WO

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

United States of America, Plaintiff, vs. Daniel David Rigmaiden, Defendant.	No. CR 08-814-PHX-DGC **ORDER**

The government has indicted Defendant Daniel Rigmaiden on 74 counts of mail and wire fraud, aggravated identity theft, and conspiracy. Doc. 200. The charges arise from a scheme to obtain fraudulent tax refunds by filing electronic tax returns in the names of hundreds of deceased persons and third parties. The government located and arrested Defendant, in part, by tracking the location of an aircard connected to a laptop computer that allegedly was used to perpetrate the fraudulent scheme. Defendant argues that the technology and methods used to locate the aircard violated his Fourth Amendment rights. He also argues that the government violated the Fourth Amendment by obtaining various documents and data through Court orders, relying on warrants that lacked particularity and probable cause, and exceeding the scope of the warrants.

Defendant has filed a motion to suppress and many related motions and memoranda.[1]

[1] These include Defendant's Motion to Suppress (Doc. 824); Supplement Memorandum re 4th Amendment Violations (Doc. 830-1); Supplement Memorandum re Destruction of Evidence (Doc. 830-2); Motion for Order Requiring Government to Comply

Although Defendant Rigmaiden represents himself and has no formal training in the law, his motions and memoranda are thoroughly researched and factually detailed. The Court and its staff have read hundreds of pages of briefing and exhibits, and oral argument was held on March 28, 2013. After thorough consideration of the parties' arguments, Defendant's motion to suppress will be denied.

I. Background.

The government alleges that in 2007 and 2008, using the identities of deceased and living individuals, including their social security numbers, Defendant e-filed more than 1,200 fraudulent tax returns claiming more than $3,000,000 in tax refunds. Doc. 873 at 3.[2] In reliance on the fraudulent filings, the IRS deposited hundreds of thousands of dollars in bank accounts and debit cards maintained by Defendant and his co-conspirators. This order will describe only the most relevant portions of the year-long investigation that led to Defendant's arrest.

In June 2007, an IRS e-file provider notified the IRS that a large volume of tax returns had been filed through its website by an unknown person using an automated process. IRS agents subpoenaed the subscriber information for one of the IP addresses from which a return was filed and learned that the IP address was associated with a Verizon Wireless broadband access card provided to a Travis Rupard in San Jose, California. This access card, which was used to make a wireless connection between a computer and the Internet, became a key focus in the investigation. The access card will be referred to in this order as "the aircard."

---

with Data Deletion Requirements (Doc. 847); Motion for Discovery re: Digital Evidence Search (Doc. 890); Motion for Leave to Place Additional Evidence on the Record (Doc. 897); Motion for Leave to File First Supplement to Motion for Order Requiring Government to Comply with Data Deletion Requirements (Doc. 926); Motion to Suppress All Digital Data Evidence as a Sanction for Failure to Preserve Evidence (Doc. 931); Motion for Sanctions for Discovery Violations re: Digital Evidence Search (Doc. 932); Motion to Amend/Correct (Doc. 934).

[2] Citations in this order are to page numbers affixed to the top of documents by the Court's CMECF system, not to pages numbers in the documents themselves.

In March of 2008, the IRS Fraud Detection Center in Austin, Texas ("AFDC") identified a number of recently-filed fraudulent tax returns which directed that refunds be sent to various debit cards connected with a single Meridian Bank account. Doc. 873 at 9-10. IRS agents subpoenaed subscriber information for these fraudulent filings and found that some of the IP addresses ultimately traced back to the Verizon aircard and the related account maintained by Travis Rupard. Investigators also found the name "Travis Rupard" to be a false identity – the aircard account subscriber information provided by "Travis Rupard" listed a non-existent address, and the California driver's license number provided by "Travis Rupard" was in fact assigned to a female with a different name.

On April 15, 2008, as a result of various investigative efforts, agents executed a search warrant on a co-conspirator's computer and obtained e-mail correspondence between the co-conspirator and an individual known to the co-conspirator as "the Hacker." The co-conspirator had never personally met the Hacker, but had communicated with the Hacker by encrypted e-mail and had, at the Hacker's direction, established bank accounts to receive refunds from the fraudulent tax return scheme. Following his arrest, the co-conspirator agreed to work with the government as a confidential informant, and is referred to by the government as "CI-2."

On April 17, 2008, the Hacker contacted CI-2 through a secure e-mail account and provided detailed encrypted instructions for delivering $68,000 in proceeds from the tax-refund scheme to the Hacker. The Hacker directed CI-2 to wash the $68,000 of cash in lantern fuel to avoid drug detection dogs, double vacuum seal the currency, place the sealed cash inside a stuffed animal, and mail the animal in a gift-wrapped box with a birthday card addressed to a dying child. The Hacker instructed CI-2 to send the package to "Patrick Stout" at a FedEx/Kinko's store in Palo Alto, California. Investigators found "Patrick Stout" to be another false identity – it was traced to a post office box in Sacramento, California, opened through the use of a fraudulent California driver's license bearing a number assigned to yet another female with a different name.

The package containing $68,000 in currency was delivered to the FedEx/Kinko's store

on May 6, 2008. The next day, at approximately 5:00 a.m., a white male wearing a dark jacket and hood entered the store, presented identification in the name of Patrick Stout, and retrieved the package. The individual opened the package outside the store, removed the cash, discarded the shipping box, and then proceeded to a nearby train station where he eluded agents who had him under surveillance. The Hacker e-mailed CI-2 on May 8, 2008, and confirmed receipt of the money.

On June 25, 2008, the government obtained Verizon transaction logs for the aircard and compared them with transaction information for other activities of the Hacker, including his e-mail communications with CI-2. The IP addresses accessed by the aircard and the date/time stamps shown for its connections were consistent with activities of the Hacker, suggesting that the Hacker was in fact using the Travis Rupard aircard. In addition, the AFDC reported that more than 100 fraudulent tax refund claims were filed between May 22 and June 5, 2008. Doc. 873 at 16-23. The times when these false filings were made corresponded with activity on the Travis Rupard aircard. Although the false filings were made from different IP addresses, investigators believed the Hacker was using the aircard to access proxy computers or other anonymous tools on the Internet to mask his IP address. Consistent with this theory, the Hacker had stated in an April 15, 2008 e-mail to CI-2 that he used a different IP address for each fraudulent tax return in order to avoid detection. *Id.* at 26. Through these and other investigative efforts, investigators became convinced that the Hacker was using the Travis Rupard aircard and that locating the aircard would lead them to the Hacker.

As discussed in more detail below, in June and July of 2008 the government obtained historical cell-site records from Verizon that reflected communications from the aircard. These cell-site records showed that the aircard communicated regularly with several cell towers in the area of Santa Clara, California. Using the cell-tower information, a map, and various calculations, a government agent was able to narrow the location of the aircard to an area of 6,412,224 square feet, or just under one-quarter of a square mile. Doc. 824-1 at 167. The government obtained an order from a Federal Magistrate Judge in the Northern District

of California that authorized the installation of a pen register and trap and trace device to obtain additional cell site information, and a warrant authorizing the use of a mobile tracking device to communicate with the aircard. On July 16, 2008, agents used this mobile device to track the aircard's location to unit 1122 of the Domicilio apartment complex in Santa Clara. The government then obtained information from the apartment complex indicating that unit 1122 was rented in the name of Steven Travis Brawner. The rental application listed a fake California driver's license bearing a number that belonged to a female with a different name, and the handwriting of "Steve Brawner" on the apartment application was found by a handwriting expert to be similar to the handwriting of "Patrick Stout" on a post office box application. In addition, "Steve Brawner" had provided a fraudulent 2006 tax return when he applied to rent the apartment. Using this and other information generated during the investigation, the government obtained a warrant to search apartment 1122.

To ascertain the arrival and departure habits of the apartment's occupant, agents obtained gate access data from the Domicilio apartment's alarm company. This information showed when the occupant of unit 1122 used his fob to enter or leave the complex. Agents conducted surveillance of the apartment through the rest of July 2008 without observing the occupant. On the night of July 22, 2008, an undercover FBI agent used the ruse of a fast food delivery to knock on the apartment's door, but nobody answered.

Finally, on August 3, 2012, at approximately 4:15 p.m., agents observed a person matching the description of Steven Brawner walking near the apartment. The person began to act suspiciously when he saw the agents, and then began running to evade the agents. After a foot chase through the surrounding area, Defendant was apprehended by local police officers who happened to be on the scene. Agents searched the suspect incident to his arrest and found a set of keys in his pocket. An agent took the keys to unit 1122 and confirmed that they fit and turned the door lock. The agent waited for the arrival of other agents with the search warrant before entering the apartment.

Once in the apartment, agents found identification bearing the suspect's photograph and the name Patrick Stout, along with many of the pre-recorded $100 bills that were part

of the $68,000 delivery in May. Agents also found the aircard, a laptop computer, and computer storage devices that eventually were found to contain much incriminating evidence. Fingerprints identified the suspect as Defendant Daniel Rigmaiden.

Following his arrest and indictment in this case, Defendant elected to represent himself after he became dissatisfied with five successive defense attorneys. Defendant sought extensive discovery from the government, including detailed discovery about the nature and operation of the mobile tracking device used to locate the aircard. The Court held several hearings, received substantial briefing, and ultimately concluded that some information regarding the mobile tracking device was protected by the qualified law enforcement privilege recognized in *Roviaro v. United States*, 353 U.S. 53 (1957). Doc. 723. The Court also concluded, however, that Defendant was fully able to make his Fourth Amendment arguments in light of the extensive disclosures provided by the government, detailed stipulations of fact agreed to by the government, and information Defendant was able to obtain through his own investigations with the aid of investigators, legal assistants, and a laptop computer provided by the Court. *Id.* Having now read Defendant's 355 -page motion to suppress, and having reviewed his thousands of pages of supporting materials, the Court confirms this conclusion. Defendant has been placed at no disadvantage by the government's withholding of sensitive law enforcement information. Unless otherwise specified in this order, the Court will assume that Defendant's factual assertions are true.

II. Discussion.

Defendant's motion to suppress and related memoranda and motions (*see* footnote 1) contain a highly detailed and granular statement of his arguments. Defendant divides the government's actions into 21 different searches and provides detailed explanations as to how they functioned, why they were covered by the Fourth Amendment, and why they were not authorized by the orders and warrants obtained by the government. The Court has reviewed these many arguments individually, but will not attempt to address them separately in this written order. The Court instead will use the following categories to address Defendant's challenges and the government's responses: whether Defendant had a legitimate expectation

of privacy in the location of the aircard; the government's collection of historical cell-site information, destination IP addresses, and data from the Domicilio apartment's alarm company; the search for the aircard using the mobile tracking device; the searches of Defendant's apartment and computer; and whether the Fourth Amendment's good faith exception applies.

A. Legitimate Expectation of Privacy.

To invoke the protections of the Fourth Amendment, a defendant must have a legitimate expectation of privacy in the place searched. *Rakas v. Illinois*, 439 U.S. 128, 143 (1978). The "legitimate expectation of privacy" inquiry has two components. *See Smith v. Maryland*, 442 U.S. 735, 740–41 (1979); *Katz v. United States*, 389 U.S. 347, 361 (1967); *United States v. Bautista*, 362 F.3d 584, 589 (9th Cir. 2004). First, the court considers whether the defendant has exhibited an actual, subjective expectation of privacy. *Smith*, 442 U.S. at 740. Second, the court must determine whether the defendant's subjective expectation of privacy is "one that society is prepared to recognize as reasonable." *Id.* at 740-41. The defendant bears the burden of demonstrating a reasonable expectation of privacy. *United States v. Caymen*, 404 F.3d 1196, 1199 (9th Cir. 2005) (citing *Rakas*, 439 U.S. at 131); *see United States v. Johnson*, 584 F.3d 995, 998 (10th Cir. 2009). Whether a defendant's expectation of privacy was objectively reasonable is a question of law. *United States v. Nerber*, 222 F.3d 597, 599 (9th Cir. 2000).

Defendant argues that he had a subjective expectation of privacy in the aircard, the computer, and apartment 1122. *See* Doc. 824 at 203–05. Defendant apparently lived alone, kept the apartment locked and the shades drawn, and used the aircard and laptop solely within the apartment. It also is true, however, that Defendant was prepared to abandon the apartment on a moment's notice. As Defendant candidly admits in his motion to suppress:

> Had the government served the defendant with a copy of the N.D.Cal. 08-90330MISC-RS order – i.e., within the 18 day period after the aircard had been located but before the in-person search of apartment No. 1122 – the defendant would have not only stopped using the aircard but he would have also packed up his belongings and permanently moved from apartment No. 1122. In other words, had the defendant been served with a copy of the order and receipt, there would have been nothing for the government to seize from

> apartment No. 1122 during the in-person search on August 3, 2008, as well as nobody for the government to arrest.

Doc. 824-1 at 321-22 (footnote omitted). The government also asserted during oral argument, without contradiction from Defendant, that Defendant's rented storage unit was found to contain $70,000 in cash, a United States passport issued to Defendant in the name of Andrew Johnson (a deceased individual), and a computer with back-up information from Defendant's laptop, all apparently awaiting a quick departure. Given Defendant's preparations to flee and his admission that he would have done so had he learned of the government's investigation, it could be argued that Defendant had already formed an intent to abandon his aircard, computer, and apartment. But even if Defendant had a subjective expectation of privacy in these items, the Court cannot conclude that his expectation is one society should be prepared to recognize as objectively reasonable. *Id.*

Defendant purchased the aircard in May of 2006 using the name of a living person, Travis Rupard. Doc. 873 at 35-36. He used Mr. Rupard's actual Social Security Number to support the false identity, and maintained the Verizon wireless account in that name. *Id.* Defendant used the name of Andrew Johnson, a deceased individual, to purchase the laptop computer he used with the aircard. *Id.* He used a fraudulent Visa card in Johnson's name to purchase the computer, and procured the Visa card by using Johnson's Social Security Number. *Id.* The Ninth Circuit has held that a defendant does not have a reasonable expectation of privacy in computer equipment obtained through fraud. *Caymen*, 404 F.3d at 1196.

Defendant also lacked an objectively reasonable expectation of privacy in apartment 1122. Defendant sought to hide under many layers of false identities. In addition to purchasing the aircard, opening the aircard account, and purchasing the laptop computer with the names of Travis Rupard and Andrew Johnson, Defendant rented apartment 1122 in the name of Steven Travis Brawner, a deceased individual. *Id.* at 36. Defendant provided a forged California driver's license in Brawner's name, along with a driver's licence number assigned to a living female. *Id.* He also provided a fraudulent 2006 tax return in Brawner's

name, using Brawner's Social Security Number. *Id.* Defendant rented a storage unit using the identity of Daniel Aldrich, a deceased person, with a fraudulent driver's license number assigned to another living person. *Id.* at 29. Defendant used the name of Patrick Stout when he rented a safety deposit box and collected proceeds of the fraudulent tax scheme, used yet another person's driver's license number in connection with the Stout identification, and filed a false tax return in Mr. Stout's name. *Id.* at 8, 30. The indictment alleges that Defendant used the aircard and the laptop computer to file hundreds of false tax returns using the names of hundreds of deceased individuals. Doc. 200.

"The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities." *United States v. Jacobsen*, 466 U.S. 109, 122 (1984). The Supreme Court has illustrated this principle with the example of a "burglar plying his trade in a summer cabin during the off season." *Rakas*, 439 U.S. at 143 n.12. The burglar "may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as 'legitimate.'" *Id.* Because the burglar's "presence . . . is 'wrongful,' his expectation of privacy is not one that society is prepared to recognize as 'reasonable.'" *Id.* (citations omitted).

The Court concludes that Defendant's presence in the apartment was wrongful in the same sense as the burglar's discussed in *Rakas*. Virtually everything about Defendant's actions related to the apartment was fraudulent. Defendant rented the apartment using the name of a deceased individual, provided a forged California driver's license to support the false identity, used the driver's license number from another person in support of the forged license, and provided a forged tax return to support his purported ability to pay rent. Defendant used the laptop he had procured through fraud in the apartment, and connected to the Internet with the aircard purchased with a false identity while using the account with Verizon that he maintained using a false identity. Even the electricity that lighted the apartment and powered the computer and aircard was purchased in a false name. What is more, while living in the apartment under false pretenses, Defendant had $70,000 in cash,

a false passport, and a copy of his laptop computer in a storage unit (also rented under false pretenses) ready for a quick escape.

One who so thoroughly immerses himself in layers of false identities should not later be heard to argue that society must recognize as legitimate his expectation of privacy in the location and implements of his fraud. The Court concludes that Defendant's presence in apartment 1122 was akin to the "burglar plying his trade in a summer cabin during the off season." *Rakas*, 439 U.S. at 143 n.12. Defendant did not have an expectation of privacy society is willing to accept as legitimate.

Defendant relies on *United States v. Bautista*, 362 F.3d 584 (9th Cir. 2004), to argue that he had a legitimate expectation of privacy in the apartment. In *Bautista*, the defendant paid for a motel room with a stolen credit card. The Ninth Circuit found that the defendant nonetheless maintained Fourth Amendment protection in the room because his occupancy had not been lawfully terminated by the motel at the time of the search. *Id.* at 586, 590. The Court finds *Bautista* distinguishable for several reasons. First, the defendant in *Bautista* rented the room in his own name. *Id.* at 586. Second, the Ninth Circuit noted, at least twice, that the motel manager would have permitted the defendant to remain in the room, even after his use of the stolen credit card, if the defendant simply had provided another means of payment. *Id.* at 587, 590. Third, law enforcement officers conducted no investigation of the defendant's use of the stolen credit card before entering the room and had no probable cause to believe he had engaged in any criminal activity. *Id.* at 590, 591.

The Ninth Circuit's decision in *United States v. Cunag*, 386 F.3d 888 (9th Cir. 2004), is more relevant. Mr. Cunag used false information to rent a hotel room, including his co-defendant's name, a false phone number, address, and employer name, and forged documents related to the credit card of another. *Id.* at 889. Using the Supreme Court's burglar example from *Rakas*, the Ninth Circuit found that Cunag had no legitimate expectation of privacy in the hotel room:

> Like the burglar, Cunag unlawfully gained entry to the premises. Like the burglar, he hoped and believed he might not get caught. But, like the burglar, those hopes and beliefs do not give rise to a legitimate expectation of privacy

that society is willing to recognize.

Id. at 894. Referring to the Supreme Court statement in *Rakas* that a thief has no reasonable expectation of privacy in an automobile he has stolen, the Ninth Circuit further held that "Cunag procured his room through deliberate and calculated fraud. Like the driver of the stolen car, Cunag was not a lawful occupant." *Id.* Citing *Rakas*, the Ninth Circuit noted that "when an individual is not legitimately on the premises, he does not enjoy the protection afforded by the Fourth Amendment." *Id.* at 893.

Cunag also cited *Bautista* and its holding that one who procures a hotel room by fraud does have a reasonable expectation of privacy so long as the hotel has not taken affirmative steps to evict him. *Id.* at 895. But because the Ninth Circuit had already concluded, under Supreme Court precedent, that Cunag was not lawfully in the room and therefore had no legitimate expectation of privacy, the Court regards this portion of *Cunag* as dicta. Moreover, as noted above, the Court finds *Bautista* distinguishable from this case.

The Court's conclusion that Defendant did not have a legitimate expectation of privacy in his apartment is also supported by the Ninth Circuit's decision in *Caymen*, 404 F.3d 1196, which upheld the search of a computer obtained through fraudulent use of a credit card. The Ninth Circuit concluded that "[t]he Fourth Amendment does not protect a defendant from a warrantless search of property that he stole, because regardless of whether he expects to maintain privacy in the contents of the stolen property, such an expectation is not one that 'society is prepared to accept as reasonable.'" *Id.* at 1201 (citing *Smith*, 442 U.S. at 740). The Ninth Circuit noted that there is "no ground on which to distinguish property obtained by fraud from property that was stolen by robbery or trespass." *Id.*

The Court's conclusion is also supported by Judge O'Scannlain's concurrence in *United Sates v. Lozano*, 623 F.3d 1055 (9th Cir. 2010) (per curiam). In *Lozano*, the court ruled that postal inspectors had reasonable suspicion to detain a package later found to contain marijuana. Judge O'Scannlain would also have ruled that the defendant had no right of privacy in the package because it was addressed to his house under a false name. *Id.* at 1064. Judge O'Scannlain noted a split of authority in cases involving defendants with

"publicly-established connections to their alter ego," *id.* at 1064, but concluded that the "better reasoned position" is set forth in cases where "the judges doubted that a defendant had a legitimate expectation of privacy in mail addressed to his public alias when that alias was used solely in a criminal scheme." *Id.* "That conclusion better accords with the principle expressed by the Supreme Court in *Jacobsen* that 'wrongful' interests do not give rise to legitimate expectations of privacy." *Id.*

Other courts have reached similar conclusions. *See, e.g., United States v. Johnson*, 584 F.3d 995 (10th Cir. 2009) (defendant had no reasonable expectation of privacy in storage unit rented in the name of another using the other person's stolen credit card); *United States v. Daniel*, 982 F.2d 146, 149 (5th Cir. 1993) (concluding that "even if we accept the Government's assertion that 'Lynn Neal' was Daniel's alias, we still question whether Daniel would have Fourth Amendment 'standing' to assert the claim, particularly when the use of that alias was obviously part of his criminal scheme"); *United States v. Lewis*, 738 F.2d 916, 919-20 n.2 (8th Cir. 1984) (explaining that "[t]he opening of the tax bill addressed to [Lewis' alias] and not to Lewis cannot be said to have infringed *his* reasonable privacy expectations" and that a "mailbox bearing a false name . . . used only to receive fraudulently obtained mailings does not permit an expectation of privacy that society is prepared to recognize as reasonable"); *United States v. Davis*, No. 10-339-HA, 2011 WL 2036463, at *2-3 (D.Or. May 24, 2011) (explaining that "although an individual may have a subjective expectation of privacy in property that is attached to a fictitious name, that is not a privacy interest that society recognizes as reasonable"); *United States v. DiMaggio*, 744 F.Supp. 43, 46 (N.D.N.Y. 1990) (holding that when an individual withholds his true identity "he has effectively repudiated any connection or interest in the item vis-a-vis society"); *United States v. Suarez-Blanca*, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *6–7 (N.D.Ga. Apr. 21, 2008) ("The subscriber name indicates that [the defendant] either was trying to distance himself from the cell phone or had no interest in the cell phone. As such, the use of a fictitious name or names of a third party indicates that [the defendant] does not have a privacy interest in the phones."); *United States v. Skinner*, No. 3:06-CR-100, 2007 WL

1556596, at *15–17 (E.D.Tenn. May 24, 2007) (the defendant had no reasonable expectation of privacy in cell phone records where he was not the legitimate subscriber to the phone. The court noted that "[w]hen a defendant uses a fictitious name as part of his criminal scheme, whether the defendant has 'standing' to assert a Fourth Amendment violation is questionable.").

Given the unique circumstances of this case and the case law discussed above, the Court concludes that Defendant did not have a legitimate expectation of privacy in the aircard, laptop, or apartment procured through fraud. Defendant acquired these items by invading the privacy of the persons from whom he stole names, social security numbers, credit cards, and driver's license numbers. Having utterly disregarded the privacy rights of Travis Rupard, Steven Brawner, and Andrew Johnson, not to mention the many other names used in his scheme, Defendant cannot now credibly argue that he had a legitimate expectation of privacy in the devices and apartment he acquired through the fraudulent use of their identities.

This conclusion is strengthened when one considers the nature of the intrusion used to locate the aircard. In *Nerber*, the Ninth Circuit explained that "the legitimacy of a citizen's expectation of privacy in a particular place may be affected by the nature of the intrusion that occurs." 222 F.3d at 601. The intrusion that allowed agents to locate the aircard – using a mobile tracking device to send signals to and receive signals from the aircard – was not a "severe intrusion." *Id*. at 602; *see id.* at 603 (noting that hidden video surveillance is a severe intrusion). The evidence in this case suggests that Defendant used the aircard and laptop computer to perpetrate an extensive scheme of fraud through electronic communications. The Court cannot conclude that the government's corresponding use of electronic communications to find the aircard violated any legitimate expectation of privacy.

In summary, under the totality of the unique circumstances in this case, the Court finds that Defendant did not have an objectively reasonable expectation of privacy in the aircard, computer, or apartment. As a result, no Fourth Amendment violation occurred when

the government searched for and located the aircard in his apartment.[3]

B. Collection of Historical Records.

Even if Defendant had a protected privacy interest in the location of the aircard, the search for the aircard did not violate his rights. Defendant argues that the government violated the Fourth Amendment by obtaining various historical records. The government responds that the records were properly obtained pursuant to an order under the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(c). The government also contends that the "third party doctrine" deprives Defendant of any privacy right in the records.

On July 9, 2008, Arizona Magistrate Judge Lawrence O. Anderson issued an order pursuant to 18 U.S.C. § 2703(d) requiring Verizon Wireless to turn over destination IP addresses associated with the aircard. *See* Doc. 576-2. On July 10, 2008, Judge Anderson issued an order requiring Verizon to turn over the aircard's historical cell-site, sector, and distance information for the previous 30 days. *See* Doc. 576-4. On July 16, 2008, Arizona Magistrate Judge Edward C. Voss issued a similar order for additional records covering July 11-18, 2008. *See* Doc. 576-6. Verizon provided the requested information, including 1.8 million destination IP addresses that had been accessed by the aircard. The orders signed by Judges Anderson and Voss will be referred to herein as "the SCA Orders."[4]

---

[3] Citing *Lavan v. City of Los Angeles*, 693 F.3d 1022 (9th Cit. 2012), Defendant asserted at oral argument that he need not show a reasonable expectation of privacy to make out a Fourth Amendment violation because the Fourth Amendment also protects property interests, and he had a property interest in his apartment, laptop, and aircard. *Lavan* did not concern a search, but instead concerned the City's seizure and destruction of personal property belonging to homeless people that was left on City sidewalks. In addition, for the reasons discussed above, the Court cannot conclude that Defendant had a legitimate Fourth Amendment property interest in the apartment, laptop, or aircard procured through fraud.

[4] On June 6 and 16, 2008, the government served grand jury subpoenas issued under § 2703 on Verizon Wireless. *See* Doc. 576-1. After learning that information concerning destination IP addresses could be obtained only under a § 2703(d) order, the government obtained a retroactive order from Judge Anderson. *Id.* Defendant does not argue the order was invalid because information previously had been obtained by subpoena.

1. Stored Communications Act.

The SCA authorizes the government to "require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service" if the government obtains a court order for such information. 18 U.S.C. § 2703(c)(1)(B). Subsection (d) provides that the court order shall issue only if "the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).

Verizon clearly is a "provider of electronic communication service" within the meaning of the SCA, and the historical cell site information and destination IP addresses clearly constitute "a record or other information pertaining to a subscriber or customer of such service." *Id.* Judges Anderson and Voss each found that the government had made the showing required by the SCA: "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* Disclosure of the historical cell site information and destination IP addresses was thus authorized by the SCA.

In addition, even if the SCA had been violated in some respect, Defendant's motion to suppress would be denied. Suppression is not an available remedy for violations of the SCA. *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) ("[T]he Stored Communications Act does not provide an exclusion remedy. It allows for civil damages . . . and criminal punishment . . . but nothing more.") (citations omitted); *see United States v. Jones*, --- F.Supp.2d ----, 2012 WL 6443136, at *4 (D.D.C. 2012) (same).[5]

2. Apartment Access Data.

The government obtained data from the apartment's security system showing when the occupant of unit 1122 had entered and exited the complex in the weeks before the aircard

[5] Defendant also argues that the SCA Orders lacked particularity, but cites no authority to suggest that the SCA includes a particularity requirement.

was located. This information was obtained in response to Arizona Grand Jury Subpoena No. 07-03-709, served on Quality Alarm, the company that operated the security system. The data was produced to the government after being extracted by a Quality Alarm employee from access equipment at the complex.

Rule 17(c)(1) of the Federal Rules of Criminal Procedure provides that a subpoena may require "a witness to produce any books, papers, documents, data, or other objects the subpoena designates." Entry and access data from the apartment's security system constitute "data" within the meaning of this rule. The government was thus authorized by Rule 17 to obtain the apartment access information.

3. Third-Party Doctrine.

In *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court recognized the "third-party doctrine." That doctrine holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-44; *see also Miller*, 425 U.S. at 442-44. In *Miller*, the Supreme Court found that a bank customer had no reasonable expectation of privacy in financial information he voluntarily conveyed to the bank for use in the ordinary course of its business. 425 U.S. at 442. In *Smith*, the Supreme Court similarly held that the defendant did not have a reasonable expectation of privacy in numbers he dialed from his telephone because he voluntarily conveyed that information to the telephone company when he placed calls. 442 U.S. at 742-45.

Defendant argues that the third-party doctrine does not apply to the historical cell-site information and destination IP addresses obtained from Verizon or to his exit and entry data obtained from Quality Alarm. He asserts that this information does not constitute routine business records because Verizon was not a party to his communications and Quality Alarm was not a party to his entry and exit of the apartment complex. Doc. 824 at 218. He further contends that he did not knowingly and voluntarily convey this information to either Verizon or Quality Alarm. *Id.* at 221.

The Court finds the government's response to this argument persuasive:

> The reasoning of *Miller* applies to the historical records obtained by the United States. They are not the customer's private papers. Once a customer makes a call, communicates over the Internet, leases an apartment, or uses the services of an alarm company, he has no control over the business record made by the business of that transaction. Instead, the record created is a business record of the provider. The choice to create and store the record is made by the provider, and the provider controls the format, content, and duration of the records it chooses to create and retain. . . . Moreover, these records pertain to transactions to which the companies were a participant. The assignment of a particular cell tower to process a call is made by the cell phone company to facilitate the functioning of its network; the ISP uses the IP address to route Internet communications it transmits; the rental company maintains a rental file for each occupant; and an alarm service independently maintains records of the equipment it installs and maintains. Thus, under *Miller*, the business records obtained by the government are not protected by the Fourth Amendment.

Doc. 873 at 41.

Courts have rejected Defendant's arguments that historical cell-site records cannot be obtained under the SCA. *See, e.g., In re Application of U.S.*, 620 F.3d 304, 313 (3rd Cir. 2010) (holding that cell-site location information "is obtainable under a § 2703(d) order"); *United States v. Graham*, 846 F.Supp.2d 384, 396 (D. Md. 2012) ("It is well established that Section 2703(c)(1)(B) of the Stored Communications Act applies to historical cell-site location data."); *see also United States v. Skinner*, 690 F.3d 772, 777 (6th Cir. 2012) (holding that locating defendant through a phone's cell-site records is not a Fourth Amendment search). Contrary to Defendant's arguments, federal courts consistently rely on *Smith* and *Miller* to hold that defendants have no reasonable expectation of privacy in historical cell-site data because the defendants voluntarily convey their location information to the cell phone company when they initiate a call and transmit their signal to a nearby cell tower, and because the companies maintain that information in the ordinary course of business. *See United States v. Ruby*, No. 12CR1073 WHQ, 2013 WL 544888, at *6 (S.D.Cal. February 12, 2013); *Jones*, 2012 WL 6443136, at *5 (D.D.C. 2012); *Graham*, 846 F.Supp.2d at 397-401; *United States v. Madison*, No. 11-60285-CR, 2012 WL 3095357, at * 8-9 (S.D.Fla. July 30, 2012).

Defendant argues that the government was able to use the cell-site information to effectively track his aircard from June 10 to July 18, 2008, a period of 38 days, and that this

"prolonged surveillance" implicated his reasonable expectation of privacy. Doc. 824 at 215-17. Defendant relies on *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), and *United States v. Jones*, 132 S.Ct. 945 (2012), but those decisions are inapposite. They do not address orders under the SCA, and the Supreme Court in *Jones* did not adopt the privacy theory advanced by Defendant.

Maynard found that a Fourth Amendment search occurred when agents conducted prolonged surveillance of the defendant's vehicle – 24 hours a day for 28 days – through the use of a GPS tracking device attached to the vehicle without a valid warrant. 615 F.3d at 558-63. The court acknowledged that the government could have physically followed the defendant's vehicle without violating the Fourth Amendment, but found that use of a GPS device to track the defendant's movements over an extended period of time violated his reasonable expectation of privacy. *Id.* at 563. According to the court, this prolonged surveillance revealed an "intimate picture" of the defendant's life. *Id.* at 562.

In this case, a government agent, working in his office with the historical cell-site information and using mathematical and triangulation techniques, was able to calculate a general location for Defendant's aircard during a 38-day period. The calculation narrowed the location of the aircard to one-quarter of a square mile. The Court cannot conclude that such use of cell-site information, obtained from a third party under the SCA, is tantamount to attaching a GPS device to a person's vehicle. Calculations made from the historical cell-site information did not provide minute-by-minute intelligence on Defendant's precise movements as did the GPS device in *Maynard*. The calculations merely identified a general area where the aircard was located – and stationary – for 38 days. The information was not used surreptitiously to track Defendant's movements over an extended period without a warrant.

In *Jones*, which also concerned a GPS tracking device installed on the defendant's vehicle, the Supreme Court found a Fourth Amendment violation. The majority based its ruling on the fact that agents physically intruded on the defendant's property for the purpose of obtaining information. 132 S.Ct. at 949. The opinion declined to address whether

monitoring the vehicle with the GPS device violated the defendant's expectation of privacy. *Id.* at 953-54. Justice Alito criticized the majority's trespass analysis and suggested, consistent with *Maynard*, that the duration of the surveillance is a principal consideration in determining whether a Fourth Amendment search occurred. *Id.* at 964 (Alito, J., concurring). For reasons explained above, the use of historical cell-site information in this case is not the same as use of the GPS device in *Jones*.

The history of the *Jones* case on remand is also instructive. Mr. Jones moved in the trial court to suppress cell-site information. *Jones*, 2012 WL 6443136, at *1-2. The cell-site records had been obtained pursuant to three orders issued by a magistrate judge under the SCA, and covered a period of four months. In denying the motion to suppress, the district court explained that "this Court knows of no federal court that has held that the use of prospective cell-site records constitutes a search under the Fourth Amendment, or of any federal court that has suppressed any type of cell-site data obtained pursuant to a court order under the SCA." *Id.*, at *7; *see also Graham*, 846 F.Supp.2d at 397-403 (denying motion to suppress cell-site information and finding mosaic theory "problematic"). The same is true for the cell-site records in this case.[6]

The Court also finds that the third-party doctrine applies to Defendant's destination IP addresses. Defendant had no legitimate expectation of privacy in the addresses of e-mail messages sent from his laptop because such information was conveyed to the third party Internet service provider. As the Ninth Circuit explained in *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), "Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the

[6] Defendant also argues that the agent's use of the historical cell-site information to calculate the general location of the aircard was itself a warrantless search. The Court concludes, however, that the government's in-office analysis of cell-site information obtained lawfully under the SCA can by no means be categorized as a search subject to the Fourth Amendment.

specific purpose of directing the routing of information." *See also United States v Bynum*, 604 F.3d 161 (4th Cir. 2010) (no privacy interest in internet subscriber information); *United States v. Qing Li*, 2008 WL 789899, *4-5 (S.D.Cal. 2008) (Fourth Amendment does not bar government from obtaining destination IP addresses under the SCA).

Nor did the government violate Defendant's Fourth Amendment rights by the volume of IP addresses it obtained. Defendant notes that the government obtained 1.8 million IP addresses from Verizon, and argues that the government should have tailored its request more narrowly and obtained only those IP address it had already connected to the tax-refund scheme. Because obtaining IP addresses is akin to obtaining telephone numbers, an act that does not implicate the Fourth Amendment at all, *Forrester*, 512 F.3d at 510–11, the Court cannot conclude that the government was required to narrowly tailor its request. Moreover, *Forrester* specifically held that there is "no difference of constitutional magnitude" between obtaining IP addresses and learning the total volume of communications with such addresses, holding that the government's monitoring of "the total volume of data transmitted to and from [the defendant's] account" did not violate the Fourth Amendment. *Id.* at 511. If the government can obtain destination IP addresses and the total volume of such communications without implicating the Fourth Amendment, the Court cannot conclude that the government somehow violated the Fourth Amendment when it obtained 1.8 million IP addresses accessed by Defendant's computer. Moreover, the SCA Order that authorized disclosure of the IP addresses was limited as to time, seeking only those addresses accessed by the aircard between March 1 and July 9, 2008. Doc. 576-2. During this period, AFDC found that more than 100 false tax returns had been filed, many with connections to the aircard. Obtaining all IP addresses accessed by the aircard during this limited time was reasonably calculated to assist the government in understanding the scale and workings of the tax-refund scheme.

Data retained by Quality Alarm regarding Defendant's access to the apartment complex falls under the same analysis. When Defendant entered a gate or door at the complex he voluntarily provided identifying information about himself through use of the fob issued by the alarm company. He did so to gain access, and the alarm company used the

information to grant access. The fact that this transaction between Defendant and the alarm company was recorded in data retained by the alarm company would come as no surprise to anyone even passingly familiar with modern electronic systems. And just as a computer user provides an IP address to an Internet service provider to obtain access to a website, Defendant provided information to the alarm company to gain access to the apartment complex. The Ninth Circuit has found no reasonable expectation of privacy in the first scenario, and the Court finds none in the second.

In summary, the Court concludes that the government's collection of historical cell-site information and destination IP addresses was authorized by the SCA, and that its collection of data from Quality Alarm was authorized by Rule 17 of the Federal Rules of Criminal Procedure. The Court also concludes that the third-party doctrine applies to this information and Defendant therefore had no reasonable expectation of privacy in it.

C. Mobile Tracking Device Search for the Aircard.

Defendant claims that use of the mobile tracking device to locate his aircard violated the Fourth Amendment. The government argues that it obtained a warrant to use the tracking device. Defendant contends that the warrant was deficient and that the government exceeded its scope when carrying out the investigation. The ACLU has filed an amicus brief making similar arguments in support of Defendant's motion to suppress. Doc. 920.

1. Facts.

On July 11, 2008, the government obtained order CR-08-90330 (the "Tracking Warrant") from United States Magistrate Judge Richard Seeborg of the Northern District of California. Doc. 470-1 at 28. The Tracking Warrant was issued under Rule 41(b) of the Federal Rules of Criminal Procedure and other statutes. *Id.* Judge Seeborg found that the application for the warrant established "probable cause to believe that the use and monitoring of a mobile tracking device" would "lead to evidence of" several specific crimes, including conspiracy to defraud the government, fraud relating to identity information, aggravated identity theft, and wire fraud, "as well as to the identification of individuals who are engaged in the commission of these offenses." *Id.* at 29. This finding was based on a 17-page

affidavit signed by FBI Special Agent William Ng. *Id.* at 10-17.

The Tracking Warrant precisely identifies the aircard to be located as "the Verizon Wireless broadband access card/cellular telephone assigned Telephone Number (415) 264-9596 and Electronic Serial Number (ESN) 005-00717190." *Id.* at 1. The warrant limited the duration of the authorized tracking to "a period not to exceed thirty (30) days," and ordered that monitoring of transmissions related to the aircard were "limited to transmissions needed to ascertain the physical location of [the aircard]." *Id.* at 2, 3.

Defendant raises several challenges to the Tracking Warrant. He asserts, among other arguments, that the warrant is not supported by probable cause, that it lacks particularity, that the government's searches and seizures exceeded the warrant's scope, and that agents executed the warrant unreasonably because they failed to comply with inventory and return requirements. Doc. 824-1 at 288-311. In its amicus brief, the ACLU argues that the search exceeded the scope of the warrant because the warrant authorized Verizon, not the government, to locate the aircard, and that the warrant was misleading and incomplete because it failed adequately to describe the technology involved in the search. Doc. 920.

As noted above, the government has stipulated to several specific facts for purposes of this order. *See* Doc. 723 at 13–14. The Court accordingly will assume these facts to be true:

- The mobile tracking device used by the FBI to locate the aircard functions as a cell-site simulator. The device mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard.
- The FBI used the device in multiple locations. The FBI analyzed signals exchanged between the mobile tracking device and the aircard. The FBI would take a reading, move to a new location, take another reading, move to another location, etc. The FBI never used more than a single piece of equipment at any given time.
- The device was used by government agents on foot within Defendant's apartment complex.

- The device generated real time data during the tracking process.
- All data generated by the mobile tracking device and received from Verizon as part of the locating mission was destroyed shortly after Defendant's arrest on August 3, 2008.
- The device used to simulate a Verizon cell tower is physically separate from the pen register trap and trace device used to collect information from Verizon.
- Signals sent by the mobile tracking device to the aircard are signals that would not have been sent to the aircard in the normal course of Verizon's operation of its cell towers.
- The mobile tracking device caused a brief disruption in service to the aircard.
- During the tracking operation, the FBI placed telephone calls to the aircard.
- The tracking operation was a Fourth Amendment search and seizure.
- The government will rely solely on the Tracking Warrant to authorize the use of equipment to communicate directly with Defendant's aircard and determine its location. The government will rely on a separate order (CR08-90331-MISC-RS) to justify obtaining cell-site and other non-content information from Verizon, but will base its defense of the use of the mobile tracking device solely on the Tracking Warrant.
- At the conclusion of the July 16, 2008, search efforts, the mobile tracking device had located the aircard precisely within Defendant's apartment.

With these assumed facts in mind, the Court will turn to an analysis of arguments made by Defendant and the ACLU.

2. Probable Cause.

Defendant argues that the actions authorized by the Tracking Warrant "were not supported by an applicable finding of probable cause." Doc. 824 at 301. As noted above, however, Judge Seeborg specifically found "probable cause to believe that the use and monitoring of a mobile tracking device for the [aircard] will lead to evidence of" several specific crimes and "to the identification of individuals who are engaged in the commission

of these offenses." Doc. 470-1 at 29.

To establish probable cause for a search warrant, the government need only show "a fair probability that contraband or evidence of a crime will be found." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The Court reviews Judge Seeborg's probable cause finding with deference, asking only whether he had a "substantial basis" for the probable cause determination. *Id.* at 238-29 *see also Ewing v. City of Stockton*, 588 F.3d 1218, 1223 (9th Cir. 2009) (issuance of a search warrant is upheld "if the issuing judge 'had a substantial basis' for concluding [that] probable cause existed based on the totality of the circumstances"); *United States v. Gil*, 58 F.3d 1414, 1418 (9th Cir. 1995) (magistrate judge's determination of probable cause is accorded significant deference).

Special Agent Ng's affidavit supports Judge Seeborg's probable cause determination. Doc. 470-1 at 10-17. The affidavit describes the fraudulent tax-refund scheme in detail (*id.*, ¶¶ 3-21), how it was connected to the Hacker (referred to in the affidavit as the "Target Subject") (*id.*, ¶¶ 13-21), various confidential informant contacts with the Target Subject that confirmed his direct involvement in the fraudulent tax-refund scheme (*id.*), the Target Subject's receipt of funds from the scheme (*id.*, ¶¶ 22-30), and that the scheme and some of its fraudulent refund filings were connected to the aircard (referred to in the affidavit as the "Target Broadband Access Card/Cellular Telephone") (*id.*, ¶¶ 1, 34, 42). The affidavit clearly establishes a "fair probability" that locating the aircard would lead to evidence of a crime. Judge Seeborg's probable cause finding satisfies the Fourth Amendment. *See Dalia v. United States*, 441 U.S. 238, 255 (1979).

Defendant disputes the language of the Tracking Warrant, arguing that Judge Seeborg's probable cause finding applied only to information provided by Verizon and not to locating the aircard. But Judge Seeborg's expressly found "probable cause to believe that the use and monitoring of a mobile tracking device for the [aircard]" would lead to evidence of various crimes. Doc. 470-1 at 29.

Defendant also argues that the phrase "mobile tracking device" describes a device attached to a vehicle and not the device used by agents to locate the aircard. The Court

concludes, however, that "mobile tracking device" is a reasonable description of the mobile device used by the government to track the aircard. The Tracking Warrant authorized "the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone," while "the agents are stationed in a public location and the Target Broadband Access Card/Cellular Telephone is . . . inside private residences, garages, and/or other locations not open to the public or visual surveillance[.]" *Id.* at 28-29. The affidavit of Agent Ng stated that the mobile tracking device would monitor the aircard and would "ultimately generate a signal that fixes the geographic position of the [aircard]." *Id.* at 26. These statements foreclose any possible confusion that the device was to be attached to a vehicle.

3. Particularity.

Defendant argues that the search exceeded the scope of the warrant because the warrant did not specifically authorize the FBI to use a cell-site simulator. He also argues that the warrant's reference to a "mobile tracking device," its description of the place to be searched, and its use of the phrase "all data, information, facilities, and technical assistance" lack particularity. The government counters that the warrant was not required to provide greater specificity concerning the methods by which the aircard was to be located.

There is no legal requirement that a search warrant specify the precise manner in which the search is to be executed. *Dalia*, 441 U.S. at 257; *see Maryland v. Garrison*, 480 U.S. 79, 84 (1987). "The Fourth Amendment . . . does not set forth some general 'particularity requirement.' It specifies only two matters that must be 'particularly describ[ed] in the warrant: 'the place to be searched' and 'the persons or things to be seized.'" *United States v. Grubbs*, 547 U.S. 90, 97 (2006) (citing *Dalia*, 441 U.S. at 257).

Dalia involved a warrant that authorized the placement of a hidden listening device in the defendant's office, but did not specify that the police would break into the office to install the device. 441 U.S. at 254-56. The Supreme Court rejected the particularity challenge, holding that authorization of the break-in was not necessary because nothing in the Fourth Amendment requires search warrants to "include a specification of the precise

manner in which they are to be executed." *Id.* at 257. The Supreme Court's explanation applies to this case:

> Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed. On the contrary, it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant – subject of course to the general Fourth Amendment protection "against unreasonable searches and seizures."
>
> [Dalia's] view of the Warrant Clause parses too finely the interests protected by the Fourth Amendment. Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant. For example, police executing an arrest warrant commonly find it necessary to enter the suspect's home in order to take him into custody, and they thereby impinge on both privacy and freedom of movement. Similarly, officers executing search warrants on occasion must damage property in order to perform their duty.

Id. at 257-58.

In *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005), the Tenth Circuit similarly explained that while a search warrant must describe with particularity the objects of the search, "the methodology used to find those objects need not be described: this court has never required warrants to contain a particularized computer search strategy." *See also United States v. Blake*, No. 1:08-cr-0284-OWW, 2010 WL 702958, at *4 (E.D. Cal. Feb. 25, 2010) ("There is no legal requirement that a search warrant include a specification of the precise manner in which the search is to be executed.").

The Court concludes that the Tracking Warrant was sufficiently particular. It precisely identified the aircard to be located by description, telephone number, and ESN number. Doc.470-1 at 28. It stated that the aircard was to be located using a "mobile tracking device," which, as noted above, reasonably describes the mobile equipment used to track signals from the aircard. *Id.* And it stated that FBI agents would be located in a public place while the aircard would be located in a private residence. *Id*. Although the warrant did not describe the precise means by which the mobile tracking device would operate, what signals it would send to the aircard, what signals it would capture, or the fact that it would cause some of Defendant's electricity to be consumed in the process, these and the many

other details of the device's operation described in Defendant's motion clearly concern the manner in which the search was to be executed, something that need not be stated with particularity in the warrant. *Dalia*, 441 U.S. at 257-58; *Grubbs*, 547 U.S. at 97-98. The objective of the warrant – locate the aircard – was clearly stated, as was the use of a mobile tracking device to make the location. Defendant's efforts to parse the warrant requirement further are no more persuasive here than were the defendants' similar efforts in *Dalia* and *Brooks*.[7]

4. Scope and Terms of the Warrant.

Defendant and the ACLU argue that the aircard locating mission exceeded the scope of the Tracking Warrant because the warrant suggests that Verizon, not the FBI, was authorized to search for the aircard. The warrant states that Verizon is "to *assist* agents of the Federal Bureau of Investigation (FBI) by providing all information, facilities, and technical assistance needed to ascertain the physical location of the [aircard] through the use and monitoring of a mobile tracking device[.]" Doc. 470-1 at 28. This language sufficiently states that the FBI was to ascertain the location of the aircard by using a mobile tracking device and that Verizon was being ordered to provide assistance. The warrant further orders that Verizon "shall provide to agents of the FBI data and information . . . while the agents are stationed in a public location and the [aircard] is . . . inside private residences, garages and/or other locations not open to the public or visual surveillance[.]" *Id.* at 2. The plain and common sense reading of these words is that Verizon was to assist the FBI by providing information and other services while the FBI used a mobile tracking device in a public location to find the aircard. *See, e.g.*, *United States v. Gorman*, 104 F.3d 272, 275 (9th Cir.

---

[7] This analysis also applies to Defendant's many arguments about things not specified in the warrant: that the mobile tracking device would force the aircard to change its cell tower connection to an emulated cell tower, would temporarily interrupt Defendant's Internet connection, would write data to the aircard and laptop, would disable encryption for aircard signals, and would download data from the aircard. These details concerned the manner of the search and were less intrusive than the physical break-in that did not have to be specified in the warrant in *Dalia*. Under *Dalia*, *Grubbs*, and related cases, the Court concludes that these methodology details were not required in the warrant.

1996) ("Plain meaning and common sense are landmarks for the execution and interpretation of the language of a search warrant.") (citations omitted).

The ACLU argues that the "most sensible reading" of the Tracking Warrant is that it authorized Verizon to install a pen register, not that it authorized the government to use a mobile tracking device. Doc. 985 at 3. Again the Court disagrees. Two orders were signed by Judge Seeborg on July 11, 2008. The Tracking Warrant was sought "pursuant to an Application under Federal Rule of Criminal Procedure 41(b); Title 18, United States Code, Sections 2703 and 3117, and Title 28, United States Code, Section 1651[.]" Doc. 470-1 at 28. As already noted, the warrant found "probable cause to believe that the use and monitoring of a mobile tracking device for the [aircard] will lead to evidence of" specific crimes, "as well as to the identification of individuals who are engaged in the commission of these offenses." *Id.* at 29.

Separate order CR-08-90331 ("the Pen and Trap Order"), also dated July 11, 2008, states that it is an "Application under 18 U.S.C. §§ 2703(c), 2703(d), 3122, and 3123 . . . requesting an Order authorizing the installation of a pen register and trap and trace device on the instrument or facility currently utilizing the following subject telephone number[.]" Doc. 470-2 at 6. The Pen and Trap Order then states that "Applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information identifying subscribers or customers . . . for Target Device are relevant and materials to an ongoing criminal investigation of the specified offenses." *Id.* at 7. This is the statutory standard for obtaining information under the SCA.

A common-sense reading of these two documents shows that the Tracking Warrant was granted under Rule 41, upon a finding of probable cause, and authorized use of a mobile tracking device to locate the aircard. The Pen and Trap Order was authorized under various statutes, upon a finding under the SCA, and authorized installation of a pen and trap device. The Court cannot agree that the Tracking Warrant authorized only a pen and trap device.

The Court agrees that the Tracking Warrant is not a model of clarity. But it contains the essential elements of a warrant. The Supreme Court has made clear that the Fourth

Amendment imposes only three requirements on warrants: "First, warrants must be issued by neutral, disinterested magistrates. Second, those seeking the warrant must demonstrate to the magistrate their probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense. Finally, warrants must particularly describe the things to be seized, as well as the place to be searched." *Dalia*, 441 U.S. at 255 (citations and quotation marks omitted); *see also Grubbs*, 547 U.S. at 97-98. The Tracking Warrant satisfied each of these requirements. It was issued by Judge Seeborg, a neutral magistrate; the judge found probable cause; and the thing to be located (the aircard) was precisely identified. The place to be searched could not be specified because it was unknown, but the warrant did note the likelihood that the aircard would be located "inside private residences, garages and/or other locations not open to the public or visual surveillance[.]" Doc. 470-1 at 29. The Tracking Warrant satisfied the essential requirements of the Fourth Amendment. Nothing more is required. *Dalia*, 441 U.S. at 257-58.[8]

5. New Technology and the Duty of Candor.

Defendant and the ACLU insist that because cell-site simulators are a new and potentially invasive technology, the government was required to include a more detailed description in its warrant application. The ACLU cites cases in which a magistrate denied the government's application to use a cell-site simulator, but in each of those cases the applications were made pursuant to statutory authority and not, as here, pursuant to a warrant based on probable cause. *See In re Application for an Order Authorizing Installation and*

---

[8] In a supplemental brief, the ACLU attaches internal e-mail communications from the North District of California suggesting that magistrates judges in that district recently have become concerned about the use of pen and trap orders to authorize the kind of aircard locating mission that occurred in this case. Doc. 985-1. The e-mails do not persuade the Court that suppression is required here. Prosecutors in this case obtained the Tracking Warrant in addition to the Pen and Trap Order. Moreover, the e-mail communications appear to reflect an evolving understanding about the use of technology, with prosecutors in the Northern District of California attempting to be responsive to concerns expressed by magistrate judges. The e-mails occurred some three years after the aircard locating mission in this case, and provide no basis to conclude that prosecutors knew or should have known their practices in 2008 were deficient.

Use of a Pen Register and Trap and Trace Device (*In re Stingray*), --- F.Supp.2d ----, 2012 WL 2120492, at *5 (S.D.Tex. June 2, 2012) (distinguishing *Rigmaiden*, with its stipulation that a Fourth Amendment search occurred, and explaining that "[h]ere, the application seeks an order authorizing the use of this equipment as a pen register as opposed to seeking a warrant."); *In re Application for an Order Pursuant to 18 U.S.C. § 2703(d)* (*In re Cell Tower Dump*), --- F.Supp.2d ----, 2012 WL 4717778, at *3-4 (S.D.Tex. Sept. 26, 2012) (rejecting application under SCA "for cell tower dump," stating that a warrant supported by probable cause was required).

In support of the argument that the government violated a "duty of candor" in applying for the warrant, Defendant and the ACLU cite *United States v. Rettig*, 589 F.2d. 418 (9th Cir. 1978), and *United States v. Comprehensive Drug Testing, Inc. ("CDT")*, 621 F.3d 1162 (9th Cir. 2010). These cases offer little support for Defendant's position.

In *Rettig*, drug enforcement agents asked a federal magistrate to issue an arrest warrant for the defendant on cocaine importation charges and a search warrant for the defendant's residence. 589 F.2d at 420. The judge issued the arrest warrant, but denied the search warrant because information provided in support of the warrant was stale. *Id.* The agents arrested the defendant. *Id.* During the arrest, they caught the defendant trying to flush marijuana down the toilet. *Id.* Defendant was taken into custody while another agent attempted to obtain a search warrant for marijuana evidence, this time from a state judge, without informing the judge of the agents' unsuccessful attempt to obtain a search warrant from the federal magistrate judge the day before. *Id.* The state marijuana warrant was obtained, and agents then spent several hours searching for evidence relating to the cocaine conspiracy as to which the federal search warrant had been denied. *Id.* at 421. They ultimately seized more than 2,000 items. *Id.*

Not surprisingly, the Ninth Circuit suppressed the evidence. The court found that agents used the state search warrant "as an instrument for conducting the search for which permission had been denied on the previous day, a search that pertained to evidence of the cocaine charge, not to the possession of marijuana," and that "the search was for purposes and

objects not disclosed to the magistrate." *Id.* The court clarified, however, that the agents' failure to apprise the state judge of their previous attempt to secure a search warrant for the cocaine conspiracy evidence "would not necessarily invalidate the search warrant or proscribe a search and incident seizures confined to the terms of the warrant." *Id.* Instead, the court found suppression necessary because "the agents did not confine their search in good faith to the objects of the [state marijuana] warrant," and "substantially exceeded any reasonable interpretation of its provisions." *Id.* at 423. It was not the agents' lack of candor with respect to the prior warrant application that required suppression, but their failure "to disclose an intent to conduct a search the purposes and dimensions of which are beyond that set forth in the affidavits." *Id.*

In this case, the application seeking authority to use a mobile tracking device did not mislead Judge Seeborg as to the purpose of the search, which was to locate the aircard. Although it is true, as the ACLU emphasizes, that the application did not disclose that the mobile tracking device would capture signals from other cell phones and aircards in the area of Defendant's apartment, the Court regards this as a detail of execution which need not be specified under *Dalia*. 441 U.S. at 258. Significantly, the agents in this case did not seek to capture third-party cell phone and aircard information so they could use it in a criminal investigation, nor is there any evidence that they used the third-party information in that manner. To the contrary, the evidence presented by the government and Defendant shows that the third-party information was deleted from the mobile tracking device immediately after the aircard was located. Thus, this was not a case like *Rettig* where agents intentionally searched for and sought to use cocaine evidence that was well beyond the scope of the marijuana search warrant.

Defendant and the ACLU also cite *CDT*, and in particular the concurring opinion by Chief Judge Kozinski. *CDT* involved a federal investigation of a business that was suspected of providing steroids to professional baseball players. *Id.* at 1166. During the investigation, the government learned of 10 players who had tested positive for steroid use. *Id.* It secured a grand jury subpoena in the Northern District of California seeking all records pertaining to

Major League Baseball in the possession of CDT. *Id.* CDT moved to quash the subpoena. *Id.* The day the motion to quash was filed, the government obtained a warrant in the Central District of California to search CDT's facilities. *Id.* The warrant was limited to the 10 players as to whom the government had probable cause, but when the government executed the warrant it "seized and promptly reviewed the drug testing record for hundreds of players in Major League Baseball (and a great many other people)." *Id.* The government also obtained a warrant from the District of Nevada for the urine samples on which drug tests had been performed. *Id.*

CDT and the players' union moved for return of seized property in the Central District of California and the District of Nevada, and moved to quash the subpoenas in the Northern District of California. *Id.* at 1166-67. The district courts granted these motions, expressing "grave dissatisfaction with the government's handling of the investigation" and accusing the government of "manipulation and misrepresentation." *Id.* at 1167. The Ninth Circuit affirmed. *Id.*

In his concurrence, Chief Judge Kozinski criticized federal authorities for submitting a warrant application that omitted information concerning CDT's agreement to keep the sought-after data intact pending a ruling on its motion to quash in the Northern District of California, an agreement that was accepted by the United States Attorney's Office. *Id.* at 1178. This omission "created the false impression that, unless the data were seized at once, it would be lost." *Id.* Chief Judge Kozinski wrote that "omitting such highly relevant information altogether is inconsistent with the government's duty of candor in presenting a warrant application. A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data." *Id.*

The Court cannot conclude that the omissions identified by Defendant and the ACLU in this case were "highly relevant." They were not material to the probable cause determination, nor did they mislead Judge Seeborg as to the object of the search. Instead, they implicated only the question of "how the search would be conducted." *United States v.*

Mittelman, 999 F.2d 440, 444 (9th Cir. 1993) (holding that "misstatements regarding the manner of a search do not bear on the issue of whether the search itself was justified"). Therefore, any omission of the fact that the mobile tracking device would also capture information from other cell phones and aircards in the area does not weigh heavily against the government.

Moreover, the warrant specifically required the government to "expunge all of the data" at the conclusion of the tracking mission. Doc. 470-1 at 30. The government explained that this was done precisely because the device captured information from cell phones and aircards unrelated to this investigation. There is no suggestion that the government's failure to disclose that the device would capture third-party information somehow allowed it to retain and review such data.

6. Other Arguments.

Defendant argues that the warrant was invalid because Agent Ng's affidavit was not incorporated in or attached to the warrant when the search was executed. Like the defendant in *United States v. Smith*, 424 F.3d 992 (9th Cir. 2005), Defendant apparently "confuses the well-settled principle that a warrant's overbreadth can be cured by an accompanying affidavit that more particularly describes the items to be seized with the contention . . . that an affidavit incorporated by reference must always be attached for the search warrant to be valid – even if the warrant is not overbroad without the attachment." *Id.* at 1007 (citation and quotation marks omitted). As in *Smith*, Defendant's argument is "unsupported by case law." *Id.*

Nor is the warrant invalid because it fails to describe the place to be searched. A warrant to locate an item need not specify the place to be searched. In such cases the particularity requirement can be satisfied if the warrant provides other information. In *United States v. Karo*, 468 U.S. 705 (1984), the government contended that it would be impossible to describe the place to be searched "because the location of the place is precisely what is sought to be discovered through the search." *Id.* at 718. The Supreme Court rejected that argument: "However true that may be, it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the

beeper, and the length of time for which beeper surveillance is requested." *Id.* The Tracking Warrant precisely identified the object to be located, found probable cause to believe that location of the aircard would produce evidence of the crimes identified in the warrant and the identification of individuals involved in those crimes, and placed a time limit on the location effort. As noted, the warrant also specifically recognized that the aircard may be located in a private residence. The affidavit of Agent Ng provided detailed information about the alleged tax-refund scheme and how location of the aircard could aid in the investigation of that scheme. These specifics satisfy the requirements of *Karo*.

Finally, Defendant notes that the Tracking Warrant did not require the FBI to make a return or serve a copy of the warrant on Defendant, and argues that this failure violated Rule 41(f)(2). The government concedes this flaw in the warrant, but correctly notes that suppression is not the appropriate remedy. There is no causal connection between the failure to serve the warrant and the government's location of the aircard. *See United States v. Hector*, 474 F.3d 1150, 1155 (9th Cir. 2007) (holding that suppression is inappropriate remedy for failure to serve copy of search warrant) (citing *Hudson v. Michigan*, 547 U.S. 586, 592 (2006)); *United States v. Motz*, 936 F.2d 1021, 1025 (9th Cir. 1991) (holding that where defendants "were not prejudiced by the agents' failure to perform the ministerial requirements" of return and inventory, "[t]he district court was correct in refusing to suppress the evidence"). Defendant argues that he would have fled and never been found if the warrant had been served, but the Court cannot conclude that his inability to evade capture is the kind of prejudice referred to in the case law.

D. Search of Apartment and Computer.

Defendant challenges the searches of his apartment and computer. The government argues that the searches were carried out pursuant to a valid warrant, issued by a neutral magistrate, based on a finding of probable cause; that the searches were conducted reasonably; and that the agents acted in good faith.

1. Apartment Search.

On July 22, 2008, United States Magistrate Judge Howard Lloyd signed a warrant approving a search of Defendant's apartment. The warrant was not executed and was returned to Magistrate Judge Patricia Trumbull on July 30, 2008. The government resubmitted the application and affidavit to Magistrate Judge Trumbull, and she approved the warrant, titling it an "Amended" warrant. Doc. 464-2 at 2. The government executed the Amended Warrant following Defendant's arrest on August 3, 2008.

Defendant argues that the Amended Warrant was facially invalid because it was neither a new warrant nor a reissued version of the old warrant. The government counters that the Amended Warrant issued by Magistrate Judge Trumbull was valid as a new warrant supported by probable cause. The Court agrees. Judge Trumbull was presented with an application setting forth probable cause for a search of Defendant's apartment and executed the Amended Warrant. The Court finds no basis for concluding that the warrant was invalid because it was preceded by the original warrant, and Defendant offers no authority for a contrary conclusion.

Defendant argues that the search warrant application failed to demonstrate probable cause. The Court does not agree. The supporting affidavit contained a detailed, 127-paragraph description of the criminal investigation, including the tax-fraud scheme perpetrated by the Hacker, confidential informant communications with the Hacker, money that was collected in bank accounts from fraudulent refunds procured by the Hacker, and money that was sent to the Hacker from these accounts. Doc. 464-2 at 3-44. The affidavit noted that historical cell tower information and IP addresses used by the aircard had led investigators to conclude that the aircard was in fact used by the Hacker to commit the tax-fraud offenses; that historical cell tower information and other investigative techniques had led the investigation team to the location of the aircard in apartment 1122 of the Domicilio apartments in Santa Clara, California; that information subpoenaed from the apartment operator revealed that unit 1122 had been rented under the false name of Steven Travis Brawner using the driver's license number of a California woman and a false 2006 tax return; and that handwriting on the apartment application was found by a handwriting expert to be

similar to handwriting used by the Hacker to rent a Sacramento Post Office Box in the false name of Patrick Stout, using a driver's license number belonging to another California woman. *Id.* at ¶¶ 34, 101-106. The detailed information in the affidavit established a "fair probability" that evidence of the tax-fraud scheme would be found in the apartment. This is particularly true when taking into account the deference to be afforded Magistrate Judge Trumbull's probable cause determination. *Gates*, 462 U.S. at 238-39; *Ewing*, 588 F.3d at 1223; *Gil*, 58 F.3d at 1418.[9]

2. Computer Search.

Defendant argues that the government violated the terms of the Amended Warrant by continuing to review digital material seized pursuant to the warrant. The Amended Warrant referred to "Attachment B" and "Attachment C" in the place identifying the things to be seized during the search. Attachment B listed the items to be seized, including Defendant's computer and any related storage devices. Doc. 464-3 at 4. Attachment C was titled "Computer Search Protocol For The Northern District Of California." Doc. 464-3 at 15. The protocol authorized the government to remove the computer and storage devices from Defendant's apartment if they could not reasonably be searched or imaged on site, or if they otherwise were required to preserve evidence. The protocol provided that "[t]he government must complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable and no later than thirty (30) calendar days after the initial execution of the warrant." *Id.* at 16.

The government seized computer equipment from Defendant's apartment during the search on August 3, 2008, including the laptop and other storage devices. The government filed a return with the magistrate judge two days later, specifying the items that had been

---

[9] Defendant argues that agents violated his Fourth Amendment rights when they took the keys found in his pocket upon his arrest and checked to see if the keys fit the lock on apartment 1122. The Court does not agree. An agent merely inserted the key into the lock and turned it to see if the key would fit; he did not open the door or enter the apartment. Even if this limited action could be viewed as a Fourth Amendment search, agents had by that time obtained the Amended Warrant to search the apartment.

seized. Doc. 873 at 65. The government then made copies of the computer hard drive and storage devices and began a search of the copies to identify relevant information. According to Defendant, the government searched the copies for 401 days, long after the 30-day period expired, and continued searching selected copies for an even longer period. Docs. 830 at 7-8; 934-1 at 5-6.

The government argues that its investigation has been reasonable "and the scope of the search has not expanded beyond the contours of the search warrant." Doc. 873 at 65. According to the government:

> The investigative agents filed a return two days after the execution of the search warrant detailing the devices seized from the premises, and within approximately 30 days after the execution of the warrant Agent Daun destroyed any forensic images of devices that did not contain material responsive to the search warrant. The physical devices that did not contain responsive material or contraband have been segregated for return to defendant and have not been searched.
>
> . . . [O]n the day the search warrant was executed, Agent Daun found a file labeled "filesalot.dcv" that contains the bulk of the incriminating information in this case. Due to the volume of data involved, Agent Daun spent considerable time identifying particular files and pieces of data within files that the search warrant commands law enforcement to seize. The images that Agent Daun continues to review were all promptly determined to contain evidence or contraband.

Id.

In reply, Defendant argues that (1) the warrant did not authorize seizure of "filesalot.dcv" because it contains files that fall outside the parameters of the protocol; (2) Agent Daun failed to complete her search within 30 days as required by the protocol; (3) the government destroyed "images" that did not contain responsive materials – as opposed to "data" as specified in the protocol; and (4) the government has retained devices and data containing contraband when the protocol allows retention only of devices and data that are themselves contraband, and when the government long ago isolated the "'contraband' data." Doc. 900 at 11-15. Defendant maintains that these alleged excesses transformed the warrant into a "general warrant" and that "wholesale suppression" is the appropriate remedy. Doc. 830-1 at 7-8. Defendant also disputes certain representations made by the Government – for example, that Agent Daun has limited her search to the materials identified in her 2009

analysis.

In a Supplemental Memorandum filed Match 26, 2013, the government reiterated that "within 30 days . . . all seized digital storage devices were either found to have materials subject to seizure under the warrants and mirrored or found to have no such materials." Doc. 984 at 4. The government states that "[a] number of files subject to seizure pursuant to the warrants were found within 30 days of seizure." Doc. 984 at 4.

Based on the parties' briefs and responses by the government during oral argument, the Court concludes that during the first 30 days after execution of the search warrant: (1) storage devices found to contain any relevant material were copied and retained by the government, (2) storage devices found not to contain relevant information were segregated and copies of them were destroyed, and (3) some relevant information was found on first category of devices. The Court also concludes that the government has continued to search copies of the devices that contained relevant information and has found additional relevant information after the 30-day period specified in the protocol.

In defending its review of copies beyond the time periods specified in the protocol, the government states that the prosecution team consulted with "a representative of the U.S. Attorney's Office for the Northern District of [California] who assisted in the preparation of the search warrants" to determine the proper interpretation of the protocol. *Id.* at 3. This person "advised that the protocol was interpreted to mean that some evidence on a computer or similar device subject to seizure pursuant to a warrant would need to be located within 30 days of seizure." *Id.* Therefore, the government explains, its failure to complete review of devices that contained relevant information within 30 days, or to seek an extension of the 30-day deadline, was based on an interpretation of the protocol that required the government merely to identify some relevant information on a device within 30 days, in which event the government could continue to review a copy of the device after 30 days. *Id.* at 2.

The protocol states in paragraph 1 that if a search of the computer or related storage devices cannot reasonably be completed on site, it may be removed "only if authorized by law because removal is (1) necessary to preserve evidence, or (2) if the item is contraband, a

forfeitable instrumentality of the crime, or fruit of the crime." Doc. 464-3 at 15. Paragraph 2 states that the government must consider duplicating the contents of a computer device on-site in lieu of removing it. *Id.* Paragraph 3 states, apparently in addition to the circumstances described in paragraph 1, that a computer or storage device can be removed "if the device cannot be searched reasonably on site, or by mirror-imaging or otherwise duplicating its contents for off site examination." *Id.* This paragraph also states that "[t]he government may also remove and retain the device, equipment, or document if the government determines that the information on the device is encrypted, until such reasonable time as it is determined that it does not contain any information that falls within the scope of the warrant." *Id.* at 15-16. Defendant's computer and devices contained at least some encrypted information.

Paragraph 4 states that "[i]f the government removes a device or related equipment or documents from the place they were found in order to complete the search off-site, within ten (10) calendar days of the removal the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents." *Id.* at 16. The government filed such a return within two days.

Paragraph 5 contains the time limits at issue in this case. The first sentence states that "[t]he government must complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable and no later than thirty (30) calendar days after the initial execution of the warrant." *Id.* Even though the protocol has already distinguished between a device and a mirror-image of the device, this sentence refers only to search of "a device," not to searching a copy of a device. If the intent of the protocol is, at least in part, to ensure that computers and related devices are withheld from their owners for as little time as possible, the distinction may have been deliberate – the protocol may require search of "a device" to be completed within 30 days while placing no such time limit on the government's search of a copy of the device. Such a reading would ensure that the owner receives the device back within a reasonably short period of time, while affording the government additional time to search what may be millions of documents on the copy of the device. This intent seems to be reinforced by the next sentence, which reads: "Within thirty

(30) calendar days after completing an off-site search of a device pursuant to this warrant [this could be up to 60 days after the initial search], the government must return any device, as well as any retained equipment or document that was removed from the site in order to complete the search, unless, under the law, the government may retain the device, equipment, or document (1) to preserve evidence, (2) because the device, equipment, or document is contraband, a forfeitable instrumentality of the crime, or fruit of crime, or (3) after reasonable efforts at decryption, the government requires additional time in order to attempt to defeat any encryption[.]" *Id.* Again, the protocol refers to returning "a device," not a copy of the device.

Paragraph 5 goes on to state that within a reasonable period, "not to exceed sixty calendar days after completing the authorized search of a device" – so this could be up to 90 days after the device was first seized – the government must destroy "copies of any data that are outside the scope of the warrant but that were copied or accessed during the search process[.]" *Id.* This language suggests that the government may not continue to search materials outside the scope of the warrant after 90 days, but may continue to search materials within the scope of the warrant.

As noted above, the government sought guidance concerning the meaning of the protocol from the U.S. Attorneys' Office in the Northern District of California and was told that agents must locate some responsive evidence on a device within 30 days of seizure in order to continue reviewing copies of the device thereafter. Doc. 984 at 3. This interpretation is reasonable if the phrase "copies of any data that are outside the scope of the warrant" is read to mean copies of any devices that contain no data responsive to the warrant. If read more literally, the phrase could mean *all* data not responsive to the warrant must be deleted within 90 days of seizure, an interpretation that would require agents to complete their review of all data within that period in order to know what data is not responsive to the warrant. The Court finds the literal reading to be more reasonable – the specific phrase used in the protocol is "any data" – but the Court cannot conclude that the interpretation applied in the Northern District of California, where the protocol was created and applies, is wholly unreasonable. Nor can the Court conclude that government agents in Arizona should have known that the

Northern District interpretation was so unreasonable as to be incorrect as a matter of law, requiring suppression of all evidence reviewed on copies of the devices after the initial 30 days. Several factors influence the Court's conclusion.

First, Defendant's computers and storage devices were seized pursuant to a valid search warrant supported by probable cause; the warrant expressly authorized government agents to examine the contents of the computer and storage devices; and, once in the government's possession, the computer and storage devices were subject to the government's full and complete review. In other words, the government's search of the devices beyond 30-days did not exceed the substantive scope of the search authorized by the warrant. If the government erred in this case, the error was one of timing.[10]

Second, courts generally have recognized that the seizure of computer information pursuant to a search warrant requires off-site examination of the computer's contents, a process that can take considerable time given the storage capacity of modern computers. Several courts have expressly concluded that neither Rule 41 nor the Fourth Amendment imposes a time constraint on the efforts of government agents to examine computer contents seized pursuant to a valid search warrant. *See, e.g.*, *United States v. Syphers*, 426 F.3d 461, 469 (1st Cir. 2005) (explaining that "[c]ourts have permitted some delay in the execution of search warrants involving computers because of the complexity of the search" and finding that the government's five-month delay in searching defendant's computer did not invalidate the search because there was "no showing that the delay caused a lapse in probable cause" or

---

[10] Defendant argues in a supplemental filing that Agent Daun violated the protocol's requirement that she minimize the examination of out-of-scope materials while searching the copies of Defendant's computer and storage devices because she looked at files herself rather than conducting a key-word search for relevant files. Doc. 934-1 at 13-14. The Court is not persuaded that Agent Daun's method of viewing the files constitutes a violation of the protocol. Even the best key-word searches miss relevant information, and the Court cannot fault the government for conducting a thorough, file-by-file review of the items seized pursuant to the search warrant. *See United States v. Giberson*, 527 F.3d 882, 889 (9th Cir. 2008) (rejecting argument that government was required to rely on folder names or other limited means of searching computer files, noting that such searches may miss critical evidence hidden as part of criminal activity).

prejudiced defendant); *United States v. Sturm*, No. CRIM 06-CR-00342-LTB, 2007 WL 601976, at *7 (D.Colo. Feb. 22, 2007) (denying suppression where agents examined CD-ROM discs two months after they were seized, explaining that Rule 41 did not "oblige the agents to examine the discs within any particular period of time" and that "[o]nce the officers obtained the discs, any danger that probable cause would cease to exist passed"); *Search of the Scranton Housing Authority*, 436 F.Supp.2d 714, 727-28 (M.D.Pa. 2006) (holding that a continuing search of computer files did not violate Rule 41, the purpose of which is to prevent stale warrants, because once the computer in question was imaged within the time specified in the warrant, the evidence was "frozen in time" alleviating the concern that probable cause would have ceased to exist); *United States v. Gorrell*, 360 F.Supp.2d 48, 55 n.5 (D.D.C. 2004) (finding suppression not required for 10-month delay in processing data recovered from computers because courts have not imposed time constraints on forensic analysis and no data was taken outside the scope of the warrant); *United States v. Hernandez*, 183 F.Supp.2d 468, 480 (D.Puerto Rico 2002) (noting that "[n]either Fed.R.Crim.P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant" and finding that "the search of Defendant's home itself took place within the time designated in the warrant" and "it was perfectly reasonable for the Government to take a longer time to search and inspect the images in the floppy disks"); *United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 66 (D.Conn. 2002) (noting that "computer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search"); *Commonwealth v. Ellis*, 10 Mass. L. Rptr. 429, 1999 WL 815818, at *10 (Mass. Super. 1999) (ruling that a two-year computer search was permissible in a workers compensation fraud case involving thousands of client files in several law offices because the length of the search was reasonable under the circumstances, probable case had not dissipated from the time the files were seized, and there was no prejudice).

Third, Rule 41 itself recognizes that searches of computers usually cannot occur at the time of the search or even within a short period afterwards. The rule provides: "A warrant

under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." Fed. R. Crim. P. 41(e)(2)(B). The Advisory Committee Note to Rule 41 further recognizes the time required to search electronic media: "Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant. . . . A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs." *Id.*, Advisory Committee Note, 2009 Amendments.

As a result, courts generally hold that the government has a reasonable time to search computers after seizing them. *See, e.g., United States v. Mutschelknaus*, 564 F.Supp.2d 1072, 1076 (D.N.D. 2008) ("Neither Fed.R.Crim.P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant."); *United States v. Grimmett*, No. 04-40005-01-RDR, 2004 WL 3171788, at *5 (D.Kan. 2004) ("The Fourth Amendment does not provide a specific time in which a computer may be subjected to a government forensic examination after it has been seized pursuant to a search warrant."); *United States v. Syphers*, 296 F.Supp.2d 50, 58 (D.N.H. 2003) (denying defendant's motion to suppress search of computer contents when search was completed seven months after seizure because time frame was not unreasonable and state did not "overstep any constitutional boundaries.").

The *Hernandez* court analogized the off-site examination of computer media to the "the 'carting off' of whole file cabinets containing pounds of unsorted paper, to be searched

off-site," which is permissible under Fourth Amendment law. *See Hernandez*, 183 F.Supp.2d at 480 (citing cases). "The rationale that searches can be executed off-site because of the volume of information has been extended to include computers." *Id*. at 480-481 (citing cases).

Fourth, the Supreme Court has held that violation of a magistrate judge's directives in executing a search warrant does not necessarily require suppression. In *Richards v. Wisconsin*, 520 U.S. 385 (1997), the magistrate who executed the search warrant specifically deleted the portion of the warrant that authorized officers to make a no-knock entry. When the search warrant was executed, however, officers concluded that the defendant was about to dispose of drugs and made a no-knock entry. The defendant argued before the Supreme Court that this action directly violated the magistrate's warrant and required suppression. The Supreme Court disagreed, holding that the officers' actions were reasonable in light of the circumstances they encountered when they arrived at the scene. *Id.* at 396-97.

The Court similarly finds the government's actions in this case to be reasonable. Agents seized computer equipment authorized in the warrant, identified the equipment in a return filed with the magistrate two days later, deleted mirrored images of devices that contain no relevant information within 30 days of the search, set aside those devices to avoid further searches (the devices could not be returned to Defendant because he was in custody), and continued searching copies of only those devices found to contain relevant information.

Fifth, as the Ninth Circuit has explained, "Rule 41 violations fall into two categories: fundamental errors and mere technical errors." *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992). Fundamental errors are those that result in clear constitutional violations. *Id.* These errors require suppression, unless the officers can show objective good faith reliance. *Id.* "Technical errors, on the other hand, require suppression only if: (1) the defendants were prejudiced by the error, or (2) there is evidence of deliberate disregard of the rule." *Id.*

The Court concludes that the government's continuing review of copies of Defendant's computer and storage devices constitutes a technical error, not a fundamental error. As noted,

the Fourth Amendment does not require that off-site searches of computers be completed in any precise amount of time, and given the volume of material contained on Defendant's computer – Defendant himself notes that his computer and storage devices contained more than 244,000 files (Doc. 934-1 at 8) – the Court does not conclude that the search time was unreasonable. Because no constitutional violation occurred, the error was technical.

Defendant has not established either of the criteria that would justify suppression based on a technical error. First, Defendant has not shown the requisite prejudice. "Prejudice in this context means the search would otherwise not have occurred or would have been less intrusive absent the error." *Id.*; *United States v. Williamson*, 439 F.3d 1125, 1133 (9th Cir. 2006). The government erred in not seeking an extension of the warrant to permit continued searching of the computer and storage device copies. If the government had not made this error – if it had obtained the extension – all of the evidence on the laptop and storage devices would have been found under the Amended Warrant. Second, the government did not deliberately violate the protocol. It sought the advice of the Northern District of California concerning interpretation of the protocol, and the interpretation was not clearly unreasonable. *Cf. United States v. Koch*, 625 F.3d 470, 478 (8th Cir. 2010) ("agents acted in good faith by seeking advice from the county attorney's office"). In addition, the protocol authorized an offsite search, which the government timely commenced and which resulted in the discovery a number of files subject to seizure. *See Hernandez*, 183 F.Supp.2d at 480 (finding suppression was not required for photographs from defendant's computer that were obtained after expiration of time period for search as specified in warrant; photographs were retrieved from floppy diskettes at a later time, but diskettes themselves were seized within warrant's time period). Nor can the Court conclude that the government unreasonably delayed its search of the device copies. Searches were started immediately, and extended over the ensuing months given the volume of the information to be reviewed. *See United States v. Metter*, 860 F.Supp.2d 205, 211-16 (E.D.N.Y. 2012) (finding suppression the appropriate remedy where the government retained copies of seized computer hard drives for more than 15 months without any review to determine whether the imaged electronic documents fell

within scope of search warrants).[11]

Sixth, the Court cannot accept Defendant's argument that the government's timing violation converted the Amended Warrant into a general warrant. This is not a case where the government engaged in a wide-ranging search for any possible kind of criminal activity. Material found by the government on Defendant's computer relates directly to the alleged tax-refund fraud; the government has not charged Defendant with new violations of law as a result of the search of his computer and storage devices. And the materials seized fall directly within the warrant's language listing the crimes committed by the tax-refund scheme and directing the seizure of "[a]ll data stored within any and all computer systems, electronic devices capable of storing data and access devices, found within [Defendant's apartment]." Doc. 464-3 at 4. The warrant further identified specific categories of electronic documentation and data to be seized from Defendant's computer. *Id.* at 5-7.

The same considerations apply to Defendant's other challenges to the search of the computer and storage devices. These arguments also allege, at most, technical violations of the computer search protocol. The arguments are based largely on allegations concerning the government's handling of data outside the scope of the warrant, including its alleged destruction of some data or images and its retention of noncontraband data and devices. Even assuming these allegations are true and the government's handling of the irrelevant data violated the warrant, Defendant cites no authority indicating that suppression of the relevant data found on his computer and storage devices is the appropriate remedy.

E. Good Faith Exception.

Even if the Court were to conclude that a Fourth Amendment violation occurred in this case, Defendant's motion would be denied. "The fact that a Fourth Amendment violation

---

[11] Defendant argues that Agent Daun waited six months to being her "forensic analysis" of relevant files, but notes that she and others were reviewing information on copies of the computer and storage devices during this six-month period. Doc. 934-1 at 5–6. In *Metter*, by contrast, the government conducted no review of seized materials for a period of 15 months after the search warrant was executed.

occurred – *i.e.*, that a search or arrest was unreasonable – does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009) (citing *Gates*, 462 U.S. at 223). The "sole purpose" of the exclusionary rule is "to deter future Fourth Amendment violations." *Davis v. United States*, 131 S. Ct. 2419, 2427 (2011). Moreover, "[r]eal deterrent value is a 'necessary condition for exclusion,' but it is not 'a sufficient' one." *Id.* (quoting *Hudson*, 547 U.S. at 596). Because the rule generates "substantial social costs," enforcement is appropriate only as a "last resort," when "the deterrence benefits of suppression . . . outweigh its heavy costs." *Id.*

One of the "important principles that constrain application of the exclusionary rule" is the good faith exception. *Herring*, 555 U.S. at 140. The good faith exception recognizes that the purpose of the exclusionary rule does not outweigh its costs "when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence." *Davis*, 131 S. Ct. at 2427-28 (citations omitted).

In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court held that when an officer acts "in the objectively reasonable belief that [his] conduct did not violate the Fourth Amendment," evidence seized under the authority of a search warrant that is later invalidated should not be suppressed. *Id.* at 918. The exception applies where law enforcement officers reasonably relied on a search warrant issued by a neutral magistrate, *Leon*, 468 U.S. at 920-21, or where they reasonably relied on a statute that was later determined to be unconstitutional, *Illinois v. Krull*, 480 U.S. 340, 349-50 (1987), or binding appellate precedent that was later overruled, *Davis*, 131 S. Ct. at 2429. For the good faith exception to apply, "the officer's affidavit must establish at least a colorable argument for probable cause." *United States v. Luong*, 470 F.3d 898, 903 (9th Cir. 2006) (citing *Leon*, 468 U.S. at 923).

Leon held that a presumption of good faith attaches to searches conducted pursuant to a warrant, explaining that "searches pursuant to a warrant will rarely require any deep inquiry into reasonableness" because "a warrant issued by a magistrate normally suffices to establish" that a law enforcement officer has "acted in good faith in conducting the search." *Id.* at 922-23 (citations omitted); *see Messerschmidt v. Millender*, 132 S. Ct. 1235, 1245 (2012) ("Where

the alleged Fourth Amendment violation involves a search or seizure pursuant to a warrant, the fact that a neutral magistrate has issued a warrant is the clearest indication that the officers acted in an objectively reasonable manner or, as we have sometimes put it, in 'objective good faith.'"). The threshold for showing that the good faith exception does not apply in such a case is "a high one." *Messerschmidt*, 132 S. Ct. at 1245.

The Court in *Leon* noted four situations in which the good faith doctrine is inapplicable: where (1) the affiant knowingly or recklessly misleads the magistrate with false information or material omissions; (2) the magistrate "wholly abandoned his judicial role"; (3) the affidavit is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) the warrant itself is facially deficient in its description of the place to be searched or the things to be seized. 468 U.S. at 923. Ultimately, the question is "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.* at 922.

None of the scenarios listed in *Leon* applies here. As described above, the government reasonably relied on the SCA and on warrants issued by magistrate judges. In applying for the Tracking Warrant, Agent Ng did not knowingly or recklessly mislead Magistrate Judge Seeborg; his affidavit contained sufficient indicia of probable cause and described with particularity the aircard to be located. As the government argues, "agents were using a relatively new technology, and they faced a lack of legal precedent regarding the proper form of a warrant to obtain the location information they sought." Doc. 873 at 63. *Cf. United States v. Wellman*, No. 1:08-cr-00043, 2009 WL 37184, at *7 n.8 (S.D.W.Va. January 7, 2009) (explaining that "law enforcement officers utilizing relatively new technology and innovative techniques in good faith should not be penalized with suppression of important evidence simply because they are at the beginning of a learning curve and have not yet been apprised of the preferences of courts on novel questions").

As previously discussed, Defendant argues that the government's application for the Tracking Warrant omitted information concerning the operation of the mobile tracking device. According to Defendant, this lack of candor precludes application of the good faith exception.

Doc. 824-1 at 341. The Court is not persuaded. There is no precedent suggesting that the agent was required to include in his warrant application technical details about the operation of the mobile tracking device. *Cf. United States v. Huggins*, 299 F.3d 1039, 1045 (9th Cir. 2002) (finding that "an officer with 'a reasonable knowledge of what the law prohibits' could . . . give credence to the magistrate judge's finding of probable cause") (quoting *Leon*, 468 U.S. at 919 n.2). Technical information about the device was not material to the probable cause determination, nor is there a basis for concluding that such details were omitted in bad faith.

The same analysis applies to the search of Defendant's computer and storage devices. The government obtained the Amended Warrant, and later sought and relied on legal advice from the Norther District of California in interpreting the deadlines set forth in the Computer Search Protocol. To the extent the government's interpretation of the protocol was mistaken, the error was, at worst, the product of negligence.

In sum, Defendant has not met the high threshold required to overcome the presumption of good faith. This is not a case where "it is obvious that no reasonably competent officer would have concluded that a warrant should issue." *Malley v. Briggs*, 475 U.S. 335, 341 (1986); *see Graham*, 846 F.Supp.2d at 406 (finding that it was "objectively reasonable for the officers who obtained the records to rely on the Stored Communications Act and the court orders issued thereunder"); *United States v. Warshack*, 631 F.3d 266, 288-90 (6th Cir. 2010) (finding a Fourth Amendment violation when government compelled ISP to release contents of defendant's e-mails, but applying good faith exception because government reasonably relied on SCA). In applying for the warrants, federal agents did not "exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights." *Davis*, 131 S. Ct. at 2427 (citing *Herring*, 555 U.S. at 144).

III. Related Motions.

Defendant filed a Motion for Order Requiring Government to Comply with Data Deletion Requirements, requesting an order directing the government to delete or destroy data not originally seized by Agent Daun. Doc. 847. Specifically, Defendant seeks an order

requiring the government to locate and isolate all the physical data storage devices that were seized from his apartment and storage unit and sanitize (by overwriting the devices with random data) or physically destroy the devices, with the exception of the files and data listed in Agent Daun's "Computer Forensic Report." *Id.* at 5-8. The government objects, contending that there is no authority for Defendant's demands. Doc. 873 at 66. The Court agrees and, as discussed above, finds that the government made a good faith effort to comply with the Computer Search Protocol by deleting mirrored images of devices that contained no relevant information. The motion is denied. Defendant's motion for leave to supplement the motion (Doc. 926) is granted.

Defendant filed a Motion for Leave to Place Additional Evidence on the Record Responsive to Government Claims Contained in Response to Motion to Suppress. Doc. 897. The Court will grant the motion.

Defendant filed a Motion for Discovery re: Digital Evidence Search, seeking "[a]ll evidence relating to government agents/actors" who accessed his data or provided it to other agents or defendants. Doc. 890. The government responded with "an additional summary of the nature and time frame of the searches conducted by all of the case agents who searched any aspect of defendant's computers in this case." Doc. 911. Defendant continues to object that the discovery was insufficient (Doc. 930), and subsequently filed a Motion to Suppress All Digital Data Evidence as a Sanction for Failure to Preserve Evidence (Doc. 931), and a Motion for Sanctions for Discovery Violations re: Digital Evidence Search (Doc. 932).

The government counters that it has provided Defendant the available information regarding the nature and timing of the search of digital evidence, including the searches conducted by three case agents besides Agent Daun. Doc. 935 at 4-5. As noted above, the government represents that results of the searches related only to the charged offenses and were not shared with agents or agencies outside the prosecution in this case. The Court has found that this aspect of the government's handling of the data was reasonable. Defendant's motions for sanctions will be denied.

Defendant filed a Motion to Amend/Correct, seeking leave to amend his First

Supplement to Motion to Suppress re: Search and Seizure of Digital Evidence. Doc. 934. The government does not object to the motion to amend, and it will be granted.

The ACLU filed a Motion for Leave to Submit Government Document. Doc. 985. The motion is unopposed and will be granted.

Defendant filed a Motion for Time to Submit Evidence of Legitimate Sources of Income. Doc. 993. The motion is denied. Notwithstanding the government's argument, *see* Doc. 986 at 5-6, information concerning the sources of Defendant's income is not necessary to the Court's analysis of Defendant's privacy interests.

Finally, Defendant has filed a Motion to Dismiss for (1) Government's Prejudicial Extrajudicial Press Comments Severe Enough to Impeach Claimed Indifference of Jurors, and/or (2) Various Government Misconduct (Doc. 1000), and a Motion to Stay Ruling on Suppression Issues until after the USDOJ Issues Retraction on Fabricated "Self-Described Hacker" Claims and Other Fabricated Claims in April 8, 2010 Press Release (Doc. 1001). The Court will deny the motion for a stay. Doc. 1001. The Court will rule on the motion to dismiss when it is fully briefed.

IV. Conclusion.

Defendant has not shown that he had a legitimate expectation of privacy in his apartment, laptop, or aircard. Defendant has not shown that his Fourth Amendment rights were violated or, if a violation did occur, that suppression is the appropriate remedy. The good faith exception applies to the contested areas of the government's investigation, including its use of the mobile tracking device pursuant to a Rule 41 warrant.

Defendant has filed literally dozens of motions in this case, many of them seeking suppression or some other form of sanction against the government. The Court has patiently sought to address each motion filed by pro se Defendant, but the time has come to resolve the government's allegations on the merits. Defendant should file no further motions to suppress or for sanctions based on the government's searches in this case or its pretrial production of discovery to Defendant.

IT IS ORDERED:

1. Defendant's Motion to Suppress (Doc. 824) is **denied**.

2. The following motions are **denied**: Defendant's Motion for Order Requiring Government to Comply with Data Deletion Requirements (Doc. 847), Motion for Discovery re: Digital Evidence Search (Doc. 890), Motion to Suppress All Digital Data Evidence as a Sanction for Failure to Preserve Evidence (Doc. 931), Motion for Sanctions for Discovery Violations re: Digital Evidence Search (Doc. 932), Motion for Time to Submit Evidence of Legitimate Sources of Income (Doc. 993), and Motion to Stay Ruling on Suppression Issues (Doc. 1001).

3. The following motions are **granted**: Defendant's Motion for Leave to Place Additional Evidence on the Record (Doc. 897), Defendant's Motion for Leave to File First Supplement to Motion for Order Requiring Government to Comply with Data Deletion Requirements (Doc. 926), Defendant's Motion to Amend/Correct (Doc. 934), and the ACLU's Motion for Leave to Submit Government Document (Doc. 985).

4. By separate order, the Court will schedule a conference to set a firm trial date and establish a schedule of events that must be completed before trial.

5. Defendant shall not file further motions to suppress or for sanctions based on the government's searches in this case or the government's pretrial production of discovery to Defendant.

Excludable delay pursuant to U.S.C. § 18:3161(h)(1)(D) is found to run from 6/4/2012.

DATED this 8th day of May, 2013.

David G. Campbell
United States District Judge