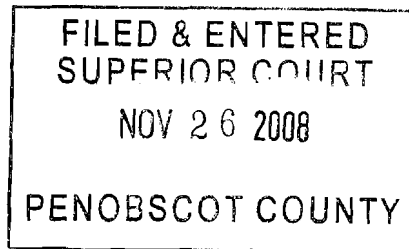


STATE OF MAINE
PENOBSCOT, ss.



SUPERIOR COURT
CRIMINAL ACTION
DOCKET NO. CR-08-229/
WRA - PEN - 116600*

THE STATE OF MAINE,

v.

ORDER

JACK D. BAILEY, II,

Defendant.

This matter is before the Court on a motion to suppress pursuant to M.R. Crim. P. 41A. Defendant argues that the warrantless search of his residence, including his computer, on February 1, 2008 was unlawful. The State argues that Defendant consented to the search. The Court held a hearing on this matter on August 29, 2008.

BACKGROUND

The Bangor Police Department executed a search warrant at a Bangor residence having obtained information from Wyoming law enforcement agents that electronic files containing child pornography were being shared through an IP address being used at that particular physical address. The files were being made available through a peer-to-peer file-sharing client called Limewire. Upon execution of the search warrant, the police discovered that the IP address through which the files were being shared was associated with an unsecured wireless router without password protection that was located at the searched residence. The IP address was not associated with any computer located at the residence searched pursuant to the warrant. Therefore, the person sharing the files through that IP address could have been anyone accessing the internet through that wireless router. More succinctly, the person that the police were searching for was

someone in the neighborhood who was “poaching” an internet signal through this unsecured wireless router.

During the execution of the search warrant, Det. Brent Beaulieu turned off the wireless router. On February 1, 2008, Det. Beaulieu began going from door to door in the surrounding area. After knocking on other doors, the detective knocked on Defendant’s door. When Defendant answered the door the detective asked if he could talk to Defendant whereupon Defendant ushered him into the entryway. A recording of the conversation reveals the following dialogue between Det. Beaulieu and Defendant in the entryway.

Det. Beaulieu: Do you have a computer here sir?
Defendant: Pardon me.
Det. Beaulieu: Do you have a computer here?
Defendant: Yes.
Det. Beaulieu: Reason I ask, what I’m doing is I’m checking the neighborhood, there’s been a problem in the neighborhood with people gaining access to someone else’s computer and I just want to make sure that you don’t have the same issue.
Defendant: Uh, no?
Det. Beaulieu: What kind of computer do you have?
Defendant: Uh, it’s a, uh, e-machine.
Det. Beaulieu: E-machine, laptops or tower or?
Defendant: No, I had a laptop and, uh, got rid of that and I’ve got a, uh, tower.
Det. Beaulieu: Can I look at it real quick just to make sure this, you don’t have the same issue?
Det. Beaulieu: Where’d your, where’d your laptop, what did ya do with it, did ya sell it, er?
Defendant: Yeah.

Defendant led the detective to his computer and the following conversation took place while the detective was seated at the computer and Defendant was standing behind him observing what was happening.¹

¹ Defendant has argued in the present motion that because he did not verbally consent to the search of his computer that no consent was given. This argument is wholly without merit in that a person can voluntarily

Det. Beaulieu: She gonna wake up on her own, er? Ah, got to hit the right switch. Do you live here alone?

Defendant: Uh, about two years?

Det. Beaulieu: Ah. I'm just gonna finish this up, just gonna search for a file.

Defendant: What are you looking for?

Det. Beaulieu: I'm looking for a file that, that, that, uh, may indicate that you've had an issue here.

Defendant: What kind of issue?

Det. Beaulieu: To, to see if anybody's accessed this computer. Oh, let's see, it takes about, well, probably two minutes.

Defendant: They've accessed this computer?

Det. Beaulieu: Well, I'm searching. Do you have wireless here at all?

Defendant: Um, I've got wireless, yeah.

Det. Beaulieu: Okay. Where, do ya, which service do you get it from?

Defendant: Um, service?

Det. Beaulieu: Yeah, um, I mean how do ya, uh, do you just pick up the wireless?

Defendant: Yeah, its just been, um, its just been, there's been wireless.

Det. Beaulieu: Okay.

Defendant: [inaudible] just been pick that up.

Det. Beaulieu: Now, you've lived hear two years, you said?

Defendant: Yeah.

Det. Beaulieu: How long those people down back lived here?

Defendant: Uh, about the same.

Det. Beaulieu: What's your name sir, I just gotta write you down?

Defendant: Jack Bailey.

Det. Beaulieu: Jack Bailey. What's your date of birth Jack?

Defendant: One, nine, sixty-two.

Det. Beaulieu: You got Limewire. How long have you had Limewire?

Defendant: Well, quite a while.

Det. Beaulieu: You have any issues with it at all?

Defendant: No.

Det. Beaulieu: Have you had to uninstall it or reinstall it at all?

Defendant: What do you mean?

Det. Beaulieu: Did you ever have to take it out and put it back in, er, whatever you had to do?

Defendant: Yeah.

Det. Beaulieu: How long ago did you have to do that?

Defendant: I don't know.

consent to a search through nonverbal conduct. *State v. Fredette*, 411 A.2d 65, 68 (Me. 1979) (consent may be given by "word or gesture"). Det. Beaulieu testified at the hearing that, after asking if he could take a look at Defendant's computer, Defendant showed him to the computer and even manipulated the key board for the detective in order to illuminate the screen. The sequence of the audio recording is entirely consistent with this testimony.

Det. Beaulieu: What, uh, I probably asked you that, I didn't write it down when I was talking to you. What's your, uh, address here Jack?
Defendant: 101.
Det. Beaulieu: Yep.
Defendant: Thomas Hill Road.
Det. Beaulieu: And a phone number?
Defendant: None.
Det. Beaulieu: No phone, you don't have a cell or anything?
Defendant: No.
Det. Beaulieu: Who are the people who live down back?
Defendant: I don't know.
Det. Beaulieu: Now, when did your wireless stop working or is it still working, er?
Defendant: No, uh, it stopped a couple days ago.
Det. Beaulieu: A couple days ago.

Throughout this conversation, Defendant continued to stand behind the detective observing what operations the detective was carrying out on the computer. In fact the detective was looking for a globally unique identifier ("GUID") number associated with Limewire in order to match it with the number provided by Wyoming agents. It was obvious that Limewire had been installed on the computer because an icon appeared on the computer's desktop; however, the GUID number did not match the number for which the detective was looking. This led to the detective's question concerning reinstallation, which could account for a different number. After this conversation, the detective searched various files on the computer and uncovered thumbnails of audio-visual files that appeared to depict child pornography. The interaction between the two continued as follows.

Det. Beaulieu: Do you know why I'm here Jack?
Defendant: I have a feeling.
Det. Beaulieu: Want to talk about it?
Defendant: [Inaudible]
Det. Beaulieu: You've got some videos on there you shouldn't have, right? How long have you had those on there?
Defendant: Since I've had Limewire, I guess.

Det. Beaulieu: About a year?
Defendant: Yeah.

After this dialogue, the detective asked Defendant questions about his use of child pornography. During this time Defendant revealed key words that he had used to search for videos, including the word “preteen.” He indicated that he believed that he had a “couple hundred” illegal videos on his computer. He told the detective that although he had once made a disk to backup some of his files that he had thrown it out.

The detective informed Defendant that he would need to take the computer and asked him if he would consent to its search. Defendant agreed at which time the detective made a phone call to request that another officer bring him a consent-to-search form. While waiting for another officer to bring the form, the detective continued to talk with Defendant. Defendant indicated that, in addition to videos, he had also obtained illegal pictures through Limewire as well. Defendant denied ever having attempted to view children in person or ever having taken any of his own pictures or videos. He also indicated that he preferred images of children around ten years of age.

When another officer arrived with a consent-to-search form, Defendant signed the form and consented to the search of his computer and his apartment. The officers conducted a brief search of his apartment, seized his computer, and left. Defendant was not arrested at that time.

DISCUSSION

In his motion to suppress, Defendant asserts that he did not give valid consent for Det. Beaulieu to search his computer because his consent was the product of trickery or deceit. He argues that his subsequent consent to the search of the computer and his

apartment were also invalid, having been tainted by the initial illegal search of the computer.

When a search is conducted without a warrant, suppression of the fruits of the search is required unless it was pursuant to an exception to the warrant requirement. *State v. McLain*, 367 A.2d 213, 216 (Me. 1976). “[A] search conducted pursuant to a valid consent is constitutionally permissible and is an established exception to the requirements of both a warrant and probable cause mandated by the Fourth and Fourteenth Amendments. *State v. Koucoules*, 343 A.2d 860, 866 (Me. 1974) (citing *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973)). The voluntariness of consent authorizing a search is a question of fact and, in the context of a motion to suppress, the State has the burden of establishing the legality of the search by a preponderance of the evidence. *State v. Fredette*, 411 A.2d 65, 68 (Me. 1979); *Koucoules*, 343 A.2d at 866. Voluntariness is determined by “analyzing all the circumstances of an individual consent.” *Schneckloth*, 412 U.S. at 233.

Defendant contends that the detective misrepresented the purpose of his search and that his consent was the product of this deceit or trickery. He argues that because his consent was the product of such deceit that it was not voluntary. Pursuant to *Schneckloth* a court must look at the entire situation surrounding an individual consent; therefore, determining whether “a police ruse amounts to a deception that undermines the validity of a consent...must be decided on a case-by-case basis.” *People v. Abrams*, 95 A.D.2d 155, 157, 465 N.Y.S.2d 208, 210 (N.Y. App. Div. 1983). See *Schneckloth*, 412 U.S. at 233. On the one hand deception by a law enforcement officer as to his or her identity in an undercover capacity does not invalidate consent obtained because the defendant does

not the true identity of the informant. *See generally Hoffa v. United States*, 385 U.S. 293 (1966); *Lewis v. United States*, 385 U.S. 206 (1966). At the other end of the spectrum, consent is per se invalid if law enforcement officers represent to the person giving consent that they have the authority to search irrespective of whether consent is given. *See Bumper v. North Carolina*, 391 U.S. 543 (1968) (officer falsely claimed that he had a search warrant). In between these situations are those in which the law enforcement officers do not disclose the nature of its investigation as criminal. Such cases are decided on a case-by-case basis in looking to see whether law enforcement officers affirmatively and materially misrepresented the nature of their purpose. *See United States v. Tweel*, 550 F.2d 297, 299 (5th Cir. 1977); *United States v. Prudden*, 424 F.2d 1021, 1033 (5th Cir. 1970); *Commonwealth v. Slanton*, 530 Pa. 207, 216, 608 A.2d 5, 9 (1992).

Defendant argues that the detective's initial representations that there was "a problem in the neighborhood with people gaining access to someone else's computer" and that he wanted to make sure that Defendant did not "have the same issue" misled Defendant into thinking that there could be a problem with other people accessing his computer. It is likely that under the circumstances that Defendant understood the comment to mean that the detective was investigating some form of community wireless poaching. The detective did not specify whether the "issue" was that Defendant was gaining access to another's computer or whether someone else was gaining access to Defendant's computer. Despite the ambiguity, which was probably intended by the detective, it is more likely than not that Defendant reasonably interpreted the detective's comments to mean that he was checking to see if Defendant was accessing another person's wireless router. Subjectively, Defendant knew that he had been accessing his

neighbor's wireless router without permission, which makes it likely that he construed the detective's comments as referring to such activity. Objectively, anyone such as Defendant, who did not have a wireless router and who was confronted by the "issue" of someone accessing another's computer, could only reasonably conclude that he was the one doing the accessing.²

The subsequent dialogue between the detective and Defendant supports this conclusion. After consent had been given and while the detective was conducting his search of Defendant's computer, Defendant asked, "What are you looking for?" The detective responded that he was checking to see if Defendant had an issue on his computer. Defendant inquired further as to what "kind of issue" the detective was looking for. The detective stated that he was checking "to see if anybody's accessed this computer." At this point Defendant, sounding confused, asked the detective, "They've accessed this computer?" Defendant's confusion demonstrates how he or any reasonable person in his position would not have believed up to that point that the officer was checking to see if anyone else had accessed Defendant's computer.³

² In the alternative, one could construe the detective's comments in a totally different manner that is still entirely consistent with the scope of his investigation, in which case there would be no misrepresentation at all to invalidate the otherwise valid consent. Defendant attempts to describe the "issue" stated by the detective as a problem with Defendant accessing an unsecured wireless router in the neighborhood, but this does not fully describe the investigation that was being conducted. This case involves Defendant making videos containing child pornography available to others through the use of a peer-to-peer computer network. In a peer-to-peer network, files are shared through the network by allowing other members of the network to access files on other network computers. Therefore, the "issue" in this case does in fact involve others accessing Defendant's computer. The "issue" was that others were accessing Defendant's computer through Limewire to view and download child pornography. That was the "issue" that led this investigation to Defendant's front door and subsequently to his computer screen.

³ Defendant has also pointed to this statement by the detective as a misrepresentation; however, this statement was made in the middle of the detective's search after consent had been given. This representation, whether false or true, could not have been the basis of Defendant's consent insofar as it was made after Defendant consented to the search. In fact Defendant's confusion regarding this statement is evidence that that Defendant's consent was not made upon a belief that his computer was being accessed. Although it could be argued that this representation could have induced Defendant to refrain from withdrawing his consent, such argument lacks merit. It is most likely that Defendant consented under the reasonable impression that the detective was investigating him for accessing another's wireless router.

Based upon all of the circumstances surrounding Defendant's consent, the court finds it most likely that the Defendant drew the only reasonable conclusion Defendant could have drawn from the detective's comments. Defendant knew that it was probable that he was being investigated for accessing his neighbor's wireless router without permission.

Defendant also argues that by saying that there was "a problem in the neighborhood with people gaining access to someone else's computer" and he wanted to make sure that Mr. Bailey did not have the "same issue", the detective misled Defendant into thinking that at least one other person had the same issue. As discussed above, it is most probable that Defendant reasonably believed that he was the one doing the accessing described by the detective; therefore, his belief as to whether others were accessing the neighbor's wireless router is immaterial to his consent. He understood that it was highly probable that he was the one being investigated and chose to make his computer available for the detective to search. Defendant knew that the detective was looking to see if he had been accessing his neighbor's wireless router. Even if the detective misled Defendant into thinking that others may also be accessing the neighbor's wireless router, which is far from clear, Defendant would very likely have consented to the search anyway. Thinking that the police may also be investigating others for criminal activity in no way induces one being investigated to open up his belongings for a search.

Defendant also asserts that the search exceeded the scope of the consent. This argument lacks merit irrespective of what the detective meant by the "issue." Whether

When the detective changed Defendant's perspective by stating that he was checking "to see if anybody's accessed this computer" Defendant did not withdraw his consent. Defendant watched everything the detective did while at the computer and could have withdrawn consent at any point if the search took a turn that was not within Defendant's contemplation.

the “issue” was Defendant accessing his neighbor’s wireless router or others accessing Defendant’s computer through Limewire, a search for files containing child pornography was what would link a computer to such an “issue”. These were the files accessed by Wyoming law enforcement agents on Defendant’s computer and were also the files that Defendant was making available to others by accessing his neighbor’s wireless router. All of this was accomplished through Limewire. The scope of the consent given by Defendant cannot reasonably said to exclude a search for the files or for information regarding Defendant’s use of Limewire.


CONCLUSION

The State has proven by the preponderance of the evidence that Defendant consented to the search of his computer and apartment. The Court finds that although law enforcement did not disclose much detail about the scope of the investigation, no affirmative misrepresentation was made to Defendant to procure his consent. Any misrepresentation by the detective in this case was made after consent was given and could not have produced such consent. At the time he consented, Defendant knew that it was highly probable that the detective wanted to look at his computer to see if he had accessed his neighbor’s wireless router. The detective did nothing inconsistent with such a purpose. Therefore, Defendant’s motion to suppress must be denied.

The entry is:

The Defendant’s motion to suppress is **DENIED**

Dated: November 26, 2008


William R. Anderson
Justice, Superior Court

STATE VS JACK D. BAILEY, II

CR-2008-229

ATTORNEY FOR THE STATE

MICHAEL ROBERTS, DEPUTY D.A.
DISTRICT ATTORNEY
97 HAMMOND ST
BANGOR ME 04401

ATTORNEY FOR THE DEFENDANT

F. DAVID WALKER ESQ
P O BOX 1401
BANGOR ME 04402-1401