testified that image c6d0 was an image of a dog performing oral sex on a naked female child, but he "was not able to tell" what was happening in image a9e7.[10] Tr. at 170. Image c6d0 was not "tainted" as it was flagged, opened and viewed by Omegle and Omeglers private monitors before being transmitted to law enforcement. It was only the indecipherable image, image a9e7, that was arguably tainted by law enforcement expanding the private search and viewing this second image.

If the "ultimate inquiry" for suppression is whether "putting aside all tainted allegations, the independent and lawful information stated in the affidavit suffices to show probable cause," (*Giordano, 416 U.S. at 555*) then the answer **[*30]** is self-evident. Image c6d0 depicts child pornography. The "tainted" file, image a9e7, does not depict child pornography and hence could not have added anything the judge's probable cause determination. Excising the tainted image from the probable cause calculation yields the same result as including it: On October 25, 2015 someone Using an IP address assigned to Scott Wilbert at 634 Carson Avenue uploaded an image of a "prepubescent" female child between age 4 and 7 who was engaged with oral sex With a K-9" through the Omegle website and Wilbert was identified as a level 2 registered sex offender who in 2014 had been investigated by the NYSP for uploading images of child pornography. See Hr'g Ex. 12. Even if the "tainted" evidence was excised, the untainted evidence would provide a "neutral magistrate" with ample probable cause to issue the search warrant.

Request or a Franks Hearing: Alternatively, Wilbert seeks a hearing pursuant to *Franks v. Delaware, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978)*. The Second Circuit has held that:

> To be entitled to a Franks hearing, a defendant must make a "substantial preliminary showing" that: (1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and **[*31]** (2) the alleged falsehoods or omissions were necessary to the judge's probable cause finding. If, after setting aside the allegedly misleading statements or omissions, the affidavit, nonetheless, presents sufficient information to support a finding of probable cause, the district court need not conduct a Franks hearing.

United States v. Salameh, 152 F.3d 88, 113 (2d Cir. 1998) (internal citations omitted).

Here, I find the defendant has failed to make the required showing necessary for the Court to order a Franks hearing. Wilbert claims that the affidavit in support of the search warrant Was deliberately and Materially inaccurate because (1) Cerrette falsely described What image c6d0 (Hr'g Ex. 1) depicted and (2) Cerretto falsely stated the time image c6d0 was Uploaded. Neither allegation Merits the convening Of a Franks hearing. As to Cerretto's description of image c6d0, the Court finds that it was reasonably accurate and certainly provides probable cause that the image depicted constituted child pornography. As to any inaccuracy in the time image c6d0 was Upleaded, Cerretto Credibly testified that he included the upload time of 2:30:12 simply because he viewed that time as the beginning of a continuous event that encompassed the upload **[*32]** of the two images. Moreover, even assuming this was inaccurate, there is no evidence to suggest that the alleged inaccuracies were deliberate or material. *United States v. Longo, 70 F. Supp. 2d 225, 254 (W.D.N.Y. 1999)* (where alleged misrepresentations and omissions in the supporting affidavit were "inconsequential to the finding of probable cause," Franks hearing unnecessary).

Motion to Dismiss Indictment: Finally, Wilbert asks this Court to dismiss the indictment because the government did not request the defendant's "actual chats." Def.'s Br. (Docket # 42-1), at ¶ 26. However, the government could not have requested the "actual chats" because, as the testimony at the hearing established, Omegle does not keep the video chats themselves; it only keeps the metadata, which was provided to the government and the defense-. The copies of the video chats simply never existed, and there was never anything to preserve. Accordingly it is my Report and Recommendation that Wilbert's motion to dismiss the indictment should be **denied**.

Conclusion

---

[10] The Court reviewed the two images during the hearing (Hr'g Exs. 1 & 2) and agrees with Cerretto's description of the images.

For the foregoing reason, it is My Report and Recommendation that the defendant's motion to suppress evidence (Docket # 42) during the search of Wilbert's computer be **denied.** It is my further Report and Recommendation **[*33]** that Wilbert's request for a "Franks hearing" be **denied** and that his motion to dismiss the Indictment for failure to preserve evidence be **denied.**

SO ORDERED.

/s/ Jonathan W. Feldman

JONATHAN W. FELDMAN

United States Magistrate Judge

Dated: August 20, 2018

Rochester, New York

Pursuant to *28 U.S.C. § 636(b) (1)*, it is hereby

ORDERED, that this Report and Recommendation be filed with the Clerk of the Court.

ANY OBJECTIONS to this Report and Recommendation must be filed with the Clerk of this Court within fourteen (14) days after receipt of a copy of this Report and Recommendation in accordance with the above statute and Rule 59(b) (2) of the Local Rules of Criminal Procedure for the Western District of New York.[1]

The district court will ordinarily refuse to consider on de novo review arguments, case law and/or evidentiary material which could have been, but was not, presented to the magistrate judge in the first instance. See, e.g., *Paterson-Leitch Co., Inc. v. Mass. Mun. Wholesale Elec. Co., 840 F.2d 985 (1st Cir. 1988)*.

Failure to file objections within the specified time or to request an extension of such time waives the right to appeal the District Court's Order. *Thomas v. Arn, 474 U.S. 140, 106 S. Ct. 466, 88 L. Ed. 2d 435 (1985)*; *Wesolek v. Canadair Ltd., 838 F.2d 55 (2d Cir. 1988)*.

The parties are reminded that, pursuant to Rule 59(b) (2) of the Local Rules of Criminal Procedure for the Western District of New York, "[w]ritten objections . . . Shall specifically identify **[*34]** the portions of the proposed findings and recommendations to which Objection is made and the basis for each objection, and shall be supported by legal authority." **Failure to comply with the provisions of Rule 59(b) (2) May result in the District Court's refusal to consider the objection**.

Let the Clerk send a copy of this Order and a copy of the Report and Recommendation to the attorneys for the Plaintiff and the Defendant.

SO ORDERED.

/s/ Jonathan W. Feldman

Jonathan W. Feldman

United States Magistrate Judge

---

[1] Counsel is advised that a new period of excludable time pursuant to *18 U.S.C. § 3161.(h)(1)(D)* commences with the filing of this Report and Recommendation. Such period of excludable delay lasts only until objections to this Report and Recommendation are filed or until the fourteen days allowed for filing objections has elapsed. *United States v. Andress, 943 F.2d 622 (6th Cir. 1991)*, cert. denied, ***502 U.S. 1103, 112 S. Ct. 1192, 117 L. Ed. 2d 433 (1992)***; *United States v. Long, 900 F.2d 1270 (8th Cir. 1990)*.

Dated: August 20, 2018

Rochester, New York

End of Document

United States v. Wilbert

United States District Court for the Western District of New York

May 22, 2017, Decided; May 22, 2017, Filed

16-CR-6084L

Reporter
2017 U.S. Dist. LEXIS 77141 *; 2017 WL 2224201

UNITED STATES OF AMERICA, Plaintiff, v. ***SCOTT T. WILBERT***, Defendant.

Prior History: *United States v. Wilbert, 2017 U.S. Dist. LEXIS 77818 (W.D.N.Y., Mar. 28, 2017)*

Core Terms

Recommendation, pornography, suppress, incriminating, pretrial, upstairs, seized

Counsel: **[*1]** For ***Scott T. Wilbert***, Defendant: Robert A. Napier, LEAD ATTORNEY, Napier & Napier, Rochester, NY.

For USA, Plaintiff: Kyle P. Rossi, Melissa M. Marangola, LEAD ATTORNEYS, U.S. Attorney's Office, Rochester, NY.

Judges: DAVID G. LARIMER, United States District Judge.

Opinion by: DAVID G. LARIMER

Opinion

DECISION AND ORDER

Defendant, ***Scott T. Wilbert*** ("Wilbert"), has been indicted in a single count of possession and receipt of child pornography. This Court referred all pretrial matters and motions to United States Magistrate Judge Jonathan W. Feldman pursuant to *28 U.S.C. § 636(b)*.

STEVEN FELDMAN

Wilbert filed several pretrial motions many of which were decided from the Bench by Magistrate Judge Feldman on December 8, 2016. Two motions were not resolved in that fashion. They included defendant's motion to suppress evidence seized pursuant to a search warrant and a motion for a so-called *Franks* hearing.[1]

The issues pending before Magistrate Judge Feldman, and now this Court, involved defendant's motion to suppress evidence relating to child pornography that was seized from an upstairs apartment at 634 Garson Avenue, Rochester, New York pursuant to a search warrant signed by Monroe County Court Judge Victoria M. Argento.

Defendant raises several issues concerning **[*2]** the warrant. He challenges the affidavit in support of the warrant and claims it did not establish proper connection between the crime and the premises sought to be searched. He also contends the warrant is overbroad and requests the *Franks* hearing contending that the information provided by the affiant was deliberately or recklessly imprecise. Defendant also contends that the execution of the warrant was delayed unreasonably and, therefore, it was stale.

Magistrate Judge Feldman issued a thorough Report and Recommendation (Dkt. #32) concerning these issues. He recommended that this Court deny the motion to suppress and deny the request for a *Franks* hearing. Defense counsel duly filed Objections to that Report and Recommendation (Dkt. #36).

I have reviewed the Report and Recommendation, the papers submitted on the motion, as well as defendant's present Objections to the Report and Recommendation. I believe the Magistrate Judge correctly analyzed the facts and the law, and I accept the Report and Recommendation. I see no basis to reverse, modify or alter that recommendation.

I believe the warrant that led to the seizure of the incriminating child pornography was sufficiently precise as **[*3]** to the premises to be searched, that is, the upstairs apartment or "Apartment Up" at 634 Garson Avenue, Rochester, New York. That was the premises searched which led to the discovery of the incriminating evidence. Magistrate Judge Feldman properly focused on the actual warrant issued rather than portions of the affidavit in support of the warrant.

I also agree with Magistrate Judge Feldman that although there was a delay of several weeks before the warrant was executed, in cases such as this, involving child pornography, especially concerning an individual that had previously been convicted of criminal sexual acts and was registered as a sex offender, as Magistrate Judge Feldman pointed out, under these circumstances delay in executing the warrant was not improper.

I also agree with Magistrate Judge Feldman that there is no basis to conduct the *Franks* hearing. Magistrate Judge Feldman determined that the warrant satisfied the particularity requirement under the *Fourth Amendment* and, therefore, there was no need for any further hearing.

CONCLUSION

I accept and adopt the Report and Recommendation (Dkt. #32) issued by United States Magistrate Judge Jonathan W. Feldman. I concur and adopt his recommendation. **[*4]**

Defendant's motion to suppress physical evidence obtained pursuant to a search warrant and his motion for a *Franks* hearing are in all respects denied.

IT IS SO ORDERED.

/s/ David G. Larimer

DAVID G. LARIMER

United States District Judge

---

[1] *Franks v. Delaware, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978)*.

Dated: Rochester, New York

May 22, 2017.

End of Document