CALIFORNIA LAW CENTERS, APLC
James V. Hairgrove
California Bar No.: 181891
501 W. Broadway, Suite A121
San Diego, CA 92101
Tel: (619) 667-3743
Fax: (619) 667-3763
Email: jvhesq@yahoo.com

Attorney for Idin Rafiee

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

HONORABLE JANIS L. SAMMARTINO

UNITED STATES OF AMERICA, Plaintiff, v. IDIN RAFIEE, Defendant.	Case No.: 14CR0240-JLS - 3 **NOTICE OF MOTION AND MOTION TO SUPPRESS EVIDENCE AND MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF (FRCP RULE 12(b)(3))** **Date:** August 22, 2014 **Time:** 2:00 P.M. **Honorable Janis L. Sammartino**

MOTION TO SUPPRESS EVIDENCE

COMES NOW, Idin Rafiee, Defendant in the above captioned matter, by and through undersigned counsel, and hereby moves this Honorable Court pursuant to Rule 12(b)(3) of the Federal Rules of Criminal Procedure, to suppress physical evidence unlawfully obtained which the government proposes to use as evidence against the Defendant at trial, and in support of the motion states as follows:

I. Procedural History

Defendant is currently charged by Indictment with one count of conspiracy to violate the International Emergency Economic Powers Act ("IEEPA") and the Iranian Transactions and Sanctions Regulations ("ITSR"), in violation of 50 U.S.C. §§ 1702, 1705, and 31 C.F.R. §§ 560.204, 560.206, and 560.208, and criminal forfeiture, in violation of 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c).

Defendant was charged by criminal complaint under seal on January 8, 2014. Defendant made his initial appearance before the Court on January 9, 2014, and was released on a personal surety bond. The complaint was superseded by indictment on February 4, 2014. Defendant was arraigned and entered a plea of not guilty on February 6, 2014. This motion is currently scheduled for August 22, 2014.

II. Factual Background

Defendant Idin Rafiee lives in San Diego, California. On October 5, 2012, he was scheduled to leave on an outbound flight from Los Angeles, California, to London, England. Defendant, who had graduated from the University of San Diego in May 2012, was traveling to London for personal reasons. He was traveling with electronic media, specifically a Dell laptop computer, an external Seagate hard drive, a cell phone (HTC smart phone), and an iPad.

While defendant was passing through security, an agent with the United States Department of Homeland Security, Customs and Border Protection, approached Defendant and told him that his electronic media was being detained. The agent said that there was reason to believe Defendant possessed child pornography on the media. It was not made clear to Defendant the justification for this assertion. Further, no cursory inspection of the devices was performed at the time of seizure. Agents allowed Defendant to continue with his travel, but seized the electronic media devices.

Before the detained property was returned to him on October 13, 2012, it was shipped to a different location for forensic imaging. Defendant never gave consent to the detainment of his electronic media and it was seized over his objection. Thereafter, the electronics were forensically imaged by a Certified Forensic Agent on October 9, 2012, meaning that the content on the devices was imaged for later review. A forensic image "is an exact physical copy of the hard drive or other electronic media." *Ex. A* - Affidavit for Search Warrant at 11, November 1, 2012. Defendant was neither requested to provide, nor did he provide, consent for his property to be forensically imaged or seized. Moreover, federal agents did not obtain a search warrant for the devices prior to detaining them at the airport or subjecting them to forensic imaging.

As a consequence, the images derived from Defendant's electronic media were obtained without a warrant or consent. Moreover, the evidence derived from the images was used as a basis for probable cause in the application of search warrants in this case, dated November 1, 2012 and January 8, 2014. The defense anticipates that the evidence seized from the electronic media, and additional evidence that flowed therefrom through subsequent search warrants, will be used during the Government's case-in-chief to demonstrate Defendant's intent to violate U.S. sanctions targeting Iran.

III. Legal Authorities

A. Border Exception to the Fourth Amendment Warrant Requirement

The Fourth Amendment protects against the unlawful search and seizure of persons and property in which there is a reasonable expectation of privacy. *Kyllo v. United States*, 533 U.S. 27, 33 (2001). Evidence obtained as a result of a Fourth Amendment violation is considered "fruit of the poisonous tree," and thus warrants exclusion. *Wong Sun v. United States*, 371 U.S. 471, 485-86 (1963).

As Supreme Court precedent dictates, the touchstone of the Fourth Amendment is reasonableness. *Ohio v. Robinette*, 519 U.S. 33, 39 (1996); *Florida v. Jimeno*, 500 U.S.

248, 250 (1991). Searches conducted outside the judicial process are per se unreasonable, subject only to a few exceptions. *Arizona v. Gant*, 129 S. Ct. 1710, 1716 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). One such exception to the warrant requirement, which generally requires neither probable cause nor reasonable suspicion are border searches. *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004); *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985).

The border search exception has been applied broadly in light of the sovereign's heightened interest in protecting itself. *Flores-Montano*, 541 U.S. at 152; See also *United States v. Arnold*, 533 F.3d 1003, 1006-07. Limitations have been imposed in certain border searches that have been deemed highly intrusive of the person or the destructive nature of property. See generally *Flores-Montano*, 541 U.S. 149; *Montoya de Hernandez*, 473 U.S. 531. The Supreme Court has ultimately left "open the question whether, under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out." *Flores-Montano*, 541 U.S. at 154 n.2 (quoting *United States v. Ramsey*, 431 U.S. 606, 618 n.13 (1977)).

While the border search exception traditionally has been applied only to persons or property entering the country, the Ninth Circuit has extended the application of the border search exception to exit searches. *United States v. Seljan*, 547 F.3d 993, 999 (9th Cir. 2008); *United States v. Cardona*, 769 F.2d 625, 628 (9th Cir. 1985); but see *United States v. Des Jardines*, 747 F.2d 499, 502-04 (9th Cir. 1984) (acknowledging the lessened government interest as to outbound searches and the inclination to hold suspicionless exit searches unreasonable, yet unable to do so due to Ninth Circuit precedent). Regardless, it "does not mean, however, that at the border 'anything goes.'" *United States v. Cotterman*, 709 F.3d 952, 960 (9th Cir. 2013) (quoting *Seljan*, 547 F.3d at 1000)).

In order to determine whether a border search exceeds the boundaries of reasonableness, a court will look to "the totality of the circumstances, including the scope

and duration of the deprivation." *Ibid*. Indeed, "Even at the border, individual privacy rights are not abandoned but balanced against the sovereign's interests." *Ibid*.

B. Warrantless Search of Electronic Media at the Border

It was not until recently that the advent of significant technological advancements required courts to face the question as to whether the search of electronic media at the border without a warrant is reasonable under the Fourth Amendment. Despite a lack of clear Supreme Court precedent on the issue, lower courts have continuously reviewed such searches through the lens of reasonable suspicion. See *United States v. Arnold*, 533 F.3d 1003, 1008-09 (9th Cir. 2008) (acknowledging that the Supreme Court has left open the possibility of requiring reasonable suspicion for border searches); *United States v. Irving*, 452 F.3d 110 (2d Cir. 2006) (holding that the search of defendant's computer diskettes was reasonable after balancing the level of intrusion with the level of suspicion); *United States v. Roberts*, 274 F.3d 1007, 1012 (5th Cir. 2001) (holding that the although the search of defendant's computer was "non-routine," reasonable suspicion that defendant was carrying contraband existed); *United States v. Furukawa*, 2006 WL 3330726 at 1 (D. Minn. Nov. 16, 2006) (holding that whether the search of defendant's laptop at the border was "routine" was not relevant because reasonable suspicion to conduct the search was found).

The modern line of reasoning as to the search of electronic devices is that it is not so much the type or nature of property searched, but the level of intrusiveness, and consequently the infringement upon privacy, that is at issue. *House v. Napolitano*, 2012 WL 1038816 (D. Mass. 2012). Thus, where a cursory inspection of electronic media conducted pursuant to border search authority has been deemed reasonable, a forensic search of property rises to a heightened level of privacy expectations and requires at least reasonable suspicion before doing so. *Cotterman*, 709 F.3d at 960-61; 962-63 (emphasis

added); see also *Arnold*, 533 F.3d 1003 (9th Cir. 2008) (holding that a cursory laptop inspection at the border was not particularly offensive under *Flores-Montano*).

The Ninth Circuit has already established clear precedent as to the unlawfulness of a warrantless forensic search of electronic media. In *Cotterman*, the defendant was entering the United States at the Mexican border. Because of a prior child molestation conviction, he was subjected to a secondary search, including a cursory search of his electronic devices. Although the search at the border did not initially reveal incriminating evidence, agents detained his laptops and digital cameras, shipped them to another location for forensic imaging, and proceeded to search until incriminating evidence was found. *Id* at pp. 957-958. The Court ultimately found that reasonable suspicion was required before forensically imagining and searching the devices, yet such a requirement was met due to a variety of factors that established a "particularized and objective basis" for the search. *Id*. At pp. 968-70.

In its decision to apply a reasonable suspicion legal standard, Judge McKeown reasoned, "It is the comprehensive and intrusive nature of a forensic examination — not the location of the examination — that is the key factor triggering the requirement of reasonable suspicion here." *Id*. at p. 962. Indeed, "notwithstanding a traveler's diminished expectation of privacy at the border, the search is still measured against the Fourth Amendment's reasonableness requirement, which considers the nature and scope of the search." *Id*. at p. 963.

C. For Search and Seizure Purposes, Detaining Property Is The Same as Detaining the Person Who Owns The Property and Requires Reasonable Suspicion and Probable Cause.

When a person is not free to leave without abandoning luggage, plane tickets or their electronic media as in the instant case, that person is not free to leave and is seized the same as if that person were in jail. The seizure of luggage from a traveller's

possession "intrudes on both the suspect's possessory interest in his luggage as well as his liberty interest in proceeding with his itinerary." *Place*, 462 U.S. 696 at 708, 103 S.Ct. at 2645. In *Place*, the Supreme Court set forth standards for assessing the constitutionality of detentions of luggage without probable cause. Applying the principles of *Terry v. Ohio*, 392 U.S. 1, 88 S.Ct. 1868 (1968), to the context of luggage detention, the Court held that a police officer may briefly detain luggage for investigation if he has a reasonable, articulable suspicion that the luggage contains narcotics. *Place*, 462 U.S. at 706. In order for the fruits of this investigatory detention to be admissible, however, the seizure itself must be conducted in a reasonable manner. Id. at 707-10. A seizure is reasonable if: (1) the length of the detention is sufficiently short, and (2) government agents act with diligence in pursuit of their investigation. Id. at 709. The Court did hold that "the [90-minute] length of the detention of [Place's] luggage alone precludes the conclusion that the seizure was reasonable in the absence of probable cause." Ibid.

In *191,910.00 in U.S. Currency*, 16 F.3d 1051, the court held that the law enforcement agents failed to act with diligence in pursuing evidence of probable cause they must not unreasonably fail to recognize or pursue avenues which would lessen the length of the detention. See *United States v. Holzman*, 871 F.2d 1496, 1501 (9th Cir.1989). These cases suggest that diligence be exercised when reasonably less intrusive means of investigation are available to law enforcement and the seizure be reasonable and the length of detention be sufficiently short for the fruits seized to be admissible and not to intrude on a suspects possessory interests and freedom of movement. The reasonableness of a border stop or search is relevant only when a stop and search is “non routine”. Since routine border stops and searches are exempted from the Fourth Amendment, no determination of reasonableness attaches. When a stop or search becomes non-routine, the reasonableness requirement of the Fourth Amendment requires

reasonable suspicion. If a stop or search reaches the level of full arrest, or is sufficiently invasive, there must be probable cause in addition to reasonable suspicion.

IV. Argument

A. Neither Reasonable Suspicion Nor Probable Cause Has Been Established

The seizure and forensic search of Defendant's electronic media violated his Fourth Amendment rights because the requirement of reasonable suspicion has not been met. In light of the decision of *Cotterman*, it is clear that the federal agents were required to establish reasonable suspicion before detaining, forensically imaging, and searching Defendant's property. Without the requisite reasonable suspicion, the search was inherently unreasonable, and evidence obtained therefrom should be suppressed.

As described in the factual review above, Defendant was approached at the San Diego Airport on October 5, 2012, and informed that agents believed his electronic devices contained child pornography. The governmental motive was disingenuous when the property was then seized with the sole purpose of forensically imaging the devices at another location before returning them to Defendant. This is evidenced by the fact that an ordinary and routine cursory inspection of the devices at the airport never occurred.

In documents and statements presented to the Court, the government asserts reasonable suspicion to detain the media was satisfied based upon information provided by a source of information ("SOI"), which led to an open source investigation into Defendant and unrelated companies utilizing the same business address and location. Indeed, during the last status hearing and discovery motion before this Court the Government stated that the open source investigation was initiated solely as a result of information provided by the SOI.

The evidence that has been provided through discovery, specifically the materials relating to the information provided by the SOI, does not appear to establish any cause to

initiate an investigation into defendant's conduct. To be specific, the government provided a one-page document of notes taken during the initial call from the SOI to the Department of Homeland Security, dated October 1, 2012. *Ex. B* – Notes with Source of Information, Ray Pack. This single page reads like the frustrations of a disgruntled employee, not a credible source of information that has provided reliable evidence of ongoing crimes, let alone any evidence that would reasonably indicate potential criminal activity. Further, the notes do not mention Iran, money laundering, or any specific details that would reasonably lead to a full-on investigation into Defendants' conduct.

Setting aside the credibility of the source, to argue that a single telephone conversation was sufficient to spark a full-fledged investigation in a matter of days, and that as a consequence of which there was sufficient evidence to justify reasonable suspicion regarding an ongoing criminal conspiracy by Defendant, is preposterous. The Government would have the Court believe that sufficient evidence was obtained through the telephone conversation with the SOI, coupled with a three or four day investigation. Either the Government has failed to comply with its discovery obligations or, more likely, the evidence to establish reasonable suspicion of wrongdoing simply does not exist.

Prior decisions are instructive as to what constitutes reasonable suspicion for a forensic search. In *Cotterman*, the Court held that the forensic search was reasonable because of the "TECS alert, prior child-related conviction, frequent travel [of the defendant], crossing from a country known for sex tourism, and collection of electronic equipment, plus the parameters of the Operation Angel Watch program, taken collectively, gave rise to reasonable suspicion of criminal activity." 709 F.3d at 969. Comparatively, the telephone call from the SOI, and whatever open source investigation could have possibly revealed in just a couple of days, plainly does not equate to the standards of *Cotterman*.

Reasonable suspicion requires that more than an inchoate or unparticularized suspicion or hunch; rather, there must be specific reasonable inferences which can be drawn from the facts or circumstances. *Terry v. Ohio*, 392 U.S. 1, 27 (1968). The government has failed to put forth any substantial evidence that would even suggest that specific inferences were present to justify the seizure and search of Defendant's electronic media without a warrant. What is apparent, however, is that without the search of Defendant's devices, the Government had no basis for probable cause to justify the application of the search warrants that were obtained later. As clearly described in Agent Hamako's affidavit, signed November 1, 2012, there is no mention of any evidence, or articulable facts, obtained prior to October 5, 2012, that would have given rise to a reasonable suspicion.

In light of the totality of the circumstances, reasonable suspicion has not been established to justify the forensic search of Defendant's property. The evidence was unlawfully seized from the forensic images of Defendant's media, and thus, such evidence should be suppressed.

B. The Warrantless Search of Defendant's Electronic Devices is Unreasonable

"A person's digital life ought not be hijacked simply by crossing a border." *Cotterman*, 709 F.3d at 965. Yet that is precisely what occurred to Defendant. Here, without even so much as a cursory examination, the devices were detained and sent to another location. Forensic images were thereafter taken of Defendant's laptop computer, external hard drive, and cell phone.[1] *Ex. A* – Affidavit at 11. The images were provided to HSI Special Agent Kevin Hamako on October 23, 2012. *Ex. A* – Affidavit at 6. Agent Hamako reviewed the images upon receipt, which included "thousands of unique email communications and documents." *Ex. A* – Affidavit at 7.

[1] Due to encryption features, agents were unable to forensically image Defendant's iPad. See *Ex. A* - Affidavit at 6.

The review of forensic images of Defendant's hard drive and laptop caused Agent Hamako to apply for a search warrant on November 1, 2012, less than one month after the items were seized from the Defendant at the airport. In the application, Agent Hamako relies on email communications that he reviewed from the images as a basis for probable cause to conducted additional review and extraction of evidence from Defendant's devices related to alleged violations of IEEPA, ITSR, and money laundering. See generally, *Ex. A*.

The actions by the Government are disconcerting and are a haphazard attempt to remediate the unlawfulness of the forensic search. Not only has the Government unquestionably crossed the line of reasonableness by detaining the devices without reasonable suspicion, but in turn relies on the unlawfully obtained evidence as a basis to obtain a warrant to search what has already been searched. Indeed, when considering the circumstances as a whole, the conduct at issue is inherently unreasonable.

Although courts have refused to impose a "complex balancing test" or "intrusiveness analysis" to determine whether searches conducted at the border are reasonable, the Supreme Court's recent decision in *Riley v. California* is instructive when determining the reasonableness of forensic searches of electronic media conducted without a warrant. ___ S. Ct. ___, Nos. 13-132, 13-212, 2014 WL 2864483 (June 25, 2014); see *Arnold*, 533 F.3d at 1008. In *Riley*, the Court was faced with the issue of whether a warrantless search of a cell phone incident to a lawful arrest was reasonable. *Id*. Similar to the border search exception, searches incident to lawful arrest generally do not require a warrant. See generally *Arizona v. Gant*, 556 U.S. 332 (2009); *United States v. Robinson*, 414 U.S. 218 (1973); *Chimel v. California*, 395 U.S. 752 (1969).

Despite the general exception to the warrant requirement, however, the United States Supreme Court held that in the context of cell phones, police officers must now obtain a warrant prior to such a search. *Riley*, 2014 WL 2864483. As the Court reasoned,

there is a distinction between detaining property at the time of arrest and conducting a search of the information contained therein at a different time and location to the arrest itself. *Id*.

While *Riley* was decided in the context of the search of cell phones seized pursuant to a lawful arrest, a parallel reasoning can be applied to the search of other types of electronic media seized pursuant to the border search exception, particularly as to the Court's analysis of the technological advancements and privacy interests implicated by modern electronic devices. Indeed, akin to Judge McKeown's analysis in *Cotterman*, the Supreme Court discusses at length the quantitative and qualitative distinctions in cell phones, citing to their "immense storage capacity," the "pervasiveness" of their existence, and ultimately concluding that the "fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Riley*, 2014 WL 2864483. It is axiomatic that the characteristics inherent in modern cell phones, specifically their storage content and gateway to large amounts of personal information and data, should be extended to laptop computers and external hard drives. Accordingly, the fact that *Riley* only addressed the unreasonable search of cell phones should not prevent this Court from applying the same principles to the unlawful forensic search of Defendant's laptop, external hard drive and cell phone.

The case at hand is not a "routine" border search that is envisioned by the warrant exception or prior case law. See generally *Flores-Montano*, 541 U.S. 149; *Arnold*, 533 F.3d 1003. Rather, the blatant actions taken by HSI agents in detaining Defendant's property, subjecting it to forensic imaging and searching its contents unrestrained, is recognizably contrary to the significant privacy interests at play and goes beyond what has been deemed a routine under the border search exception. As held in *Cotterman*:

> [Electronic devices] contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails. This type of material implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers.'

709 F.3d at 964 (citing U.S. Const. amend. IV). Thus, to allow the admission of such evidence would be in direct violation of the privacy concerns recited in *Cotterman*.

In consideration of the requirement of reasonable suspicion held in *Cotterman*, and further supported by comparison to the Supreme Court's decision in *Riley*, the evidence obtained from Defendant's laptop, external hard drive and cell phone, should be deemed the result of an unreasonable search and suppressed in accordance with Fourth Amendment jurisprudence.

CONCLUSION

WHEREFORE, for the above reasons and for any other reasons the Court deems proper, the Defendant respectfully moves this Honorable Court to suppress all evidence which the Government proposes to use against him as a result of the seizure of electronic media at the San Diego Airport on October 5, 2012, and any evidence that flowed therefrom, whether oral, written or otherwise recorded.

Respectfully submitted this 6th day of August, 2014.

Respectfully Submitted

/s James V. Hairgrove_____
James V. Hairgrove
Attorney for Idin Rafiee