**UNITED STATES COURT OF APPEALS**
**FOR THE ELEVENTH CIRCUIT**

**CASE NO. 14-14506-E**

---

**UNITED STATES OF AMERICA,**

**Plaintiff/Appellee,**

**v.**

**ALEXANDER ROUSSEAU,**

**Defendant/Appellant.**

---

**ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF FLORIDA. HON. K. MICHAEL MOORE, DISTRICT JUDGE**

---

# REPLY BRIEF OF APPELLANT ALEXANDER ROUSSEAU

---

**BENEDICT P. KUEHNE**
**MICHAEL T. DAVIS**
**LAW OFFICE OF**
**BENEDICT P. KUEHNE, P.A.**
**100 S.E. 2nd St., Suite 3550**
**Miami, FL 33131-2154**
**Tel: 305.789.5989**
**Fax: 305.789.5987**
**Efiling@kuehnelaw.com**
**Counsel for Appellant**

## CERTIFICATE OF INTERESTED PERSONS

Appellant Alexander Rousseau certifies the following persons and entities may have an interest in this case:

Michael T. Davis

Joel DeFabio

Eloisa D. Fernandez

Vanessa S. Johannes

Benedict P. Kuehne

Nicole D. Mariani

Hon. Chris M. McAliley, U.S. Magistrate Judge

Hon. K. Michael Moore, Chief U.S. District Judge

Hon. Alicia Otazo-Reyes, U.S. Magistrate Judge

George T. Pallas

Alexander Rousseau

Lisa Rubio

Emily M. Smachetti

Kathleen M. Salyer

Benjamin J. Widlanski

## TABLE OF CONTENTS

# TABLE OF AUTHORITIES

**CASES** **PAGE**



**Other Authorities**

## ARGUMENT

### I. THE TRIAL COURT ERRED IN FAILING TO HOLD A *FRANKS* HEARING, WHERE THE SEARCH WARRANT AFFIDAVIT CONTAINED MATERIAL MISREPRESENTATIONS AND OMISSIONS THAT UNDERMINED PROBABLE CAUSE.

Rousseau argues the trial court erred in granting a *Frank*'s hearing on his motion to suppress, where the warrant contained material misrepresentations (Initial Br. 25-33). The government claims "Rousseau did not present any evidence showing that the alleged misrepresentation resulted from deceptive intent or recklessness, as opposed to mere negligence or something even less, on Agent Carpinteri's part." (Answer Br. 24-25). The record shows otherwise. At the hearing, Mr. Rousseau established how plain and obvious it was that a public park bordered the fire station. Defense counsel explained that a simple Google search or a casual review of the publicly accessible Miami-Dade online Property Appraiser's website demonstrated it was impossible to not notice the

public park abutting the fire station:

> One thing that may be useful to your Honor and it is exactly what I did in this case is particularly when you're confronted with a search warrant of a structure I always go to Google Maps and I go to the Miami-Dade or whatever jurisdiction property appraisers and they have digital photos and that's where I was able to focus on that property from, you know, aerial view and front and side. And you can see, I mean you just can't park in front of the Firehouse and miss a public park. There is like thirteen tennis courts in this park, it's huge, I was totally unfamiliar . . . .

(DE43:36). The government did not dispute the underlying reliance on this unquestionably reliable evidence at the suppression hearing.

Mr. Rousseau further challenges Agent Carpinteri's failure to disclose in the warrant the information establishing there was no need or even factual basis to search every single electronic device on the premises, yet the warrant authorized exactly that broad and unlimited search. Even if the issue was not raised contemporaneously at trial (although Mr. Rousseau asserts that is was sufficiently preserved), the issue was an integral part of the suppression motion's second issue, which challenged the overbreadth of the warrant. The omission is

particularly relevant, as will be discussed, to the government's claim that the *Leon* good-faith exception to the exclusionary rule applies. *See United States v. Harris*, 172 Fed. Appx. 950, 957 (11th Cir. 2006) (good-faith exception to the exclusionary rule does not apply where the magistrate judge was misled by deliberately misleading information provided by law enforcement).

Accordingly, the district court's failure to conduct an evidentiary hearing on the omission of this crucial, probable-cause impacting issue, requires a reversal of the convictions and a remand for further proceedings concerning the suppression motion.

## II. THE TRIAL COURT ERRED IN DENYING THE MOTION TO SUPPRESS, WHERE THE OVERLY BROAD WARRANT AUTHORIZED THE SEARCH AND ULTIMATE SEIZURE OF MATERIAL NOT CONNECTED TO THE FBI'S ARES INVESTIGATION.

Mr. Rousseau argues on appeal, as he did at trial, that the search warrant violated the Fourth Amendment's particularity requirement because it permitted the search of every firefighter's electronic device, regardless of any connection or lack thereof to the asserted unlawful

activity. Attachment A, Paragraph 1 authorized the search of every "computer" located on the premises of Miami Fire Station 6, based on the search warrant affidavit's broad allegation that the computers could potentially access the open wireless network and/or store illicit materials. The government concedes the warrant's broad and expansive scope, yet maintains the search warrant was supported by probable cause (Answer Br. 38). This contention should be rejected by the court.

### A. The Government's Preservation Argument Fails, Where the District Court Specifically Acknowledged and Overruled Mr. Rousseau's Overbreadth and Particularity Argument.

The government erroneously contends Mr. Rousseau's overbreadth claim was not preserved. The district court, in overruling Mr. Rousseau's objections to the report and recommendation, recognized the precise argument raised by Mr. Rousseau raised on appeal: "Defendant's Motion to Suppress raises two arguments: . . . "that the search warrant was unconstitutionally overbroad." (DE50:1-2). The district court affirmed its

understanding of Mr. Rousseau's precisely contoured argument in stating:

> Specifically, Defendant objects to the second paragraph contained in Attachment A, as well as paragraphs 3(d), 3(e), 5, and 6 contained in Attachment B of the search warrant, on the basis that they are "so broadly written that they essentially call for the seizure and review of nearly every piece of electronic data on any computer as well as other electronic devices at the Target Premises (Firehouse 6)." Mot., at 8-9. Judge McAliley's Report clearly sets forth the law on the particularity of search warrants in this Circuit.

(DE50:3). This latter quote, noticeably absent from the government ten-page explication of the course of proceedings, forecloses the government's contrary argument. The district court clearly understood the nature of Mr. Rousseau's claim but expressly rejected it.[1]

[1] Moreover, the motion was titled *Motion to Suppress Physical Evidence (Overbreadth)*. In it, Mr. Rousseau quoted Paragraph 2 Attachment A, which authorized the search of every "computer" found on the premises, and claimed that broad and unrestricted language violated the Fourth Amendment by authorizing "the seizure of the following items whether or not they have any relationship to criminal activity." (DE29:7).

For this reason, the proper standard of review for this issue is *de novo*. *United States v. Braslow*, 586 Fed. Appx. 578 (11th Cir. 2014) (citing *United States v. Mathis,* 767 F.3d 1264, 1274–75 (11th Cir. 2014)).

### B. The Government's Claim That It Had Probable Cause to Search Each and Every Firefighter's Electronic Device On the Premises at The Time of The Warrant's Execution Is Indefensible.

1. *Probable cause to search the larger premises of Miami Fire Station 6 did not extend to the firefighter's personally-owned electronic devices because individualized probable cause was required to search and seize each item listed in the warrant.*

The government argues that "as long as there was probable cause to search the entire Miami Fire Station 6 when the warrant was issued, then the warrant was valid and not overbroad." (Answer Br. 36). This red herring ignores that the search of the station was but one of two categories of items sought to be searched. The search warrant requested permission to search the station as a whole as well as any "computer" located thereon:

**DESCRIPTION OF PROPERTY TO BE SEARCHED:**

The Target Premises, located at 701 NW 36 Street, Miami, Florida 33127, consists of Miami Fire Station #6, which is facing south. The building is beige in color, with brown trim, four metal garage bay doors, and a white front door. The City of Miami Fire Station No. 6 is affixed in brown lettering to the building.

Any computers (that is, any electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, including electronic mobile devices (such as cellular telephones, smartphones, tablets, electronic notebooks) and data storage devices (such as fixed disks, internal and external hard drives, floppy disk drives and diskettes, CD and DVDs, flash memory cards, thumb drives, SIM cards, and other internal and peripheral magnetic, optical, and electrical storage devices)) found in the Target Premises.

(DE:33-1:29).

The Fourth Amendment required that there be "probable cause . . . to seize each item specified in the warrant." *In Matter of Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.*, 21 F. Supp. 3d 1, 6 (D.D.C. 2013). Thus, even if probable cause existed to enter the premises, the government was still required to establish probable cause to search and seize every firefighter's personal "computer," which was broadly defined to include all personal electronic devices including cell phones.

2. *The government's search warrant was not narrowly tailored, where all its evidence pointed to one single person not disclosed to the issuing magistrate, yet it requested a warrant authorizing the search of every electronic device on premises.*

The government attempts to justify its conduct, claiming it faced "the challenge of searching for digital data without knowing where that file might be stored, both in terms of the device or devices to which that data was downloaded and of the location of that device or devices within the fire station." (Answer Br. 37). The government's needle-in-a-haystack claim does not comport with the trial evidence. The government, in its case-in-chief, was direct and laser-like in its position that it connected only one person to the illegal downloading. According to the government, only one person was on duty each time the illicit material was downloaded (DE100:48, 54, 56, 83). Also according to the government, that same person, though discovered after the search warrant's execution, was also on duty at other stations when illicit material was downloaded (DE100:48, 86-87). Agent Carpinteri was so confident that this person was "her guy" that she scheduled the warrant's execution on

a day that same person would be on duty. The government's contrary appellate claims should unequivocally be rejected.

For this same reason, the government's claim on appeal that the "search warrant was narrowly tailored to ensure that, while the entire fire station was to be searched, that search was as limited as possible" should also be rejected (Answer Br. 38). The government plainly had no reason to believe that every single firefighter on duty the night of April 6, 2014, was downloading illicit material and needed to have their private electronic devices seized and searched. Indeed, Agent Carpenteri was so confident that she had her guy that when she learned another firefighter had secreted his personal property in his trunk while they gathered for and executed the raid, and then refused to grant law enforcement access to the trunk, she did not use FBI resources to follow up and conducted no inquiry as to the likelihood that this person was in fact disposing of evidence connected to the investigation and the scope of the warrant (DE100:121-22). Instead, she deferred to the local police (DE100:122).

3. *The government lacked probable cause to believe there was illicit materials on every device on the premises. It only had arguable probable cause regarding one person's device.*

The government alternatively argues it had probable cause to search each computer because "there was a fair probability that child pornography was present on an electronic device that was able to access the Internet using the wireless network at any location within Miami Fire Station 6 as opposed to in some narrower subsection of the fire station." (Answer Br. 37). The mere ability to access an open wireless network did not and does not establish probable cause to search and seize every personal device on premises, particularly given the fluidity of the fire station's occupancy. This was a public government building with "lots of employees." (DE100:46). There were three shifts at the station each day (DE100:59; DE109:102). The firefighters worked a 24 hour shift, then had 48 hours off (DE100:56).

To justify the broad and unfettered intrusion into all the personal electronic devices, the government was required to articulate an individualized suspicion. For this reason, the proposed search was much

akin to the search of individual units in a multiple-dwelling unit, where a general suspicion of ongoing criminal conduct does not justify the wholesale search of each individual unit. *United States v. Shamaeizadeh*, 80 F.3d 1131, 1137 (6th Cir. 1996); *United States v. Hinton*, 219 F.2d 324, 326 (7th Cir. 1955); *Jacobs v. City of Chicago*, 215 F.3d 758, 767 (7th Cir. 2000). *See also Booth v. Antill*, 849 F.2d 604 (4th Cir. 1988); *United States v. Perez*, 484 F.3d 735, 741 (5th Cir. 2007); *United States v. Whitney*, 633 F.2d 902, 907 (9th Cir. 1980); *United States v. Rios*, 611 F.2d 1335, 1347 (10th Cir. 1979).

The government attempts to distinguish the cited case law, claiming the multi-dwelling rule applies only where the suspect has access to solely one unit inside the larger building (Answer Br. 40). In this case, according to the government, the search warrant's scope was justified because Mr. Rousseau had access to the entire station. (Answer Br. 40). This purported distinction only underscores the government's lack of probable cause. First, as explained above, the justification to enter

and search all parts of the fire station, where the wireless network could be accessed, was a separate and distinct inquiry from the question of probable cause to search and seize each device on premises during the search warrant's execution.

Furthermore, the government had no reason to believe the person it identified as accessing illicit materials was potentially downloading illicit material on another device, much less on the other on-duty firefighter's personal devices, including cell phones. Quite the opposite. The government's evidence pointed to Ares as being a desktop computer software (DE109:153-54, 156-57), not an Android or IPhone software application. Professor Malex explained that peer-to-peer systems worked with your personal computer and your personal laptop (DE109:156, 158). And the same Ares-assigned user name was involved in all monitored transactions (DE33-1:14, 17; DE109:150).

The government further claims Agent Carpenteri testified at trial that "it was going to be tough to identify who it was" that was

downloading the illicit material (Answer Br. 28). This inaccurate characterization of her testimony omits the fact that Agent Carpenteri continued her investigation with the express purpose of trying to "determine if it could have been a specific one or two employees." (DE100:47). Through the employment records, she was able to narrow it down to a single name:

> **Carpenteri**: I was given those records in the end of January and I sat down and went one by one through the firefighters listed to see if I saw any -- I was hoping to see one or two names.
>
> **Government**: Did you see one or two names?
>
> **Carpenteri**: **No, I only saw one name** that stuck out as consistently being on duty on the dates that I saw activity on the Ares network.

(DE100:48-49) (emphasis added).

The government purposely hid its hand from the magistrate judge. Truthful disclosure of the results of its investigation, which clearly showed it lacked probable cause to believe every single firefighter's personal electronic device, would have severely undercut its broad and unlimited probable cause quest. The district court therefore erred in

concluding there was probable cause to justify the wholesale search and seizure of every electronic device. This error is prejudicial and reversible.

### C. The Government Cannot Claim Good Faith Reliance on the Search Warrant, Where It Failed to Disclose All Material Facts to the Magistrate Judge.

The government alternatively contends the good faith exception to the exclusionary rule applies. This argument, too, is misplaced. The *United States v. Leon*, 468 U.S. 897, 922 (1984), exception does not apply where the "the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." *United States v. Martin*, 297 F.3d 1308, 1313 (11th Cir. 2002) (internal quotes omitted). It likewise does not apply where the "warrant is so facially deficient — i.e., in failing to particularize the place to be searched or the things to be seized — that the executing officers cannot reasonably presume it to be valid." *Id*. (citations omitted).

In this case, the government cannot satisfy its "burden of demonstrating the applicability of the *Leon* good faith exception." *United*

*States v. Robinson*, 336 F.3d 1293, 1297 (11th Cir. 2003). The judge heard no evidence from Agent Carpinteri regarding her intent in drafting the warrant affidavit, expressly declining to convene an evidentiary hearing (DE43:34-35). And the government's reliance on the affidavit does not prove there was no intentional omission or reckless disregard of the truth.[2] As already discussed, the FBI had comprehensive evidence of *one* employee downloading illicit materials. They knew when that employee would be working, and executed the warrant on a day that employee was working. Disclosure of this extensive evidence undoubtedly would have undermined its claim of probable cause to search every device on the station; and if disclosed, would have radically transformed the character of the magistrate judge's probable cause analysis.

[2] *See United States v. Lara*, 588 Fed. Appx. 935, 939 (11th Cir. 2014) (holding that "the government's lack of extrinsic evidence does not preclude a finding of good faith" where "the government submitted lengthy affidavits to support the warrant application").

This lack of disclosure was not the only material misrepresentation, as the affidavit itself materially distorted the accessibility of Ares on electronic devices. After broadly defining computer to include smart phones and cell phones,[3] the government claimed that peer-to-peer file-sharing "software is designed to allow users to trade digital files through a worldwide network that is formed by linking **computers** together." (DE33-1:11) (emphasis added). Under its affidavit, peer-to-peer file sharing software was available on smart phones and could be linked to desktop computers for peer-to-peer file sharing. The search warrant contained a similar suggestion in Paragraph 9: "The download of a file can be achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file." (DE33-1:12).

[3] "The term "computer," as used throughout the entirety of this affidavit and attachments, includes electronic mobile devices, such as, cellular telephones, smartphones, tablets, electronic notebooks, and data storage devices (as defined below)." (DE33-1:8).

Finally, the affidavit extended its claim that peer-to-peer software was available on all computers to Ares: "In ARES, a user who is attempting to trade files can place files from his local computer into a "shared" file directory." (DE33-13). According to the search warrant affidavit, the government was proffering supposed probable cause to search all personal electronic devices, including smart phones, because Ares could universally be used to share and store illicit materials across all platforms.

The trial evidence established the opposite. Sam Malek, Professor of Computer Science at George Mason University, explained that Ares and other peer-to-peer networking software linked personal desktop computers and laptop computers (DE109:134-35, 156, 158). Consider the following testimony:

> Q. Professor, what are all these peers?
>
> A. These peers are -- these peers are just computers. These could be personal computers. These would be your personal laptop, personal desktop that is connected to something like Internet and is able to talk to other computers that are running the same application.

> Q. So I'm sure that it's a lot more complicated than what you just described, but is this the basic structure of peer-to-peer file sharing?
>
> A. Right.

(DE109:156). At the conclusion of his direct examination testimony, Professor Malek was asked to summarize what peer-to-peer software was:

> Q. Professor, could you describe in one sentence basically what Ares and peer-to-peer file-sharing networks in general do?
>
> A. So they are -- they -- so Ares file -- peer-to-peer file-sharing application provides a way for users to download files from other users on a computer network.

(DE109:158). This testimony materially contradicted the government claim in its search warrant affidavit that smart phones and other cellular phones could participate in the peer-to-peer sharing of illicit materials. Because the government's warrant contained material omissions and misrepresentations that undermined probable cause, the government cannot satisfy its burden of establishing its entitlement to *Leon*'s good faith exception.

## CONCLUSION

Alexander Rousseau is entitled to a vacation of his convictions due to the erroneous and prejudicial denial of the motion to suppress evidence, and a remand with directions for the district court to order a *Franks* hearing or otherwise order suppression of the evidence so the evidence is not considered at a new trial.

## CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation in Rule 32(a)(7)(B) of the Federal Rules of Appellate Procedure. This brief is printed in Century Schoolbook 14-point font and contains 3,242 words, as counted by MS Word.

Respectfully submitted,

*s/ Benedict P. Kuehne*
**BENEDICT P. KUEHNE**
Florida Bar No. 233293
**MICHAEL T. DAVIS**
Florida Bar No. 63374
**LAW OFFICE OF BENEDICT P. KUEHNE, P.A.**

100 S.E. 2nd St., Suite 3550
Miami, FL 33131-2154
Tel: 305.789.5989
Fax: 305.789.5987
ben.kuehne@kuehnelaw.com
efiling@kuehnelaw.com

## CERTIFICATE OF SERVICE

I CERTIFY on June 8, 2015, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF. I also certify the foregoing document is being served this day on all counsel of record either via transmission of Notices of Electronic Filing generated by CM/ECF or in another authorized manner for those counsel or parties not authorized to receive electronically Notices of Electronic Filing.

By: *S/ Benedict P. Kuehne*
**BENEDICT P. KUEHNE**