

**UNITED STATES DISTRICT COURT  
DISTRICT OF MAINE**

<b>UNITED STATES OF AMERICA</b>	)	
	)	
<b>v.</b>	)	<b>CRIMINAL No. 2:11-CR-113-DBH</b>
	)	
<b>SHAWN SAYER,</b>	)	
	)	
<b>DEFENDANT</b>	)	

**DECISION AND ORDER ON DEFENDANT’S MOTION TO SUPPRESS  
OR EXCLUDE EVIDENCE AND REQUEST FOR A FRANKS HEARING**

The issue on this motion is whether I should suppress as evidence a variety of statements (spoken and digital); physical materials; and observations law enforcement agents made while on or near the defendant’s property. The defendant raises a variety of constitutional, statutory and Federal Rule issues. After oral argument and a partial evidentiary hearing on May 4, 2012 (the evidentiary hearing concerned whether the defendant was in custody at the time he was questioned on November 5, 2009), the motion is **DENIED**.

**NATURE OF THE CASE**

The grand jury indicted the defendant for both interstate cyberstalking and identity theft. 18 U.S.C. § 2261A; 18 U.S.C. § 1028. As summarized in my ruling on the defendant’s motion to dismiss the cyberstalking charge, the government’s contention is that, after the defendant’s former girlfriend changed her name and moved from Maine to Louisiana to escape him, the defendant, still in Maine,

created fictitious internet advertisements and social media profiles using [the victim's] name and other identifying information. The fictitious internet postings included [the victim's] address and invited men to come to her home for sexual encounters. The Defendant also posted video clips to several adult pornography websites depicting sexual acts [the victim] had consensually performed with him during their relationship. The Defendant edited the clips so they also displayed [the victim's] name and actual address. As a result of the Defendant's actions, numerous men arrived at [the victim's] Louisiana residence seeking sexual encounters, terrifying her and causing her to fear that she would be raped or assaulted.

Gov't's Opp'n to Def.'s Mot. to Dismiss Count One of the Indictment at 2 (ECF No. 84). The defendant largely agrees that such is the government's case. See Order on Def. Sayer's Mot. to Dismiss Count One of the Indictment and Def. Thomas's Mot. to Dismiss Count Eight of the Superseding Indictment (ECF No. 108). But those allegations are not yet proven, and I repeat them only so that the significance of the evidentiary disputes can be understood.

## **ANALYSIS**

### **A. *Evidence Obtained without a Warrant***

#### ***(1) Invasion of Curtilage***

The defendant argues that law enforcement violated his Fourth Amendment rights by obtaining certain information without a warrant on October 29, 2009,<sup>1</sup> inside the curtilage of his residence. What law enforcement did was drive into his driveway entrance, ostensibly to turn around, and while in the entrance used a laptop computer to determine what wireless signals could be detected there.

---

<sup>1</sup> The defendant's brief provides the date as October 29, 2011, but that year is clearly an error.

The Supreme Court has held that the Fourth Amendment protects not only the house, but the “curtilage” of a house, an area that should be treated as the home itself as distinguished from open fields that might surround it.

United States v. Dunn, 480 U.S. 294 (1987). According to Dunn:

curtilage questions should be resolved with particular reference to four factors: the proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by.

Dunn, 480 U.S. at 301. This defendant’s driveway entrance satisfies none of those four factors. His driveway entrance is not close to his home; there is no enclosure; the area is used to access the driveway from the public street (for example by delivery people); and nothing protects the area from observation by people passing by. A photograph of the house and driveway makes that all obvious. Photograph attached as Ex. B to the Decl. of Detective Laurie N. Northrup (ECF No. 82). Moreover, the First Circuit has stated: “If the relevant part of the driveway is freely exposed to public view, it does not fall within the curtilage.” United States v. Brown, 510 F.3d 57, 65 (1st Cir. 2007). That is the case here.

I conclude that law enforcement did not invade the curtilage of the defendant’s residence. What they observed in the driveway turnaround, therefore, need not be suppressed.

**(2) Wireless Survey of WiFi/Internet Signals With no Warrant**

The defendant argues that regardless of the legality of the driveway turnaround, it was still an illegal warrantless search to do a “wireless survey of

WiFi/Internet signals” on October 29, 2009. Def.’s Mot. to Suppress/Exclude Evid. and Request for Testimonial Hr’g, including *Franks* Hr’g at 9 (“Def.’s Mot. to Exclude/Suppress Evid.”) (ECF No. 65). The defendant relies upon the reasoning of Kyllo v. United States, 533 U.S. 27 (2001). There, the Court held that law enforcement “use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home,” 533 U.S. at 29, was a search for Fourth Amendment purposes—“at least where (as [in Kyllo]) the technology in question is not in general public use.” Id. at 35.

Unlike Kyllo, what law enforcement detected here was not a signal that was in or coming from the defendant’s residence; instead, the assertion is that the detected signals came from a wireless router in a neighbor’s house across the street. (Apparently part of the government’s case is that the defendant used others’ wireless access so that his actions could not be traced to him.) Moreover, the technology that they used is in general public use; anyone with a laptop with wireless capability can find evidence of WiFi signals. This is not Kyllo’s advanced technology “not in general public use.”

Moreover, if the police did not invade his curtilage, then the defendant has no standing to object to their discovery of the signals they detected, because they did not come from the defendant or his residence, but from others. The defendant therefore has no standing to challenge their detection.<sup>2</sup>

---

<sup>2</sup> At oral argument the defendant’s lawyer said that earlier references to password-protected online accounts have no relevance to this issue.

### ***(3) Installation of Live-Feed Camera Trained on Defendant's Front Door***

With a neighbor's permission, on April 1, 2010, law enforcement positioned a small live-feed video camera in a yard across from the defendant's house and left it there until early May. The government says that the camera recovered nothing useful and that no observations from it will be used at trial. As a result, at oral argument the defendant's lawyer no longer pressed the issue.<sup>3</sup>

### ***(4) Statutory Violations***

At oral argument, the defendant waived his written contention that I should suppress a variety of evidence that he says law enforcement obtained in violation of the Stored Communications Act (part of the Electronic Communications Privacy Act) by using subpoenas to obtain information from PayPal, Facebook, MySpace and Yahoo. Def.'s Mot. to Exclude/Suppress Evid. at 11.<sup>4</sup>

---

<sup>3</sup> I note that the affidavit submitted to the Magistrate Judge for a warrant in September 2010, does refer to an observation from the live feed. Specifically, paragraph 26 of that affidavit says that the camera showed the defendant leaving his house at 1:45 p.m. on April 2, and that at 6:37 p.m. a new Facebook account was created purporting to be the victim. Aff. of Laurie Northrup in Support of an Application for a Search Warrant ¶ 26 (ECF No. 78-6). Nevertheless, I conclude that paragraph 26 played no role in the determination of probable cause for the September 2010 warrant. There was an abundant amount of probable cause without that paragraph, and the paragraph does not even explain how leaving his house five hours earlier would suggest that the defendant was the one who created the new Facebook account. There is no other reference to the date and time. I therefore find it unnecessary to address the constitutionality of law enforcement using the live-feed camera in this fashion.

<sup>4</sup> In any event, a plain reading of the statutory language forecloses the relief he seeks. According to 18 U.S.C. § 2708, "[t]he remedies and sanctions described in this chapter [which covers the two Acts] are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." Suppression of evidence is not one of the statutorily provided remedies and sanctions. See 18 U.S.C. §§ 2701, 2707, 2712. Thus, if there were any statutory violations, suppression is not available. The cases agree. See, e.g., United States v. Clenney, 631 F.3d 658, 667 (4th Cir. 2011); United States v. Li, 2008 WL 789899 at \*3 (S.D. Cal. 2008).

### ***(5) Custodial Questioning***

The defendant contends that his November 5, 2009, statements should be suppressed because law enforcement officers did not give him Miranda warnings. Miranda v. Arizona, 384 U.S. 436 (1966). The necessity for Miranda warnings depends on whether a suspect is in custody. Oregon v. Mathiason, 429 U.S. 492, 495 (1977); United States v. Quinn, 815 F.2d 153, 160 (1st Cir. 1987). When making such a determination, I must examine whether “there is a formal arrest or restraint on freedom of movement of the degree associated with a formal arrest.” Maryland v. Shatzer, 130 S. Ct. 1213, 1224 (2010) (quoting New York v. Quarles, 467 U.S. 649, 655 (1984)). In the absence of a formal arrest, determining whether a person is in custody requires me to engage in a two-step inquiry. First, I must ascertain the circumstances surrounding the interrogation. Thompson v. Keohane, 516 U.S. 99, 112 (1995). Second, I must examine whether, viewed objectively, the discerned circumstances constitute the requisite “restraint on freedom of movement of the degree associated with a formal arrest.” California v. Beheler, 463 U.S. 1121, 1125 (1983) (per curiam) (internal quotation omitted). The determination of whether custody exists “depends on the objective circumstances of the interrogation, not on the subjective views harbored by either the interrogating officers or the person being questioned.” Stansbury v. California, 511 U.S. 318, 323 (1994).

The First Circuit has identified four factors that, among others, may inform a determination of whether, short of actual arrest, an individual is in custody. These factors include “where the questioning occurred, the number of

officers, the degree of physical restraint, and the duration and character of the interrogation.” United States v. Teemer, 394 F.3d 59, 66 (1st Cir. 2005); see also Ventura, 85 F.3d 708, 711 (1st Cir. 1996) (quoting United States v. Masse, 816 F.2d 805, 809 (1st Cir. 1987)) (custody inquiry includes “whether the suspect was questioned in familiar or at least neutral surroundings, the number of law enforcement officers present at the scene, the degree of physical restraint placed upon the suspect, and the duration and character of the interrogation.”); United States v. Hughes, 640 F.3d 428, 434-35 (1st Cir. 2011). Measuring the defendant’s encounter with law enforcement against these factors, I conclude that it did not rise to the level of custodial interrogation.

The defendant moves to suppress the statements he made to law enforcement officers during the November 5, 2009 search of his home. His argument is a simple one: under the totality of the circumstances, he was “in custody” and should have been advised of his Miranda rights before law enforcement began asking questions. Miranda v. Arizona, 384 U.S. at 478–79. The defendant did not testify at the suppression hearing. But Maine State Police Officer Glenn Lang did, and this is what he says happened. At approximately 11:00 a.m. three law enforcement officers arrived at the defendant’s home—Maine State Police officers Glenn Lang and Laurie Northrup, and Secret Service Agent Manning Jeter. Lang was wearing battle fatigues with a bulletproof vest and a weapon visible on his hip. Northrup and Jeter wore plain clothes and their weapons were not visible. In addition, there were two or three uniformed Biddeford police officers outside the defendant’s home at the beginning of the search.

After arriving, the officers told the defendant that they had a search warrant, gave him a copy of the warrant and explained that they believed that he was stalking his former girlfriend by creating fictitious Internet advertisements and social media profiles using the victim's name. The defendant denied any involvement. Importantly, Lang explained to the defendant that he was not under arrest and that he was free to leave the home during the search but, if he stayed, he had to remain in the kitchen. The defendant stayed in the kitchen. At one point during the search, the defendant told Lang he had to go to the bathroom and the defendant was escorted to the bathroom but he was not allowed to close the door.

At various points in the search, Lang engaged in conversation and questioning of the defendant. Specifically, the defendant was asked if he was involved and whether he wanted to talk to them about his involvement. Lang told the defendant that he believed that the defendant had committed a crime under Maine and federal law. Lang testified that at the end of the search he became more "abrasive" with the defendant telling him that he did not believe the defendant's explanation that someone else was attempting to set the defendant up. Indeed, Lang conveyed to the defendant that he thought he was lying. Even when Lang turned up the heat on the defendant, Lang described the defendant as calm.

During the search the officers found two desktop computers without hard drives, numerous computer components, a laptop case and a digital camera with a USB cable attached. The officers asked the defendant about the absence of the hard drives and the whereabouts of the laptop that went in the

case. The defendant explained that the desktop computers had become corrupt so the hard drives were thrown away. The laptop had water spilled on it, the defendant told Lang, so it too had to be discarded. At one point in the search, the defendant used the telephone and Lang thought that he spoke to either his brother or his attorney. At another point during the search, the defendant's father came home. The officers were at the defendant's home for 60 to 90 minutes. The defendant never asked to stop talking with the officers. Beyond being asked to stay in the kitchen, the defendant was never restrained and no physical force was ever used on the defendant. The officers never unholstered their weapons.

Measured against these factors, the complained-of encounter did not rise to the level of a custodial interrogation. True, officers questioned the defendant during the search of his home. But the defendant was specifically told that he was not under arrest and did not have to stay during the search. See, e.g., United States v. McCarty, 475 F.3d 39, 46 (1st Cir. 2007) (stressing that details like these support a no-custody finding); United States v. Ellison, 632 F.3d 727, 730 (1st Cir. 2010) (similar). The interaction between the defendant and the officers was calm and nonthreatening, and the defendant expressed no qualms about talking with them. Although Lang was in "battle fatigues" with his weapon visible, the other officers wore plain clothes and their weapons were not visible. See, e.g., Hughes, 640 F.3d at 436 (finding no custody in a factually similar situation). No one screamed at the defendant, badgered him for answers, or menaced him in any way. See, e.g., id. at 437 (highlighting caselaw finding no custody where officers acted in a similarly nonthreatening

way). The search lasted a relatively short time too, roughly 60 to 90 minutes, and the defendant was questioned only intermittently throughout the search. See, e.g., *id.* (ruling that an interview lasting 90 minutes was not custodial); *United States v. Nishnianidze*, 342 F.3d 6, 14 (1st Cir. 2003) (holding that a 45-minute interview did not implicate *Miranda*). Based on these facts, I find that the interview was noncustodial.

**B. Warrant Issues**

**(1) *Franks* Hearing**

The defendant argues that the affidavits law enforcement submitted in support of three separate warrants and two tracking orders<sup>5</sup> were consciously false or contained material omissions, and that I should hold an evidentiary hearing in accordance with the standards of *Franks v. Delaware*, 438 U.S. 154 (1978), to allow the defendant to establish his assertion.

There is a “presumption of validity with respect to the affidavit supporting the search warrant.” *Id.* at 171. To obtain a *Franks* hearing, the defendant first must “make a substantial preliminary showing that the affidavit included a false statement which was made either knowingly or intentionally or with reckless disregard for the truth, and that this misstatement was necessary to the finding of probable cause.” *United States v. Materas*, 483 F.3d 27, 31 (1st Cir. 2007) (internal quotations omitted). Likewise, “[a] material omission in the affidavit may also qualify for a *Franks* hearing in place of a false direct statement, provided the same requisite showing is made.” *United States v.*

---

<sup>5</sup> In the end, only one tracking order generated evidence. See section (B)(2)(c) *infra*.

Nelson-Rodriguez, 319 F.3d 12, 34 (1st Cir. 2003). If an omission is involved, a defendant must demonstrate that inclusion of the item would have negated the finding of probable cause. United States v. Castillo, 287 F.3d 21, 25 n.4 (1st Cir. 2002).

***(2) Probable Cause for each of Three Separate Warrants and a Tracking Order***

***(a) November 4, 2009, Warrant Application***

The first search warrant issued in this case was signed November 4, 2009, and was for the defendant's house. The application for that search warrant included the following information, which I summarize from Northrup's affidavit. Aff. of Detective Laurie Northrup (ECF No. 78-1).

While living in Maine, the victim dated the defendant. In January 2006, after they broke up, the defendant began to stalk and harass the victim. Thereafter, the defendant was convicted in Maine Superior Court for stalking the victim. The victim then obtained a protection from abuse order against the defendant and in February 2008 the defendant was convicted of violating that protective order. On several occasions in October 2008 men came to the victim's home saying that they had met her on the Internet and were looking for sexual encounters. Later, the victim found an ad on Craigslist under the heading "casual encounters" that provided pictures of her in lingerie that the defendant had taken before they split up. In addition, the ad included directions to her

home and a list of “sexual things” she would do when they got there.

To get away from the stalking, the victim changed her name and moved to Louisiana. In August 2009, the same thing started to happen—men whom she did not know started to arrive at her home in Louisiana, saying that they had met her on the Internet and were looking for sexual encounters. During August 2009, a sexually explicit video of the victim, consensually taken with the defendant while they were dating, was posted on several adult pornography sites. These sites also listed the victim’s new name as well as her original given name and her Louisiana address. The internet postings were not made by the victim.

In September 2009, a new Facebook account was created in the victim’s name and included a photograph of her. The victim did not create this account, but the IP address of where the account was created was in Biddeford, Maine and assigned to Richard Cook, who lived across the street from the defendant and had an unsecure wireless internet connection.

Based on this information, a Maine District Court Judge issued a warrant to search the defendant’s home, and to seize computers, computer equipment, cameras, and computer records or data. Search Warrant at 2 (ECF No. 78-1).

***(i) Franks Issues***

The defendant contends that Detective Northrup's affidavit contains the false statement that "[o]nly [the defendant] would have had access to the pictures which had been posted." Northrup Aff. ¶ 5 (ECF No. 78-1). The defendant explains that, prior to 2008, sexually explicit photographs of the victim had been uploaded to the Internet and, thus, that many people had access to the photographs referenced in the affidavit. In the context of the affidavit, however, it is clear that Northrup is recounting information reported by the victim, not making a direct assertion. The defendant further points out that when these photographs surfaced in 2008, the South Portland Police investigated and told the victim that they could not prove that the defendant was posting them. Therefore, the defendant asserts that Detective Northrup should have known and told the warrant-issuing judge that the defendant was not the only person to have access to the photographs. But there is no information in the record as to why the South Portland police declined to investigate or take any action on the victim's complaint. Those additional circumstances do not amount to a substantial preliminary showing of an intentional false statement or omission by Northrup.

Moreover, there was abundant evidence to support a finding of probable cause, independent of this dispute over who else had access to the pictures. The victim dated the defendant, the defendant was previously convicted of stalking the victim, the victim obtained a protection from abuse order against the defendant and in February 2008 the defendant was convicted of violating that protective order. Later, men came to the victim's home saying that they

had met her on the Internet and were looking for sexual encounters. The victim found an ad on Craigslist that included pictures of her in lingerie that the defendant had taken and directions to her home. The victim changed her name and moved to Louisiana. Men whom the victim did not know again started to arrive at her new home, indicating that they had met her on the internet and were looking for sexual encounters. During this timeframe, sexually explicit video of the victim, taken with the defendant while they were dating, was posted on several adult pornography sites. These sites also listed the victim's names and her Louisiana address. In September 2009, a new Facebook account was created in the victim's name and included a photograph of her. The IP address that created that Facebook account was assigned to the defendant's neighbor, who had an unsecure wireless internet connection. Any misstatement about who had access to the photographs is not material to the finding of probable cause.

With respect to the videos, the defendant contends that Detective Northrup omitted the fact that sexually explicit video of the victim and the defendant were uploaded to the Internet before 2009, and that once on the Internet, those videos would be available to anyone for download and reposting. But the victim's complaint was significantly more comprehensive than simply reposting sexually explicit video. It was the context: postings on adult sites soliciting men for sexual encounters, providing the victim's new home address in Louisiana and including her new name after it was legally changed. In 2006 the defendant was convicted of stalking the victim and there was a protection from abuse order in place providing that the defendant not have contact with

or harass her. Protection from Abuse Order (ECF No. 101). Although the videos may have been available for others to repost, there is no evidence that anyone else was inclined to harass the victim. Stating that others could repost the video would not have negated a finding of probable cause.

The defendant asserts that Secret Service Agent Jeter, who participated in the November 5, 2009, search, stated in his report that the November 5, 2009, search and interview of the defendant was recorded. Def.'s Mot. to Suppress/Exclude Evidence at 19 n.11. The recording has not been made available to the defendant and the defendant was told that Detective Northrup does not have a recording of the search and interview. The defendant asserts that if the recording were available it would demonstrate that Detective Northrup knew on November 4, 2009, that videos of the victim were available on the Internet before the creation of the posting the victim complains about. The government does not respond to the failure to disclose the alleged recording. But even if Northrup knew of the earlier posting on the Internet, her failure to say so in her affidavit does not weaken the probable cause showing. As stated above, the harasser's conduct was more distinctive than simply reposting sexually explicit video.<sup>6</sup>

The defendant next asserts that Detective Northrup's statements that she was unsuccessful in finding contact information to send subpoenas to the adult sites where the video of the victim was posted are untruthful. The

---

<sup>6</sup> With respect to disclosure of the recording of the November 5 search and interview, the defendant has failed to establish that the government has the recording. Although the defendant asserts that the recording is mentioned in a report by Jeter, the Jeter report was not submitted in connection with this motion.

defendant hired a Certified Computer Forensics Examiner who was able to find contact information for the sites where the video was posted. Because the information was available, however, does not show that Detective Northrup's statement that she was unable to find the websites' contact information was untrue.

In her affidavit dated November 4, 2009, Detective Northrup stated that she received a response from Time Warner regarding the IP address used to create a Facebook page in the victim's name. The defendant points out that the formal response from Time Warner was dated November 23, 2009. Northrup Aff. ¶ 12 (ECF No. 78-1); Time Warner Response to Subpoena (ECF No. 67-6). The defendant asserts that there arises an inference that Detective Northrup's affidavit falsely stated that the IP address was from an Internet connection near the defendant's home. But Detective Northrup's declaration clarifies that she obtained an informal response from Time Warner while drafting the November 4, 2009, search warrant affidavit and she has now attached the informal responsive email from Time Warner. Decl. of Laurie Northrup ¶ 3 (ECF No. 82). Time Warner followed up with its formal response on to the subpoena on November 23, 2009.

The defendant complains that the information included in Detective Northrup's affidavit that an unsecure "Belkin 54G" wireless internet signal from a neighbor's home (the Cooks) was available in the defendant's driveway was misleading because it was not disclosed that a "Belkin 54G" is a commonly used brand of wireless router. Although Detective Northrup did not say that the unsecure wireless connection was a generic name, it is correct that the

Cooks had an unsecure “Belkin 54G” wireless connection. The defendant further points out that his house is 30 feet from the road and that it would be likely that the “Belkin 54G” wireless signal would not have been accessible from inside the defendant’s home. This omission is also not critical. Assuming the unsecure wireless signal was not available from inside the defendant’s home, there is no evidence that Detective Northrup knew the range. Moreover, the defendant could have accessed the signal from a laptop in his truck in the driveway, as law enforcement did from their vehicle. The inclusion of these omissions would not negate a finding of probable cause.

Detective Northrup’s affidavit states that neighbor Cook told her that he saw a computer in the defendant’s home and thought that it was in the defendant’s bedroom. According to the defendant’s private investigator, Cook denied to the investigator ever being in the defendant’s home, seeing a computer in the defendant’s home, or ever talking to the police. The investigator’s affidavit is hearsay as to the truth of what Cook told him, and there may be another explanation why Cook would say that to an investigator. The defendant has not asserted that Cook will testify under oath that he was never in the defendant’s home, never saw a computer in the defendant’s home, and never talked to the police about the defendant. Therefore, the defendant has not made a sufficient showing to support the need for a Franks hearing.

Most of the issues raised by the defendant are legitimate jury issues for the jury to consider in assessing whether or not the offender is guilty of the crime charged, but they do not meet the Franks standard for an evidentiary hearing on this warrant application.

***(ii) Taint***

The defendant contends that the information in the November 4, 2009, warrant application regarding the wireless signals in the driveway is tainted as a result of the unlawful accessing of the wireless signals. Because I found no Fourth Amendment violation when the police backed into the defendant's driveway and captured wireless signals, there is no taint.

***(iii) Nexus***

The defendant asserts that after excising the tainted evidence and false statements, including the material omissions, the November 4, 2009, warrant application does not satisfy the nexus element of probable cause. Because there is no tainted evidence, no false statements or material omissions, I find there to be sufficient nexus between the victim's complaints and the defendant's residence.

***(iv) Staleness***

The defendant says that the affidavit refers to stale information including an October 2008 Craigslist advertisement and a Facebook page created in August 2009 with logins on August 21 and September 26, 2009, from the Cook IP address. In addition, the defendant points out that the response from Time Warner does not state that the IP address in question was assigned to Cook in August when the fictitious Facebook account was created. Def.'s Mot. to Suppress/Exclude Evidence at 27.

In assessing a staleness claim, courts consider a variety of factors, including the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information.

United States v. Trinh, 665 F.3d 1, 13-14 (1st Cir. 2011). Here, the underlying facts point to the defendant repeatedly stalking and harassing the victim from 2006 to 2008. Given this pattern of activity, the creation of a Craigslist ad in October 2008 and a Facebook account in August 2009 are not too remote in time. This conclusion is supported by Northrup's affidavit, which noted that the defendant lived across the street from the Cooks on September 26, 2009, less than six weeks prior to the date of the warrant application, when the Cooks' IP address accessed the fictitious Facebook account. Moreover, the warrant at issue targeted the seizure of electronic equipment and the data contained in that equipment, information that would likely endure for a lengthy period of time. This evidence in the warrant application was not stale.

The defendant is correct that the response from Time Warner did not state that the IP address in question was assigned to Cook in August when the fictitious Facebook account was created. In fact, the subpoena did not request any information about any activity in August 2009. Because law enforcement did not request information about the IP address used to create the Facebook account, however, does not make stale the information they already had.

***(v) Particularity***

The defendant asserts that “[t]here is not a single allegation in the affidavit for search warrant that Defendant ever used his computer or the internet to do any of the acts prohibited by the [January 2009 protection from abuse] order” and that the warrant is a “fishing expedition for evidence of any misuse of Defendant’s computer.” Def.’s Mot. to Suppress/Exclude Evidence at 29. The defendant contends, therefore, that the November 4 warrant is

“overbroad and leaves too much to the discretion of the executing officers.” Id. at 28.

The November 4 warrant is based on the premise that the defendant violated the protection from abuse order issued in January 2009. There are allegations in Detective Northrup’s affidavit that the defendant used his computer or the Internet to engage in conduct prohibited by the protection order. The protection order prohibits the defendant from “threatening, assaulting, molesting, attacking, harassing or otherwise abusing” the victim. Protection from Abuse Order at 1 (ECF No. 101). The Northrup affidavit provides a factual basis to investigate the defendant for posting fictitious Internet advertisements and social networking profiles under the victim’s name that solicited sexual encounters with strangers, conduct being accomplished using computers and the Internet. That conduct certainly qualifies as “harassing” behavior in violation of the protective order. Thus, the warrant reasonably authorized a search for all computer records and data constituting evidence of the violation of the protection from abuse order.

***(b) December 29, 2009, Tracking Order Application***

Detective Northrup applied for, and received, a Tracking Order for the defendant’s pickup truck on December 29, 2009. Northrup Aff. (ECF No. 67-1); Order Authorizing the Installation and Use of an Electronic Tracking Device (ECF No. 67-1). The defendant requests a Franks hearing based on statements and omissions in Northrup’s application for the December 29, 2009, tracking order. But that GPS tracking device was never installed on the defendant’s vehicle. Therefore, it is not necessary for me to address the defendant’s

concerns about the affidavit submitted in support of the December 29, 2009, tracking order because no evidence was collected as a result of it. Moreover, I do not need to address the December 2009 tracking order separately because all of Detective Northrup's statements from the December 2009 application are repeated in the January 2010 tracking order application discussed below.

***(c) January 15, 2010, Tracking Order Application***<sup>7</sup>

The application for the January 15, 2010, tracking order to place a GPS device on the defendant's green 1999 Ford Ranger pick-up truck included the information used to support the November 4, 2009, warrant application and the following additional information, which I summarize from Northrup's affidavit. Aff. of Detective Laurie Northrup (Docket Item 67-2).

On November 5, 2009, Detective Northrup executed the search warrant on the defendant's house. In addition to several dozen old computer components, the search turned up two desktop computers, without hard drives, and a laptop case. The defendant explained that the laptop had gotten wet so he threw it away and the hard drives had been "hacked" and were unusable. The search also turned up a Nikon digital camera with a USB cable attached. During the search, the green 1999 Ford Ranger pick-up truck registered to the defendant was parked in the driveway.

---

<sup>7</sup> The parties agree that a tracking order is the functional equivalent of a warrant. I note that after the defendant filed this motion, the Supreme Court decided that use of a GPS tracking device to monitor a vehicle's movement constitutes a Fourth Amendment search. United States v. Jones, 132 S. Ct. 945, 949 (2012).

In November 2009 the victim moved back to Maine. In December 2009 the victim contacted Detective Northrup and reported that a new MySpace profile had been created in her name, which included her new name, her original given name, and her address, and linked to pornographic videos of the victim. The victim claimed that she did not create the profile. Detective Northrup obtained subscriber information and a connection log associated with the MySpace profile. She learned that the profile was created and accessed by numerous IP addresses all registered to users in Saco, Maine. When Detective Northrup visited each of the addresses, she determined that all had unsecure wireless networks that would allow someone parked near the location to access the internet through their unsecure wireless connection.

One of the unsecure wireless connections was owned by Pepperell Sweets Boutique in Saco, Maine. Saco House of Pizza, a restaurant located across the street from Pepperell Sweets, operated and controlled a surveillance camera that was directed at Pepperell Sweets. The owner of Saco House of Pizza gave Detective Northrup the video surveillance tape from December 12, 2009, the date when Pepperell Sweet's wireless had been used to access the MySpace profile of the victim. The video shows a small green pickup truck pulling into a parking space in front of Pepperell Sweets minutes before the connection was made to the MySpace

profile. The truck stayed parked for 21 minutes.<sup>8</sup> The truck in the video was later identified as having the same body style as a 1999 Ford Ranger.

On January 13, 2010, the victim reported that a man came to her home stating that he had corresponded with her after responding to her advertisement on Craigslist. The victim reportedly told the man that she had not communicated with him and asked the man to send the email correspondence to her at an email address that she provided him. The email correspondence indicates that the man is looking for a sexual encounter and the response provides directions to the victim's house. Detective Northrup's investigation revealed the Craigslist advertisement, which appears to be posted by the victim and states that she is looking to have sex with multiple men. The advertisement also provided the victim's address and directions to her home.

***(i) Franks Issues***

The January 15, 2010, tracking order was issued by a Maine District Court judge and the tracking device was installed on the defendant's vehicle on January 20, 2010. Northrup Aff. ¶¶ 37-38 (ECF No. 67-3). It is undisputed that both federal and state law enforcement was involved in the investigation. The defendant argues that any evidence that the tracking device revealed

---

<sup>8</sup> I have examined the video in connection with ruling on this motion. Given the lighting and the position of the truck in the video, I am not able to determine whether anyone got out of or into the truck while it was parked.

should be suppressed because the procedures used to obtain the Order did not comply with the provisions of Fed. R. Crim. P. 41 that governs warrants for tracking devices. (I deal separately with any constitutional issues.) Def.'s Mot. to Suppress/Exclude Evidence at 34. The First Circuit agrees with the Fifth Circuit in how to analyze cases where state warrants have been used to obtain evidence that will be used in federal court:

If . . . the warrant was issued under authority of state law then every requirement of Rule 41 is not a *sine qua non* to federal court use of the fruits of a search predicated on the warrant, even though federal officials participated in its procurement or execution. The products of a search conducted under the authority of a validly issued state warrant are lawfully obtained for federal prosecutorial purposes if that warrant satisfies constitutional requirements and does not contravene any Rule-embodied policy designed to protect the integrity of the federal courts or to govern the conduct of federal officers.

United States v. Mitro, 880 F.2d 1480, 1485 (1st Cir. 1989) (quoting United States v. Sellers, 483 F.2d 37, 43 (5th Cir. 1973)). Here, the application established probable cause for the tracking order, it was reviewed by a neutral judicial officer, and it was reasonable in scope and time, the most important issues of Rule-embodied policy.

The parts of Federal Rule 41 that were *not* satisfied by this state court tracking order do not “contravene any Rule-embodied policy designed to protect the integrity of the federal courts or to govern the conduct of federal officers.” Id. (The noncompliance issues the defendant lists are: signature by a state judge rather than a federal magistrate judge, Rule 41(b)(4); failure to designate the magistrate judge to whom the warrant must be returned, Rule 41(e)(2)(C); failure to limit the Order’s authorization to 45 days, Rule 41(e)(2)(C), instead

allowing 60 days; failure to specify daytime execution or to state good cause for nighttime execution, Rule 41(e)(2)(C); failure by the executing officer to enter on the warrant the exact date and time of the tracking device installation, Rule 41(f)(2)(A); failure to return the warrant to the designated magistrate judge within 10 days after use of the tracking device ended, Rule 41(f)(2)(B); and failure of the executing officer to serve a copy of the warrant on the person tracked after the tracking period ended, Rule 41(f)(2)(C)). Def.'s Mot. to Suppress/Exclude Evidence at 34-36). The defendant has not shown how any of those are policies integral to the integrity of the federal courts or the conduct of federal officers.

In his reply memorandum, the defendant lays out what he says is the extensive involvement of federal agents in the investigation and the U.S. Attorney's office indications of interest in a federal prosecution.<sup>9</sup> Def.'s Reply to Gov't Opp'n to Mot. to Suppress at 2-5 (ECF No. 83). That does not change my analysis. A Maine State Police detective obtained the tracking order from a Maine District Court judge following state procedures. There is no suggestion of bad faith or that somehow an unfair advantage was obtained as a result. Moreover, the defendant does not assert that the Maine Rules of Criminal Procedure were not followed in the issuance and execution of the tracking order.

---

<sup>9</sup> The defendant argues that the U.S. Attorney's office demonstrated interest starting in January 2009. Def.'s Reply to Gov't's Opp'n to Mot. to Suppress at 5. That appears to be in error, caused by some January 2010 entries by the agent that mistakenly used the year 2009. The record shows that the investigation did not begin until September 2009 when Maine's Attorney General referred a complaint to the Maine Computer Crimes Task Force, including a Secret Service Agent who was then assigned to that Task Force.

The defendant complains that the preamble to Detective Northrup's affidavit listed the victim as living in Louisiana when in fact she had moved back to Maine more than a month before the tracking order application. Def.'s Mot. to Suppress/Exclude Evidence at 36. In context, it is clear from Northrup's affidavit that she is recounting the events as they occurred and some of the events occurred while the victim was living in Louisiana. Even if I were to consider the reference in the preamble as a false statement, the statement is not necessary for a finding of probable cause to believe that the defendant committed or is committing stalking, criminal invasion of computer privacy, harassment or the violation of a protective order as the affidavit alleges. Order authorizing the Installation and Use of an Electronic Tracking Device at 1 (ECF No. 67-2) (the defendant "committed or is committing violation of Title 17-A M.R.S., Sections 210-A, 432, 506-A and 506-B").

The defendant asserts that Northrup's affidavit falsely states that during the November 5 search the officers found "dozens of old computer components" in the residence. The defendant points out that neither the inventory of the search nor the photos taken during the search demonstrate the presence of old computer parts. Inventory of November 5, 2009 Search (ECF No. 67). I note that the absence of photos of the computer parts and the failure to list each of those parts on the inventory does not support the conclusion that Northrup made a false statement. It is customary to inventory only items that are seized during a search. Because those parts were not seized, they were never inventoried. At the suppression hearing, Lang corroborated the presence of "a

lot” of old computer parts at the defendant’s home. I find no evidence to support the assertion that Northrup’s statement was false.

The defendant also challenges Northrup’s statement that “hard drives would be one of the components people are least likely to throw away.” Northrup Aff. ¶ 19 (ECF No. 67-1). According to the defendant this statement is misleading because “Northrup knows that a hard drive is useless if it is damaged beyond repair by either water, impact, viruses, result of harmful hacking or any of many other causes.” Def.’s Mot. to Suppress/Exclude Evidence at 36. These two statements are not mutually exclusive. The hard drive is the part of the computer that stores data. As such, it is particularly valuable and unlikely to be discarded. In using the phrase “least likely”, it is reasonable to understand Northrup to mean that the computer owner would generally maintain the hard drive unless it became inoperable for one of the reasons the defendant supplies. There is nothing misleading about Northrup’s statement.

Finally, the defendant complains that the inclusion of email correspondence in response to a fictitious Craigslist advertisement that appears to be posted by the victim is misleading because there is no tie between it and the defendant. But Northrup does not claim that she has connected the defendant and the advertisement. It was properly included in the affidavit because of the similarity of the Craigslist advertisement to the other fictitious Internet postings about the victim.

***(ii) Taint***

Because I find that the wireless survey and the November 5, 2009, search were lawful, the defendant's argument that including this evidence tainted the affidavit is unavailing.

***(iii) Nexus***

The defendant contends that Northrup's January 15, 2010, affidavit does not demonstrate adequate evidence to support either the "commission" element, or the nexus element of the probable cause analysis. Again because nothing needs to be removed from the affidavit, I find that there is sufficient nexus between the criminal conduct and the defendant's vehicle.

The defendant asserts that the evidence of a green pickup truck parked near Pepperell Sweets on December 12, 2009, is too remote in time from the January 15, 2010, affidavit to support a finding of probable cause. The January 15 tracking order application contained ample evidence of the defendant's recent use of his vehicle to commit the criminal activity being investigated. In December 2009, the victim contacted Detective Northrup and reported that a new MySpace profile had been created in her name. Detective Northrup obtained a connection log associated with the MySpace profile and learned that the profile was created and accessed by numerous IP addresses all registered to users in Saco, Maine that had unsecure wireless networks, including Pepperell Sweets' unsecure wireless. The video surveillance tape from December 12, 2009, shows a small green pickup truck pulling into a parking space in front of Pepperell Sweets minutes before the connection was made to the victim's fictitious MySpace profile. The truck stayed parked for 21

minutes. On January 13, 2010, the victim reported that a man came to her home stating that he had corresponded with her after responding to her advertisement on Craigslist. The email correspondence indicates that the man is looking for a sexual encounter and the response provides directions to the victim's house. Given the presence of a truck similar to the defendant's, parked in the vicinity of Pepperell Sweets when the MySpace account was created, and the ongoing nature of the stalking, the December 12 facts were not too remote in time. Trinh, 665 F.3d at 13-14.

***(d) July 1, 2010, Warrant Application***<sup>10</sup>

The application for the July 1, 2010, warrant to search the defendant's home included the information used to support the November 4, 2009, warrant application, the January 15, 2010, tracking order and the following additional information, which I summarize from Northrup's affidavit. Aff. of Detective Laurie Northrup (ECF No. 67-3).

On January 20, 2010, a GPS tracking device was installed on the defendant's vehicle. Over the next week, the defendant's pickup truck was detected driving and stopping for periods of time in areas corresponding to the IP addresses that accessed the fraudulent MySpace account for the victim. In addition, the defendant's vehicle was parked near Pepperell Sweets for over one hour. On January 23, 2010, the defendant's vehicle was parked in

---

<sup>10</sup> The defendant reasserts the arguments he has previously made in the November 4, 2009, and January 15, 2010, warrant applications. For the reasons already discussed, these arguments are rejected.

Pepperell Square and the man in the vehicle was working on a laptop. The GPS tracker last detected movement of the defendant's vehicle on January 23 and thereafter it stopped operating. In February 2010, the defendant found the GPS tracking device on his vehicle and turned it over to the local police department.

In March, 2010, two new MySpace profiles were created under the victim's name. The profiles invited men to have sex with the victim, posted sexually explicit videos made of the victim by the defendant when they were dating and provided the victim's address. The IP addresses of these MySpace profiles were Pepperell Square. Thereafter, the victim notified Detective Northrup that male strangers were showing up at her home and workplace with increasing frequency.

In early April 2010, with the permission of the Cooks, the individuals who lived across the street from the defendant, a small camera was installed in the Cooks' yard and pointed at the defendant's residence. On the evening of April 2, 2010, a new Facebook account in the victim's name was created. At that time the camera was not being monitored. In May 2010, the Cooks asked that the camera be removed. In June 2010, another Facebook account was created in the victim's name. Pornographic pictures and videos were posted on that Facebook site. In addition, the posting solicited men for sex and gave the victim's address and vehicle information.

In late June 2010, the victim advised that up to six men a night show up at her apartment and knock on the windows as directed on the Facebook site. In addition, the victim found a note on her car when leaving work that was sexually graphic. Thereafter, Detective Northrup received subpoena results from Yahoo! for an email address that was listed when one of the fraudulent Facebook pages of the victim was created. From this data it was determined that on three separate dates, IP addresses used to access the email address that was used to create the fraudulent Facebook page of the victim matched the IP address used to access the defendant's MySpace account.

Also in June, Northrup received results from subpoenas sent to MySpace for the defendant's account and Yahoo! for an email address that was used to create a fictitious Facebook profile of the victim. Three separate IP addresses were used to access both the defendant's MySpace account and the victim's fictitious email account. One of these IP addresses was designated to Stacey Sylvain at 22 Marion Avenue, Biddeford, a neighbor living across the street from the defendant.

***(i) Franks Issues***

The defendant contends that when providing information about obtaining and viewing the surveillance tapes for January 22, 2010, Northrup's affidavit failed to state that there are many other businesses in the Pepperell Square area. By omitting that piece of information, the defendant asserts, Northrup

prevented a reasonable inference that the defendant may have been shopping or dining, legitimate activities, when he was parked in the Pepperell Square area.<sup>11</sup>

Northrup's affidavit includes three pieces of evidence in the paragraphs that the defendant indicates are missing evidence: (1) the fictitious MySpace postings were made from the Pepperell Square area in December 2009, (2) the defendant's vehicle was observed (via the tracking device) being parked in the Pepperell Square area for over one hour on January 22, 2010, and (3) a witness saw a man sitting in the defendant's parked vehicle typing on a laptop in Pepperell Square on January 23, 2010. Northrup Aff. ¶¶ 39-41 (ECF No. 67-3). The affidavit does not preclude the possibility that the individual who parked the defendant's vehicle in Pepperell Square for approximately one hour on January 22 left the vehicle for some period of time. In fact, it is clear from

---

<sup>11</sup> It is unclear from the defendant's brief what other information he claims is "missing" from Northrup's affidavit. The defendant's brief states the following:

Paragraphs 40-41, of the July 1, 2010 Affidavit include a statement that Secret Service Agent Jeter called the owner of Saco House of Pizza to request a copy of his surveillance tapes for January 22, 2010; and that Agent Jeter went to the Saco House of Pizza to retrieve the tapes. Further, Paragraphs [sic] 40 includes the statement that the owner, Marc Hill, reported to Agent Jeter that he saw a truck meeting the description of the Defendant's vehicle, including his license plate number, and he observed a man inside the truck typing on a laptop.

In Paragraphs 39-41, Detective Northrup offers that on January 22, 2011 "The vehicle was observed parked at Pepperell Square for over an hour." At hearing the Defendant expects testimony that there are numerous shops and restaurants in Pepperell Square. Quatrano Affidavit, Paragraph 14. Absent any evidence to the contrary, it is just as likely as anything else that the Defendant was having a meal or shopping.

Def.'s Mot. to Suppress/Exclude Evidence at 41. Other than the failure to include information about Pepperell Square as a shopping area, I do not know what other information the defendant believes should have been included in Northrup's affidavit.

Northrup's affidavit that Pepperell Square has a number of businesses, including a restaurant. Northrup Aff. ¶¶ 28-29 (ECF No. 67-3). Omitting information that the defendant could have been parked in Pepperell Square and dining nearby does not dilute any one of the three pieces of evidence or the overall probable cause established by Northrup's affidavit.

The defendant also asserts that "the evidence offered by Detective Northrup should not be credited in the probable cause analysis" because the January 2010 surveillance tapes are not available and the December 2009 surveillance tape is not of adequate quality to read the license plate on the "green pickup" or determine whether anyone exits the vehicle while it is parked. Def.'s Mot. to Suppress/Exclude Evidence at 42. Northrup's affidavit states:

The video shows a small green pickup truck pulling into a parking space in front of PEPPERELL SWEETS at 7: 14 p.m. Eastern Time. This would be four minutes before the connection to the MySpace profile was created on the 12th of December, 2009. The truck appears to look very much like Shawn Sayer's truck. The vehicle is parked in front of PEPPERELL SWEETS for 21 minutes and no one is seen getting out of the truck before it leaves the area.

On December 2, 2009, Chris Hull showed a copy of the photographs above to Otis Soohey who is the General Manager of the Darling's Ford in Bangor. Mr. Soohey stated that the truck in the pictures is a Ford Ranger and has the same body style as was used in the 1999 Ford Rangers.

Northrup Aff. ¶¶ 29-30 (ECF No. 67-3).

I watched the video and agree that the video is of poor quality. Def.'s Ex. 12 admitted at May 4, 2012 Hearing (ECF No. 107). Because the video is dimly lit and the resolution is not sharp enough to make out details, I could not

determine whether anyone got out of the vehicle during the 21 minutes it was parked at Pepperell Square. But omitting the statement that “no one is seen getting out of the truck” does not undermine the finding of probable cause to issue the July 1, 2010 search warrant.

The defendant asks that paragraphs 17 through 21—related to the November 5, 2009, search and seizure of materials at the defendant’s home—be excised from Northrup’s July 1, 2010, affidavit. Specifically, the defendant asserts that at the time of the July 1 search warrant application, law enforcement believed that the items seized on November 5, 2009, contained no incriminating evidence and, if that fact has been included, it would have impacted the probable cause analysis. Def.’s Mot. to Suppress/Exclude Evidence at 43. But it is clear from Northrup’s affidavit that nothing of evidentiary value was found in the items seized on November 5, 2009. In fact, Northrup explains that she believes that no incriminating evidence was found at the defendant’s home because he became aware of the investigation. Northrup Aff. ¶ 20 (ECF No. 67-3). Even if Northrup had explicitly stated in the affidavit that no evidence was found in the seized materials, there was still a substantial basis for concluding that probable cause existed.

Northrup’s affidavit recounts further that subpoenas were sent to Craigslist and Fairpoint Communications for subscriber information on the IP address captured at the time a Craigslist advertisement was posted on January 10, 2010. Northrup Aff. ¶ 37 (Docket Item 67-3). In her affidavit, Northrup inserted a copy of the actual response to the Craigslist subpoena that provides the IP address as 70.105.255.31. Although she states that the

Attorney General's office sent a subpoena to Fairpoint Communications to get the subscriber information for that IP address,<sup>12</sup> Northrup never offers any information about the location of the subscriber's IP address who posted the Craigslist advertisement. What the defendant asserts is missing is that the IP address that posted the Craigslist advertisement was not in the Biddeford/Saco area and that law enforcement was unable to draw any connection between that IP address and the defendant. But the defendant gives me no basis to conclude that Northrup knew this was so when she filed her affidavit. Moreover, in light of all the evidence in Northrup's affidavit linking the defendant with creating and accessing Internet accounts related to the victim, the disclosure of additional IP addresses with no obvious connection to the defendant does not impact probable cause.

The defendant also asserts that Northrup's affidavit intentionally omitted the fact that a Facebook and a MySpace account created on December 14, 2009 and December 26, 2009, respectively, were not linked to the defendant. Def.'s Mot. to Suppress/Exclude Evidence at 43. The defendant maintains that the creation of these accounts is associated with IP addresses in other southern Maine towns. Id. at 44, n.15. The crime being investigated in this case involves use of numerous unsecure wireless connections to post fictitious Internet advertisements and social media profiles related to the victim. Thus, even if Northrup's affidavit had identified the origin of the IP addresses that created the December 2009 Facebook and MySpace accounts as located in

---

<sup>12</sup> The defendant obliquely challenges whether the subpoena was sent. Def.'s Mot. to Suppress/Exclude Evidence at 43, n.14.

other nearby southern Maine towns, there would still be sufficient probable cause to support the issuance of the July search warrant.

The defendant contends that Northrup's affidavit falsely states that over the course of a week the defendant was stopping in areas where there were IP addresses that correspond to previous Internet logins under investigation. According to the defendant this statement is false because the tracking logs demonstrate that the defendant was tracked for less than 24 hours during that week and the defendant was not parked at one location for over one hour. Def.'s Mot. to Suppress/Exclude Evidence at 44.

Neither party has put the tracking logs in the record. Based on the arguments presented by the parties, Northrup's descriptions of the data obtained by the tracking device installed on January 20, 2010, are not materially false. The total time that the defendant's vehicle was tracked during a one week period of time does not undermine the fact that the defendant's vehicle stopped in places that correspond to IP addresses of locations where previous Internet postings related to the victim were accessed. With respect to the statement that the defendant's vehicle was "parked at Pepperell Square for over one hour," Northrup Aff. ¶ 39 (ECF No. 67-3), the government admits that the tracking logs indicate that the defendant's vehicle was parked for 44 minutes on January 22 and 45 minutes on January 23. Although on both instances the time is short of one hour, I do not find the difference to be material.

***(ii) Taint***

Because I find that the initial wireless survey, the November 5, 2009, search, and the January tracking order were lawful, the defendant's argument that including this evidence tainted the affidavit is unavailing.

***(iii) Nexus***

With respect to the nexus between the information in the July 1, 2010, search warrant application and his residence, the defendant asserts that it is insufficient. Specifically, the defendant asserts that the MySpace profiles created on March 7, 2010, and March 20, 2010, are unconnected to him or his residence. The defendant also asserts that there is no link between him and an IP address assigned to Stacey Sylvain, a neighbor located across the street from the defendant's home. Both of these pieces of information are reasonably linked to the defendant. First, the IP address for the MySpace profiles created on March 7, 2010, and March 20, 2010, was designated to the Pepperell Square area, a location that had previously been linked to the defendant and fictitious postings about the victim. With respect to the IP address designated to Stacey Sylvain, the defendant's neighbor across the street, there is a distinct connection with the defendant. That is, not only did someone using the Sylvain IP address access the victim's fake Facebook account but that same IP address was used to access the defendant's own MySpace account.

The defendant finally asserts that there is inadequate information in the July 1, 2010, warrant application to justify a "no knock and announce" warrant. Def.'s Mot. to Suppress/Exclude Evidence at 46. I disagree. Northrup indicated that based on the absence of the two hard drives and the

laptop when they searched the defendant's home on November 5, she believed that the defendant had already removed and hidden the hard drives from his computers. A no-knock warrant was properly issued. To support a no-knock entry into a home, "the police must have a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be dangerous or futile, or that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence." Richards v. Wisconsin, 520 U.S. 385, 394 (1997). Given the facts of this case, it was reasonable to conclude that if law enforcement were required to knock and announce their presence when executing the second warrant, the defendant would have time to tamper with the evidence.

***(e) September 27, 2010, Warrant Application***

During the July 1, 2010, search of the defendant's home law enforcement found a Gateway desktop and an Acer laptop computer. Examination of the Acer laptop computer seized from the defendant's home identified 49 Yahoo! profiles and accounts that had been created on the defendant's laptop that are associated with the victim.<sup>13</sup> Later, an application was made for the September 27, 2010, warrant to obtain the disclosure of the contents of all emails or other data and account information associated with the 49 Yahoo! profiles and accounts.<sup>14</sup> It included all the information contained

---

<sup>13</sup> Only two of these accounts are actual email addresses belonging to the victim.

<sup>14</sup> I note that at oral argument the defendant stated that he had standing to challenge the search of two of the 49 Yahoo! profiles. In any event, it does not matter to which email addresses the defendant believes his September 2010 search warrant challenges apply: his arguments are generic and, therefore, apply to all of the Yahoo! profiles and accounts.

in the earlier warrant requests, Northrup Aff. (ECF No. 67-4), as well as the laptop information.

***(i) Franks Issues***

The defendant reasserts all the arguments that he made with respect to the other three search warrants and tracking order. For the reasons I have already laid out, I find that there are no material false statements or omissions in the statements included in earlier search warrant and tracking order applications.

For the September 27, 2010, warrant, Northrup's affidavit explained an IP address as follows:

An internet protocol (IP) address is a numeric code used to uniquely identify each computer or wireless router connected to the Internet at a particular time, and which typically remains assigned to that computer or router for the duration of the internet connection. No two connections will have the same IP address at the same time. IP addresses are assigned in blocks to Internet service providers, who in turn assign the IP addresses to their customers. Internet service providers typically keep records of what subscriber was assigned to what IP address at what time.

Northrup Aff. at 4 n.1 (ECF No. 67-4). The defendant contends that although Northrup's explanation of an IP address is "technically correct" it is "functionally false and misleading" because she fails to distinguish between "public" and "private" IP addresses. Def.'s Mot. to Suppress/Exclude Evidence at 48. The defendant explains that "more than one computer can, and will, have the same 'public' IP address at the same time when a consumer grade router is used." *Id.* I do not find Northrup's description of an IP address misleading. Although if two computers are using the same wireless router at

the same time, both computers will register as having the same public IP address, omission of that clarification does not affect the probable cause for the warrant.

The defendant also asserts that Northrup omitted the fact that one of the videos of the victim was posted on a pornographic website on August 22, 2010, a date on which Northrup knew that the defendant was in York County Jail. Perhaps a jury will find this significant in deciding whether the government can establish this defendant's guilt beyond a reasonable doubt, but it does not detract from the abundant probable cause already established.

The defendant next asserts that Northrup's affidavit mischaracterizes the October 2008 incident during which men showed up at the victim's house looking for a sexual encounter. Northrup's affidavit states that "[s]everal more male strangers came to [the victim's] residence seeking sexual encounters in the following days." Northrup Aff. ¶ 8 (ECF No. 67-4). The defendant points out that the victim's letter to the Maine Attorney General describes the October 2008 events as occurring on a single night. To the extent that there is a discrepancy, it is immaterial and removal of the statement that the incidents took place over the course of multiple days does not result in a lack of probable cause.

The defendant claims that Northrup should have notified the warrant-issuing court that the forensic examination of the laptop seized from the defendant's home in July 2010 did not reveal any evidence that the laptop was used to access various MySpace accounts—specifically, that there was no evidence that the laptop was used to (1) access a MySpace account on

December 12, 2009, when the defendant's truck was parked at Pepperell Square or (2) create MySpace accounts on March 7 and March 15, 2010. The preliminary forensic examination of the laptop identified a large number of Yahoo! profiles that had been created on the laptop. When Northrup applied for the Yahoo! search warrant in September 2010, she included the information that was identified by this preliminary examination of the laptop. When the forensic examination of the laptop was complete in April 2011, it revealed that the laptop contained no connection to those MySpace accounts and that there was no internet history on it after October 2009. Forensic Synopsis (ECF No. 101-1). But the defendant gives me no basis to conclude that Northrup knew this when she filed her affidavit in September 2010.

The defendant states that Northrup's discussion of the IP addresses that were used to access the defendant's MySpace account and an email associated with one of the victim's fictitious MySpace accounts is misleading. Def.'s Mot. to Suppress/Exclude Evidence at 50. Northrup's description of the link between the IP addresses, the defendant contends, is not supported by the IP address logs. Although the record does not contain the logs that the defendant relies on, I do not agree with the defendant's characterization of Northrup's affidavit.

Northrup's affidavit states:

In early June of 2010, I received records from MySpace related to the connection logs for Sayer's personal MySpace profile. In late June of 2010, I also received records provided to me by Yahoo! which suggested that the email address listed as a contact address for [the victim's] Facebook profile #1 was luvmarriedmen29@yahoo.com. I compared the MySpace connection logs for Sayer's personal

profile with the Yahoo! connection logs for `luvmarriedmen29@yahoo.com`. The majority of the IP addresses shown connecting to the `luvmarriedmen29@yahoo.com` address were spoofed. However, on three separate dates, the same IP address was used to access both `luvmarriedmen29@yahoo.com` and Sayer's MySpace profile. One such example is IP address 74.75.62.40, which was used to access `luvmarriedmen29@yahoo.com` on March 26, 2010 and was used almost continually on Sayer's MySpace account throughout the month of March of 2010. According to records provided to me by Time Warner Cable, the subscriber associated with IP address 74.75.62.40 is a woman who lives across the street from Sayer's residence on Marion Avenue in Biddeford.

Northrup Aff. ¶ 28 (ECF No. 67-4). The affidavit does not state that the defendant's MySpace account and the email associated with a fictitious MySpace account were accessed at or near the same time using the same IP address. Given the crime being investigated in this case, it is enough that the same IP address accessed both accounts on different dates and that the IP address is associated with the defendant's neighbor.

Also with respect to the `luvmarriedmen29@yahoo.com` email address to which the Northrup affidavit refers, the defendant asserts that his expert found that from March 26, 2010, through June 23, 2010, an IP address from Amsterdam, Netherlands logged onto that email account. Fahey Aff. ¶¶ 31-32 (ECF No. 67-9). This is not inconsistent with the Northrup affidavit statement that the majority of the IP addresses connecting to the Yahoo! email were "spoofed," which according to Northrup means that someone had disguised the IP address through the use of a proxy server. Northrup Aff. at 13 n.4 (ECF No. 67-4). There is no indication that Northrup knew and covered up that the IP address actually was located in Amsterdam. In any event, the inclusion of a

specific statement that the many of the IP addresses connected to that Yahoo! email address were from Amsterdam does not undermine the already strong showing of probable cause for the September 2010 warrant.

Finally, the defendant takes issue with Northrup's statement that the email accounts found on the defendant's computer were associated with the victim. Def.'s Mot. to Suppress/Exclude Evidence at 51. He points to two, out of the forty-nine, addresses found on the laptop. Even if these two accounts were in fact not associated with the victim, this would have no bearing on the existence of probable cause, given the number of email accounts found on the laptop computer that were plainly associated with the victim.

***(ii) Taint***

Because no evidence was obtained in violation of the defendant's rights, no tainted evidence needs to be removed from Northrup's September 27, 2010 search warrant application.

**CONCLUSION**

For all these reasons, the defendant's motion to suppress/exclude evidence is **DENIED**. I decline to hold a Franks hearing because the defendant has failed to make the necessary "substantial preliminary showing that the affidavit includes a false statement which was made either knowingly or intentionally or with reckless disregard for the truth, and that this misstatement was necessary to the finding of probable cause." Nelson-

Rodriguez, 319 F.3d at 34.<sup>15</sup> Northrup's affidavits contain no deliberately or recklessly false statements or omissions material to finding probable cause.

**SO ORDERED.**

**DATED THIS 13<sup>TH</sup> DAY OF JUNE, 2012**

/s/D. BROCK HORNBY  
**D. BROCK HORNBY**  
**UNITED STATES DISTRICT JUDGE**

---

<sup>15</sup> The defendant offered no direct evidence of Northrup's state of mind or inferential evidence that she had obvious reasons for omitting facts in order to prove deliberate falsehood or reckless disregard. United States v. Silva, 554 F.3d 13, 19 n.7 (1st Cir. 2009) (citing Franks, 438 U.S. at 165).

**U.S. DISTRICT COURT  
DISTRICT OF MAINE (PORTLAND)  
CRIMINAL DOCKET No. 2:11CR113 (DBH)**

**United States of America**

Represented by Craig M. Wolff  
Darcie N. McElwee  
Assistant United States Attorneys  
District of Maine  
100 Middle Street Plaza  
Portland, ME 04101  
(207) 780-3257  
email: [craig.wolff@usdoj.gov](mailto:craig.wolff@usdoj.gov)  
[darcie.mcelwee@usdoj.gov](mailto:darcie.mcelwee@usdoj.gov)

v.

**Shawn Sayer,  
Defendant**

Represented By Peter E. Rodway  
Rodway & Horodyski  
30 City Center  
Portland, ME 04104  
(207) 773-8449  
email: [rodlaw@maine.rr.com](mailto:rodlaw@maine.rr.com)