844 F.Supp.2d 982
United States District Court,
D. Arizona.

UNITED STATES of America, Plaintiff,
v.
Daniel David RIGMAIDEN (1), Defendant.

No. CR08–0814–01–PHX–DGC. | Jan. 5, 2012.

Synopsis
Background: Defendant, who was charged by indictment with 50 counts of mail and wire fraud, aggravated identity theft, and conspiracy, moved for disclosure of evidence and for additional discovery.

Holdings: The District Court, David G. Campbell, J., held that:

[1] government was not required to disclose identities of agents involved in tracking the location of an aircard connected to defendant's laptop;

[2] detailed technical information related to the devices and techniques used to locate the aircard was privileged;

[3] evidence relating to the real time and historical geolocation techniques used to locate the aircard was privileged;

[4] information showing the geographical paths of the wireless device locators used to locate the aircard was privileged;

[5] evidence relating to the specific mobile tracking device used by the government to locate the aircard was privileged;

[6] evidence related to the Pen/Trap Network Architecture used to locate the aircard was privileged;

[7] communications between the government and private entities during search for the aircard were privileged; and

[8] defendant did not make threshold showing of materiality required for disclosure of purported policy regarding the destruction of data related to search for the aircard.

Motions denied.

West Headnotes (28)

[1] **Criminal Law**
Constitutional obligations regarding disclosure

Government disclosure of exculpatory evidence is required by *Brady*..

Cases that cite this headnote

[2] **Criminal Law**
Application, motion or request; affidavits

To obtain discovery under rule requiring the government to disclose a document or object material to preparing the defense, defendant must make a threshold showing of materiality, which requires a presentation of facts which would tend to show that the government is in possession of information helpful to the defense. Fed.Rules Cr.Proc.Rule 16(a)(1)(E)(i), 18 U.S.C.A.

Cases that cite this headnote

[3] **Criminal Law**
Application, motion or request; affidavits

A general description of the materials sought or a conclusory argument as to their materiality is insufficient to satisfy the requirements of rule requiring the government to disclose a document or object material to preparing the defense. Fed.Rules Cr.Proc.Rule 16(a)(1)(E)(i), 18 U.S.C.A.

Cases that cite this headnote

[4] **Criminal Law**
Informers or Agents, Disclosure

The privilege not to produce the identity of a confidential government informant is limited.

Cases that cite this headnote

[5] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

Even sensitive law enforcement information must be disclosed if it is needed for an effective defense. Fed.Rules Cr.Proc.Rule 16, 18 U.S.C.A.

Cases that cite this headnote

[6] **Criminal Law**
Informers or Agents, Disclosure

Where the disclosure of an informer's identity, or the contents of his communication, is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the privilege not to produce the identity of a confidential government informant must give way. Fed.Rules Cr.Proc.Rule 16, 18 U.S.C.A.

Cases that cite this headnote

[7] **Criminal Law**
Proceedings in general

The level of government disclosure required for a suppression hearing under the Fourth Amendment is less than the level of disclosure required for trial. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[8] **Criminal Law**
Degree of proof

The burden of proof at a suppression hearing is a preponderance of the evidence.

Cases that cite this headnote

[9] **Criminal Law**
Proceedings in general

In deciding whether defendant needs disclosure of allegedly sensitive law enforcement information to assert his Fourth Amendment suppression argument, the Court may consider not only the evidence that has already been disclosed to defendant, but also whether there are alternative sources of information upon which Defendant can rely. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[10] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

In evaluating the government's assertion that information sought by defendant is subject to a qualified law enforcement privilege, the Court may hold an ex parte hearing.

Cases that cite this headnote

[11] **Criminal Law**
Documents or tangible objects

The identities of agents involved in tracking the location of an aircard connected to a laptop computer that defendant allegedly used to

perpetuate scheme to commit mail and wire fraud and aggravated identity theft were not documents or other tangible objects within governments possession, custody, or control, and thus fell outside rule requiring the government to disclose such documents or objects material to preparing the defense. Fed.Rules Cr.Proc.Rule 16(a)(1)(E)(i), 18 U.S.C.A.

Cases that cite this headnote

[12] **Criminal Law**
Documents or tangible objects

Rule requiring the government to disclose documents or other tangible objects within its possession, custody, or control does not require the government to create documents that may provide information a defendant desires to obtain, nor does it require the government to present agents or witnesses for interviews or in-court examination. Fed.Rules Cr.Proc.Rule 16(a)(1)(E)(i), 18 U.S.C.A.

Cases that cite this headnote

[13] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

The identities of agents involved in tracking the location of an aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft was sensitive information protected by the qualified law enforcement privilege; revealing the identities of these agents could compromise their safety during future law enforcement missions, and if the identities of these agents were disclosed, they no longer could safely participate in such missions, a fact that would seriously limit the government's law enforcement capabilities given the unique training and skill set of individuals involved in the operation.

Cases that cite this headnote

[14] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

Defendant did not make the showing required to overcome the qualified law enforcement privilege protecting the identities of agents involved in tracking the location of an aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft; the government conceded that the search for the aircard constituted a Fourth Amendment search, questioning the agents in order to challenge the government's reliance on a good faith exception to the warrant requirement would not be helpful or relevant to the defense as it would not address the objective reasonableness of their actions, and defendant could assert the bad faith destruction of potentially exculpatory evidence through other means. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[15] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

Detailed technical information related to the devices and techniques used to track the location of an aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft was protected by the qualified law enforcement privilege; disclosure of this information would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection, and each of defendant's reasons for obtaining this information was satisfied by the government's concessions.

Cases that cite this headnote

Cases that cite this headnote

[16] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

All evidence relating to the real time and historical geolocation techniques used by the government while searching for the location of an aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft was protected by the qualified law enforcement privilege; disclosure of techniques used by the government would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection.

Cases that cite this headnote

[17] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

Defendant did not present sufficient reason to overcome the qualified law enforcement privilege protecting from disclosure all evidence relating to the real time and historical geolocation techniques used by the government while searching for the location of an aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft; to the extent defendant sought information to show that locating the aircard was a search and to show that the search exceeded the scope of the relevant warrants and court orders, the government had conceded its efforts to locate the aircard were a search and defendant had ample alternative means to challenge the particularity of the warrant, and the government also conceded that agents made phone calls to the aircard during the tracking operation, thereby enabling defendant to make arguments that the mobile tracking operation exceeded the scope of the relevant warrants and orders. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[18] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

Information showing the geographical paths of the wireless device locators used by the government while searching for the location of an aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft was protected by the qualified law enforcement privilege; disclosure of this information would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection.

Cases that cite this headnote

[19] **Criminal Law**
Application, motion or request; affidavits

Defendant failed to make the required threshold showing of materiality in order to obtain disclosure of all evidence relating to the specific mobile tracking device used by the government, including user manuals, test data, and related software, while searching for the location of an aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft; defendant stated he needed this evidence because it might reveal additional Fourth Amendment violations he was currently unaware of. U.S.C.A. Const.Amend. 4; Fed.Rules Cr.Proc.Rule 16(a)(1)(E)(i), 18 U.S.C.A.

1 Cases that cite this headnote

[20] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

All evidence relating to the specific mobile tracking device used by the government, including user manuals, test data, and related software, while searching for the location of an aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft was protected by the qualified law enforcement privilege; disclosure of the specific equipment used by the government to locate the aircard would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection, and defendant had ample alternative information with which to challenge the government's use of this equipment.

1 Cases that cite this headnote

[21] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

All evidence related to the Pen/Trap Network Architecture used by the government in its efforts to locate an aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft was protected by the qualified law enforcement privilege; disclosure of the specific equipment and techniques used by the government to locate the aircard would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection, and defendant had ample alternative information with which to assert that the provisions of a court order were violated.

Cases that cite this headnote

[22] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

The original storage devices used by the government to locate an aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft were protected by the qualified law enforcement privilege; disclosure of the specific devices used by the government to locate the aircard would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection.

Cases that cite this headnote

[23] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

The government's concession that all data generated during the efforts to locate the aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft were destroyed shortly after defendant's arrest enabled defendant to construct legal arguments arising from the destruction of such evidence, and thus precluded the need for the government to disclose original storage devices used by the government to locate the aircard, which devices were protected by the qualified law enforcement privilege.

Cases that cite this headnote

[24] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

All communications between the government and private entities associated with wireless company and various companies that manufactured electronic surveillance equipment during government's efforts to locate the aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft were protected by the qualified law enforcement privilege; these communications would concern

equipment and techniques used by the government to locate the aircard, and disclosure of such equipment and techniques would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection.

Cases that cite this headnote

[25] **Criminal Law**
Application, motion or request; affidavits

The possibility of further information does not satisfy the threshold showing of materiality required for production under rule requiring the government to disclose a document or object material to preparing the defense. Fed.Rules Cr.Proc.Rule 16(a)(1)(E)(i), 18 U.S.C.A.

Cases that cite this headnote

[26] **Privileged Communications and Confidentiality**
Investigatory or law enforcement records

Unredacted and unsummarized documents related to the government's motion to search for and locate the aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft were protected by the qualified law enforcement privilege; documents concerned equipment and techniques used by the government to locate the aircard, and disclosure of such equipment and techniques would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection.

Cases that cite this headnote

[27] **Criminal Law**
Application, motion or request; affidavits

Defendant's assertion, based on a newspaper article regarding his prosecution for conspiracy, mail and wire fraud, and aggravated identity theft, that the government possessed a written policy regarding the destruction of data in connection with efforts to locate the aircard connected to a laptop computer that defendant allegedly used to perpetuate the fraudulent scheme, did not satisfy the threshold showing of materiality required for disclosure under rule requiring the government to disclose a document or object material to preparing the defense; defendant admitted that the government's concession that the aircard was located precisely within his apartment may have eliminated his need for the destroyed evidence. Fed.Rules Cr.Proc.Rule 16(a)(1)(E)(i), 18 U.S.C.A.

Cases that cite this headnote

[28] **Criminal Law**
Particular documents or tangible objects

Defendant's request that the government question FBI agents for an explanation of various issues related to the search for the aircard connected to a laptop computer that defendant allegedly used to perpetuate scheme to commit mail and wire fraud and aggravated identity theft, including the degree of interruption with the aircard, whether the mobile tracking device was forwarding signals to wireless carrier, whether the device was denying the aircard Internet access, and why the agents needed to call the aircard repeatedly over a six hour period, were not proper requests for disclosure under rule requiring the government to disclose a document or object material to preparing the defense. Fed.Rules Cr.Proc.Rule 16(a)(1)(E)(i), 18 U.S.C.A.

1 Cases that cite this headnote

Attorneys and Law Firms

***987** Frederick A. Battista, James Richard Knapp, Peter S. Sexton, U.S. Attorney's Office, Phoenix, AZ, for

Plaintiff.

ORDER

DAVID G. CAMPBELL, District Judge.

The government indicted Defendant Daniel Rigmaiden on July 23, 2008, charging him with 50 counts of mail and wire fraud, aggravated identity theft, and conspiracy. Doc. 3. A Superseding Indictment was filed on January 27, 2010. Doc. 200. The charges arise from an alleged scheme to obtain fraudulent tax refunds by filing electronic tax returns in the names of numerous 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 perpetuate the fraudulent scheme. Defendant alleges that the technology and methods used to locate the aircard violated his Fourth Amendment rights. Defendant has sought extensive discovery from the government regarding the technology, methods, and personnel involved in tracking the aircard. Although the government has responded with the disclosure of substantial information, Defendant contends that additional information must be disclosed if he is to litigate his Fourth Amendment arguments effectively. The government opposes disclosure of additional information sought by Defendant, arguing that the information is protected by a qualified law enforcement privilege under *Roviaro v. United States*, 353 U.S. 53, 77 S.Ct. 623, 1 L.Ed.2d 639 (1957), and its progeny, including *United States v. Van Horn*, 789 F.2d 1492 (11th Cir.1986).

Defendant has filed a Motion For Disclosure Of All Relevant And Helpful Evidence Withheld By The Government Based On A Claim Of Privilege. Doc. 592. Defendant has also filed a Motion For Additional Discovery Due To Government Ignoring Defendant's Recent Discovery Requests. Doc. 697. The Court held hearings related to the first motion on September 22 and October 28, 2011, and held an *ex parte* hearing on the government's privilege claim on December 14, 2011. For reasons set forth below, the Court concludes that the government is entitled to a qualified law enforcement privilege, that Defendant has not made the showing necessary to overcome the privilege, and that Defendant's first motion for discovery (Doc. 592) should be denied. The Court also concludes that portions of Defendant's second motion (Doc. 697) should be denied, and will await completion of briefing to rule on the remaining issues raised in the second motion.[1]

***988 I. Legal Standards.**

[1] Historically, defendants in the United States have not enjoyed a right to unfettered discovery in criminal cases. Government disclosure of exculpatory evidence is, of course, required by *Brady v. Maryland*, 373 U.S. 83, 83 S.Ct. 1194, 10 L.Ed.2d 215 (1963), and disclosure of other information is required by the Jencks Act, 18 U.S.C. § 3500. Through the Rules Enabling Act process, Congress has also created limited additional discovery rights through Federal Rule of Criminal Procedure 16. This order particularly concerns the discovery rights found in Rule 16(a)(1)(E)(i).

[2] [3] Under this rule, the government must disclose a document or object "if the item is within the government's possession, custody, or control and ... the item is material to preparing the defense[.]" Fed.R.Crim.P. 16(a)(1)(E)(i). To obtain discovery under this rule, Defendant "must make a threshold showing of materiality, which requires a presentation of 'facts which would tend to show that the Government is in possession of information helpful to the defense.' " *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir.1995) (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir.1990)). "A general description of the materials sought or a conclusory argument as to their materiality is insufficient to satisfy the requirements of [Rule 16(a)(1)(E)(i)]." *United States v. Cadet*, 727 F.2d 1453, 1468 (9th Cir.1984); *see Santiago*, 46 F.3d at 894.

With respect to most of the items addressed in this order, the Court already has concluded that Defendant has satisfied the requirements of Rule 16(a)(1)(E)(i). With respect to a few of the items identified in Defendant's motions, that showing has not been made. These items will be addressed later in this order.

Even if a defendant is entitled to discovery under Rule 16, however, the Supreme Court has held that the discovery may be withheld when the government is entitled to a law enforcement privilege. In *Roviaro*, the Court held that the government was not required to produce the identity of a confidential government informant. 353 U.S. 53, 77 S.Ct. 623. The Court explained that "[t]he purpose of the privilege is the furtherance and protection of the public interest in effective law enforcement. The privilege recognizes the obligation of citizens to communicate their knowledge of the commission of crimes to law-enforcement officials and, by preserving their anonymity, encourages them to perform that obligation." *Id.* at 59, 77 S.Ct. 623.

[4] [5] [6] The privilege recognized in *Roviaro* is limited. Even sensitive law enforcement information must be disclosed if it is needed for an effective defense. "Where the disclosure of an informer's identity, or the contents of his communication, is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the privilege must give way." *Id.* at 60–61, 77 S.Ct. 623. In deciding whether the privilege applies and whether it has been overcome by a showing of need, the Supreme Court declined to establish fixed rules, holding instead that trial courts must engage in balancing on a case-by-case basis:

> We believe that no fixed rule with respect to disclosure is justifiable. The problem is one that calls for balancing the public interest and protecting the flow of information against the individual's right to prepare his defense. ***989** Whether a proper balance renders non-disclosure erroneous must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors.

Id. at 62, 77 S.Ct. 623.[2]

Subsequent cases have expanded the qualified law enforcement privilege beyond the context of confidential government informants. In *Van Horn,* the Eleventh Circuit held that the privilege applies to sensitive law enforcement surveillance equipment. 789 F.2d at 1507. The Eleventh Circuit explained:

> We hold that the privilege applies equally to the nature and location of electronic surveillance equipment. Disclosing the precise locations where surveillance devices are hidden or their price specifications will educate criminals regarding how to protect themselves against police surveillance. Electronic surveillance is an important tool of law enforcement, and it's effectiveness should not be unnecessarily compromised. Disclosure of such information will also educate persons on how to employ such techniques themselves[.]

Id. at 1508. As in *Roviaro,* the Eleventh Circuit recognized that the privilege is qualified. "The privilege will give way if the defendant can show need for the information." *Id.* The court also recognized that "the necessity determination requires a case by case balancing process, and ... we have established no fixed rules about the discovery of electronic surveillance techniques in criminal cases." *Id.*

In this case, the government contends that the technology used to locate Defendant's aircard, the manner in which the technology was employed, and the identities of the agents who operated the equipment all constitute sensitive law enforcement information subject to the qualified privilege recognized in *Roviaro* and *Van Horn.* Defendant does not disagree with the assertion that these cases can cover the kind of equipment and techniques used here. Rather, Defendant contends that the technology used by the government is already publicly known and therefore not entitled to a qualified privilege, and, in any event, that his need for the information overcomes the privilege. In resolving this dispute, the Court must engage in the balancing called for in *Roviaro* and *Van Horn.* While doing so, the Court must also keep several additional legal principles in mind.

First, Defendant seeks disclosure not for trial, but for a motion to suppress—Defendant intends to argue that steps taken by the government to locate the aircard violated his Fourth Amendment rights. The government has never suggested that it intends to present evidence about its location of the aircard at trial.[3]

***990** [7] The level of government disclosure required for a suppression hearing under the Fourth Amendment is less that the level of disclosure required for trial. The Supreme Court has explained:

> This Court on other occasions has noted that the interests at stake in a suppression hearing are of a lesser magnitude than those in the criminal trial itself. At a suppression hearing, the court may rely on hearsay and other evidence, even though that evidence would not be admissible at trial. Furthermore, although the Due

> Process Clause has been held to require the Government to disclose the identity of an informant at trial, provided the identity is shown to be relevant and helpful to the defense, *Roviaro v. United States*, 353 U.S. 53, 60–61, 77 S.Ct. 623, 1 L.Ed.2d 639 (1957), it has never been held to require the disclosure of an informant's identity at a suppression hearing. *McCray v. Illinois*, 386 U.S. 300, 87 S.Ct. 1056, 18 L.Ed.2d 62 (1967). We conclude that the process due at a suppression hearing may be less demanding and elaborate than the protections accorded the defendant at the trial itself.

United States v. Raddatz, 447 U.S. 667, 679, 100 S.Ct. 2406, 65 L.Ed.2d 424 (1980).

The District of Columbia Circuit has provided further explanation of the difference between disclosures required for a suppression hearing and those required for trial:

> The proceedings have different functions. Suppression hearings determine whether the police engaged in unlawful conduct, and seek to deter such conduct by excluding evidence. Trials decide whether the accused committed the offense charged. Privileges shield witnesses from cross-examination. A defendant's right to cross-examination is more limited at suppression hearings than at trials, which is why hearsay is generally admissible at the former but not the latter.

United States v. Foster, 986 F.2d 541, 543 (D.C.Cir.1993).

The Supreme Court has specifically applied this rationale in the context of the *Roviaro* privilege. In *McCray v. Illinois*, 386 U.S. 300, 87 S.Ct. 1056, 18 L.Ed.2d 62 (1967), the Supreme Court provided this explanation:

> What *Roviaro* thus makes clear is that this Court was unwilling to impose any absolute rule requiring disclosure of an informer's identity even in formulating evidentiary issues for federal criminal trials. Much less has the Court ever approached the formulation of a federal evidentiary rule of compulsory disclosure where the issue is the preliminary one of probable cause, and guilt or innocence is not at stake. Indeed, we have repeatedly made clear that federal officers need not disclose an informer's identity in applying for an arrest of search warrant.

Id. at 311, 87 S.Ct. 1056.

Other courts likewise have recognized the more limited nature of disclosures required for suppression hearings. *See United States v. Garey*, No. 5:03–CR–83, 2004 WL 2663023 at *4 n. 7 (N.D.Ga., Nov. 15, 2004) ("The Court also observes that the reason for requiring disclosure of privileged information at the search warrant stage are less compelling than those for disclosure in preparation for trial.") (citing *McCray* and *Roviaro*).

Thus, in this case, when evaluating Defendant's motions, the Court must keep in mind the less demanding disclosure requirements for a suppression hearing.

[8] Second, the burden of proof at a suppression hearing is a preponderance of the evidence. *See United States v. Jordan*, 291 F.3d 1091, 1100 (9th Cir.2002); ***991** *Collazo v. Estelle*, 940 F.2d 411, 421 (9th Cir.1991); *United States v. Vasey*, 834 F.2d 782, 785 (9th Cir.1987). To the extent Defendant seeks to show a violation of his Fourth Amendment rights, he must produce only a preponderance of the evidence. If Defendant presents credible evidence to support a fact, and the government is unable to rebut that fact because it has withheld as privileged the information that would enable it to rebut the fact, Defendant likely will have established the fact by a preponderance of the evidence.[4]

[9] Third, in deciding whether Defendant needs allegedly sensitive law enforcement information to assert his Fourth Amendment argument, the Court may consider not only the evidence that has already been disclosed to Defendant, but also whether there are alternative sources of information upon which Defendant can rely. As one federal court has explained in applying the *Roviaro* privilege: "A defendant seeking to learn the location of a police surveillance post should ordinarily show that he needs the evidence to conduct his defense and *that there are no adequate alternative means of getting at the same*

point." *United States v. Harley,* 682 F.2d 1018, 1020 (D.C.Cir.1982) (emphasis added). Other federal cases have repeated this principle. *See United States v. Cintolo,* 818 F.2d 980, 1002 (1st Cir.1987); *Sanders v. Crotty,* No. 06–C–5159, 2008 WL 905993 at *6 (N.D.Ill., Apr. 3, 2008). Thus, in addressing Defendant's arguments, the Court will consider not only the evidence already disclosed by the government, but also the considerable evidence Defendant has secured from other sources.

[10] Fourth, in evaluating the government's assertion that information sought by Defendant is subject to a qualified law enforcement privilege, the Court may hold an *ex parte* hearing. This circuit and other courts have approved *ex parte* hearings for the purpose of considering *Roviaro*-type privilege claims. *See, e.g., United States v. Johns,* 948 F.2d 599, 606 (9th Cir.1991) (district court's *ex parte* hearing to consider government's request to maintain confidentiality of informant approved over defendant's objection); *United States v. Fixen,* 780 F.2d 1434, 1439–40 (9th Cir.1986) (suggesting use of *in camera* proceedings to resolve *Roviaro* issues); *Global Relief Found., Inc. v. O'Neill,* 315 F.3d 748, 754 (7th Cir.2002) ("*Ex parte* consideration is common in criminal cases where, say, the identity of informants otherwise might be revealed, *see Roviaro v. United States* [.]"); *United States v. Gonzalez,* 2009 WL 742309 *1 (C.D.Cal.2009) (court conducted *ex parte* hearing to evaluate *Roviaro* privilege claim); *United States v. Salemme,* 978 F.Supp. 386, 389 n. 8 (D.Mass.1997) (*ex parte* submission used to evaluate *Roviaro* privilege claim); *see also* 39 Geo. L.J. Ann. Rev.Crim. Proc. at 376 (2010) ("The trial court may be required to conduct an *in camera* inspection to determine whether *Roviaro* requires disclosure of an informant's identity") (citing numerous federal decisions); *cf. United States v. Klimavicius–Viloria,* 144 F.3d 1249, 1261 (9th Cir.1998) ("*Ex parte* hearings are generally disfavored. In a case involving classified documents, however, *ex parte, in camera* hearings in which government counsel participates to the exclusion of defense counsel are part of the process that the district court may use in order to ***992** decide the relevancy of the information.") (citation omitted). As noted above, the Court held such an *ex parte* hearing on December 14, 2011. The hearing will be discussed below.

II. Procedural History.

The discovery dispute between Defendant and the government has been ongoing for almost two years. On February 18, 2010, Defendant sent an extensive discovery request to the government. Doc. 592–2 at 1[5]. Motions on this issue were filed as early as March 25, 2010. *See* Doc. 251. Through extensive written communications, including requests by Defendant exceeding 70 pages, Defendant and the government were able to narrow some of the discovery issues. *See, e.g.,* Docs. 335, 592–2. Discovery issues were discussed with the Court at hearings held on July 15, September 8, and November 9, 2010, and on January 6, February 10, May 5, July 20, September 8, and October 28, 2011. *See* Docs. 329, 364, 399, 422, 447, 535, 582, 613, 681.

Throughout the course of this discovery dispute, the government has produced substantial information to Defendant. This information had included applications for warrants and orders, copies of warrants and orders, technical data generated during the aircard locating mission, and email and written communications among counsel and FBI agents related to the mission. As Defendant has refined his Fourth Amendment arguments, he has repeatedly sought additional information from the government. The government has responded to many of these requests, producing additional information, but also has continued to maintain that some information is subject to a qualified law enforcement privilege.

Defendant's primary discovery motion was filed on August 12, 2011. Doc. 592. The motion included a 101–page memorandum of points and authorities and more than 300 pages of exhibits. *See* Docs. 587, 592. Although Defendant is representing himself, the memorandum is remarkably well researched and well written. The Court has not seen better work product from criminal defense attorneys.

During a lengthy hearing on September 22, 2011, the Court discussed Defendant's motion with Defendant and counsel for the government. The parties and the Court were able to agree on factual concessions by the government that resolved some of Defendant's discovery requests. Those factual concessions will be discussed below. Following the hearing, the Court entered an order that itemized these factual concessions and identified additional factual issues on which additional stipulations would be helpful. Doc. 644. The Court directed counsel for the government to discuss these issues with the Department of Justice and the FBI, and directed the parties to meet and confer in an effort to reach additional stipulations. *Id.* Unfortunately, the meeting did not occur.

Following the hearing on September 22, 2011, Defendant sent a letter to counsel for the government setting forth nine demands in connection with the anticipated meeting. These included that the meeting not occur at the federal facility where Defendant is incarcerated, that the meeting not occur through a security screen or security window,

that Defendant not be subject to sleep deprivation before the meeting as was typical before his appearances in Court, that Defendant be provided drinking water before and after the meeting, that Defendant be provided drinking water during the meeting, that ***993** Defendant not be transported in the painful restraints applied during court transportation, that Defendant not be handcuffed during the meeting, that Defendant not be strip searched before the meeting, and that officials from the Department of Justice enter into a written contract with Defendant granting him use immunity and derivative use immunity for all statements and information provided during the meeting, applicable not only to this case but to any other case that might be brought against Defendant elsewhere in the United States. *See* Doc. 667–1 at 5–6. Because the government was unwilling or unable to comply with each of these conditions, the meeting did not occur. The government advised the Court at the hearing on October 28, 2011, that the meeting had not taken place. Prior to the hearing, however, the government provided a memorandum setting forth additional factual concessions and stipulations. *See* Doc. 674. The Court concluded at the hearing on October 28, 2011 that further meetings and hearings would not result in additional progress toward resolution of the discovery issues and stated that it would proceed to rule on Defendant's pending motion. Doc. 592. The Court also stated it would determine whether an *ex parte* hearing was required in connection with its ruling on the motion.

On November 16, 2011, the Court entered an order scheduling an *ex parte* hearing. Doc. 700. The Court explained that the purpose of the hearing would be to allow the government to present evidence in support of its claim that information sought by Defendant is subject to a qualified law enforcement privilege. The order was erroneously labeled *Ex Parte* and was therefore sealed. The Court recognized this error as it prepared this order, and has corrected the error by removing the sealed status of the order so that it is now available through the Court's docket.

The Court held an *ex parte* hearing with the government on December 14, 2011. FBI Supervising Agent Bradley Morrison provided testimony in which he explained the nature of the equipment used in this case, how it was used, and why information sought by Defendant is law enforcement sensitive. At the end of the hearing, the Court made a finding on the record that the information described during agent Morrison's testimony is law enforcement sensitive and therefore entitled to a qualified law enforcement privilege under the *Roviaro* line of cases. A more complete description of the Court's findings will be provided below.

On November 10, 2011, Defendant filed his motion for additional discovery. Doc. 697. The motion identifies some additional categories of information sought by Defendant. This motion will be resolved in part below. The Court will await the government's response to the motion and Defendant's reply before ruling on the remaining issues. In addition, the government and Defendant have made other filings related to the pending discovery issues. *See* Docs. 698, 711, 716.

III. Ex Parte Hearing.

Although the government has produced substantial information regarding its efforts to locate Defendant's aircard, Defendant seeks highly specific and detailed information concerning the government's technology and techniques. For example, Defendant seeks the "manufacturer model information, instructions manuals, operations manuals, user manuals, schematics, patent information, proprietary information, trade secrets, test data, the actual physical devices themselves and the calibration certification information for each device used" by the government to locate the aircard, as well as the "user manuals and/or other documents explaining the ***994** general operation/functionality of the software for the devices and end user instructions." Doc. 698 at 6. Defendant also seeks "all evidence relating to the real-time and historical geolocation techniques (e.g., triangulation techniques) and radio wave collection methods (e.g., cell site emulation, interrogation, active approach) used by the government agents/personnel and by the wireless device locators while searching for the aircard." *Id.* at 7. Defendant also seeks disclosures of the identities, training, and experience of agents and other personnel who operated the equipment when locating his aircard. Doc. 592 at 49–53.

At the *ex parte* hearing, Agent Morrison explained how the equipment used in locating the aircard operates, how it was used in this particular case, and why disclosure of information regarding the equipment and techniques used to locate the aircard would hamper future law enforcement efforts. Agent Morrison also explained the training and skill required to operate the equipment, that only a limited number of agents have acquired the training and skill, and why disclosure of their identities would jeopardize their safety and make it impossible for the FBI to use these agents in future surveillance operations, eliminating them as valuable law enforcement assets.

The Court found Agent Morrison testimony to be credible. The Court concludes that disclosure of the

additional information sought by Defendant would compromise the ability of the FBI and other law enforcement agencies to combat crime. Disclosure would enable adversaries of law enforcement to defeat electronic surveillance operations and to avoid detection by such surveillance. Disclosure of the information would also place law enforcement agents at risk when conducting such surveillance. Disclosures of the specific identities of agents involved in this operation could jeopardize their safety and would effectively eliminate them as law enforcement assets used in electronic surveillance. With only a limited number of individuals trained and skilled in operating this equipment, disclosure would therefore seriously hamper law enforcement efforts. The Court's findings with respect to specific categories of information will be identified below.

Defendant argues that the equipment used by the government in this case is publicly known and publicly available. Defendant has provided extensive technical information concerning devices available on the market that can be used to locate cell phones and aircards. He has provided information concerning Harris Corporation, a manufacturer of such devices, as well law enforcement materials reflecting the use of some technical devices. *See* Docs. 587, 592. The government, however, has not disclosed the specific devices used in locating Defendant's aircard or how the equipment was operated, and the Court concludes that the precise equipment used by the FBI and the precise manner in which it was used constitutes sensitive law enforcement information. Disclosing the particular equipment used, and how it was used, would disclose how the FBI seeks to track mobile electronic devices such as the aircard. Even if some of the technology were publicly available, the precise technology used by the FBI in this case and the precise manner in which it was used, if disclosed, would educate the public and adversaries of law enforcement on how precisely to defeat FBI surveillance efforts. The Court is not persuaded by Defendant's arguments that the privilege is inapplicable because modern surveillance technology is widely understood.

The government's claim of privilege in this case is based solely on the *Roviaro* line of cases. The government has not ***995** invoked a state secrets or executive privilege. Although the government has mentioned from time to time that the surveillance techniques used in this case are also used in matters of national security, the government has made clear that its claim of privilege in this case is based solely on *Roviaro* and its progeny. The government made this clear in the hearing on May 5, 2011, and at the *ex parte* hearing on December 14, 2011. Thus, Defendant's arguments that the privilege claim must be rejected because the government has failed to comply with procedural requirements for asserting national security or executive privileges (*see, e.g.,* Docs. 698, 715), are unpersuasive. Defendant's motion asking the Court to reject the government's privilege claim for failure to follow such procedures (Doc. 715) will therefore be denied.

IV. Factual Agreements.

As noted above, the Court and the parties reached a number of factual agreements during the hearing on September 22, 2011. The purpose of these agreements was to resolve some of Defendant's outstanding discovery requests while enabling him to make his Fourth Amendment arguments. In addition, the government made certain factual admissions before the hearing (Doc. 602) and additional concessions after the hearing (Doc. 674). Thus, for purposes of the Fourth Amendment arguments in this case, the following facts are taken as established:

A. The mobile tracking device used by the FBI to locate the aircard functions as a cell site simulator. The mobile tracking device mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard. Doc. 602 at 3.

B. The FBI used the mobile tracking 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. *Id.;* Doc. 644 at 2.

C. The mobile tracking device was used by government agents on foot within Defendant's apartment complex. Doc. 644 at 2.

D. The mobile tracking device generated real time data during the tracking process. *Id.*

E. All data generated by the mobile tracking device and received from Verizon as part of the locating mission was destroyed by the government shortly after Defendant's arrest on August 3, 2008. *Id.;* Doc. 674–1 at 3. The mobile tracking 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. Doc. 644 at 2–3.

F. 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. *Id.* at 3.

G. The mobile tracking device caused a brief disruption in service to the aircard. Doc. 674 at 2 (as clarified at the October 28, 2011 hearing).

H. During the tracking operation, the FBI placed telephone calls to the aircard. Doc. 697 at 10 n. 8.

In addition to these factual agreements, the government has made other concessions for purposes of Defendant's Fourth Amendment argument.

First, for purposes of Defendant's motion to suppress, the government agrees that the Court may assume that the aircard tracking operation was a Fourth ***996** Amendment search and seizure. Doc. 674 at 1.[6]

Second, the government agrees to rely solely on the Rule 41 tracking warrant, application, and affidavit (CR08–90330–MISC–RS) 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. Doc. 674 at 2.

Third, the Court may assume that, at the conclusion of the July 16, 2008 search efforts, the mobile tracking device had located the aircard precisely within Defendant's apartment—Unit 1122 of the Domicilio Apartments. *Id.*

Fourth, as noted above, the government will not rely on facts presented during the *ex parte* hearing to rebut any of Defendant's factual arguments. The government will rely only on evidence disclosed to Defendant. *Id.*

V. Rulings on Defendant's Initial Motion (Doc. 592).

With the applicable legal standards, the Court's findings from the *ex parte* hearing, and the government's factual admissions and concessions in mind, the Court will now address Defendant's various discovery requests. The Court will use the same letter and number designations set forth in Defendant's motion (Doc. 592).

A. Individuals Involved in the Aircard Search.

Defendant seeks the disclosure of all evidence related to the identities and roles of the witnesses to the aircard search. Doc. 592–1 at 46. Defendant seeks this information so that he may question agents involved in efforts to locate the aircard. Questioning the agents will be relevant, Defendant contends, in order to determine whether the search was conducted on foot or by helicopter, to establish the date and time of data destruction, to rebut any government reliance on the good faith exception to the warrant requirement, and to challenge the government's claim of good faith in destroying ***997** data generated during the search effort. *Id.* at 46–53.

[11] [12] As an initial matter, the Court concludes that Defendant has not shown his right to this information under Rule 16(a)(1)(E)(i). That rule requires the government to disclose documents or other tangible objects within its possession, custody, or control. The rule does not require the government to create documents that may provide information a defendant desires to obtain, nor does it require the government to present agents or witnesses for interviews or in-court examination. *United States v. Mahon*, No. CR09–0712–PHX–DGC, 2011 WL 5006737 at *3 (D.Ariz., Oct. 20, 2011) (citing cases). The rule "triggers the government's disclosure obligation only with respect to documents within the federal government's actual possession, custody or control." *United States v. Gatto*, 763 F.2d 1040, 1048 (9th Cir.1985).

[13] In addition, the Court finds on the basis of Agent Morrison's testimony at the *ex parte* hearing that the identities of individuals involved in locating the aircard is law enforcement sensitive information. Agent Morrison testified credibly that revealing the identities of these individuals could compromise their safety during future law enforcement missions. He also testified credibly that if the identities of these individuals were disclosed, they no longer could safely participate in such missions, a fact that would seriously limit the government's law enforcement capabilities given the unique training and skill set of individuals involved in the operation. The Court finds that the identities of individuals involved in locating the aircard are subject to a *Roviaro* privilege. For reasons that follow, the Court also finds that Defendant has not made the showing required to overcome the privilege.

[14] Determining whether the search in this case was conducted on foot or by helicopter would not be helpful or relevant to the defense. The government has conceded that the search was conducted, in part, on foot. It also has asserted that no helicopter was used. Doc. 602 at 3. Defendant's only reason for seeking to establish that a helicopter was used is his reliance on the Supreme Court's holding in *Florida v. Riley*, 488 U.S. 445, 109

S.Ct. 693, 102 L.Ed.2d 835 (1989), that use of a helicopter to conduct surveillance over a private residence constituted a Fourth Amendment search. Doc. 592–1 at 49. Because the government has conceded that the search for the aircard constituted a Fourth Amendment search, use of a helicopter would thus add nothing to Defendant's motion to suppress.

Questioning agents to determine the date and time of data destruction would not be helpful or relevant to the defense. The government has conceded that all data generated during the search for the aircard was destroyed shortly after Defendant's arrest on August 3, 2008. Doc. 644 at 2.

Questioning agents in order to challenge the government's reliance on a good faith exception to the warrant requirement would not be helpful or relevant to the defense because such a good faith exception depends on the *objective* reasonableness of the law enforcement officers' actions. *See United States v. Leon*, 468 U.S. 897, 919 n. 20, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984) ("We emphasize that the standard of reasonableness we adopt is an objective one. Many objections to a good-faith exception assume that the exception will turn on the subjective good faith of individual officers. Grounding the modification in objective reasonableness, however, retains the value of the exclusionary rule as an incentive for the law enforcement profession as a whole to conduct themselves in accord with the Fourth ***998** Amendment.") (quotation marks and citations omitted).

Finally, the Court cannot conclude that Defendant's desire to show the bad faith destruction of potentially exculpatory evidence justifies disclosure of the identities of agents who located the aircard. The government has conceded that all real time data generated during the aircard locating effort was destroyed. The government has asserted that FBI policy requires technical personnel to purge all data generated during such a locating effort because the data includes electronic serial numbers or equivalent information from all wireless devices in the area searched by the FBI that subscribe to a particular provider, including those of innocent, non-target devices. Doc. 674–1 at 3. The government also notes that the Northern District of California court order that authorized use of the mobile tracking device required, "at the conclusion of the tracking mission," that "the investigating agency shall expunge all the data obtained by this Court Order[.]" Doc. 470–1 at 30.

Moreover, the Court concludes that questioning agents is not necessary for Defendant to make his bad faith argument. Such an argument can be made through other means, a fact the Court may consider in conducting a *Roviaro* analysis. *See Harley*, 682 F.2d at 1020. The government has described the kind of data collected during the tracking mission and has conceded that it was destroyed shortly after Defendant's arrest on August 3, 2008. Doc. 644 at 2. The government has also disclosed emails related to the tracking mission from which Defendant already has argued that the government acted in bad faith when it destroyed the data. *See* Doc. 595–1 at 7. Given the preponderance of the evidence standard that will apply to Defendant's motion to suppress and the lower level of disclosure required for suppression hearings as opposed to trial, the Court concludes that sufficient information has been disclosed for Defendant to argue effectively that data collected during the tracking mission was destroyed in bad faith.

B. Unredacted Documents Related to Court Orders.

Defendant asks the Court to compel the government to disclose unredacted applications and attachments to orders 08–90330–MISC–RS and 09–90331–MISC–RS issued by the court in the Northern District of California. Doc. 592–1 at 55. The government stated during the *ex parte* hearing that these unredacted documents were being produced to Defendant. As a result, the Court concludes that this request is moot.

C. Materials and Evidence Collected Under Order 08–90330–MISC–RS.

Defendant asks the Court to compel production of all materials, returns, and evidence related to order 08–90330–MISC–RS obtained during location of the aircard. The government already has produced much of this information, including applications for the warrants and orders, copies of warrants and orders, technical data generated during the aircard locating mission, and email and written communications among counsel and FBI agents related to the mission. Defendant seeks production of detailed technical information related to the devices and techniques used during the mission.

[15] As noted above, the Court finds that these devices and techniques are subject to a *Roviaro* privilege. For reasons explained credibly by Supervising Agent Morrison at the *ex parte* hearing, their disclosure would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection. For reasons that follow, the Court also ***999** concludes that the arguments provided by Defendant for overcoming the privilege are not sufficient.

First, Defendant argues that this information is needed for him to prove that the mobile tracking device located the aircard precisely within Unit 1122 of the Domicilio Apartments. As noted above, however, the government has conceded that the Court may assume this occurred for purposes of Defendant's Fourth Amendment argument.

Second, Defendant asserts that this information will allow him to show that the government verified the location of the aircard within Unit 1122 on July 25 and 28, 2008, which required the mobile tracking device to locate the aircard precisely within the apartment. The government's concession resolves this need as well.

Finally, Defendant argues that this information will show that the mobile tracking device generated real time data that was destroyed by the government. The government has conceded, however, that the mobile tracking device generated real time data and that data generated by the device and received from Verizon were destroyed shortly after Defendant was arrested on August 3, 2008. Doc. 644 at 2.

Because each of Defendant's reasons for obtaining this information has been satisfied by the government's concessions, no additional disclosure will be required.

D. Evidence Relating to Geolocation Techniques.

[16] Defendant seeks all evidence relating to the real time and historical geolocation techniques used by the government, which Defendant refers to as triangulation techniques, as well as radio wave collection methods (*e.g.*, cell site emulation, interrogation, active approach) used by the government while searching for the aircard. Doc. 592–1 at 66.

On the basis of testimony provided by Supervising Agent Morrison at the *ex parte* hearing, the Court concludes that this information is subject to the *Roviaro* privilege. Disclosure of techniques used by the government to locate the aircard would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection. For reasons that follow, the Court also concludes that the arguments provided by Defendant for overcoming the privilege are not sufficient.

[17] First, Defendant seeks to prove that the government obtained non-public keys, codes, masks, and data. Defendant primarily seeks this information to show that locating the aircard was sufficiently intrusive to constitute a Fourth Amendment search. The government has conceded, however, that use of the mobile tracking device constituted a search for purposes of the Fourth Amendment.

Defendant also seeks this information to show that the warrant received from the Northern District of California was not sufficiently particular and that government agents exceeded the scope of the warrant in their search for the aircard. Defendant has ample alternative methods of making this argument. *See Harley*, 682 F.2d at 1020. Defendant's motion and his supplemental filings contain extensive technical data regarding cell tower simulation technology. *See, e.g.*, Docs. 587, 595. Defendant cites product brochures, patent applications, articles, websites, and textbooks to show the manner in which cell tower emulation occurs. Defendant has been able to access this information because the Court has arranged for him to have a laptop computer and related equipment at the federal facility in which he is housed, has appointed investigators and shadow counsel to assist in preparing his defense, has funded Defendant's purchase of text books, ***1000** has arranged for the pick-up by and delivery of materials from and to his defense team, has authorized the retention of an electronic surveillance expert, and has required the federal facility to permit Defendant to confer with his expert and other members of his defense team without his calls being monitored or recorded. Utilizing these resources, Defendant has compiled an impressive array of information from which he asserts that the government necessarily obtained access to non-public keys, codes, masks, and data. *See, e.g.*, Docs. 587, 595. Because Defendant has ample alternative means of making his arguments with respect to the particularity of the warrant and the scope of the search, the Court concludes that he has not made a showing sufficient to overcome the privilege.

Second, Defendant argues that he needs this information to distinguish between the mobile tracking device used to locate his aircard and the pen register trap and trace device authorized by order 08–90331–MISC–RS. The government has conceded, however, that it will not rely on this order as a justification for use of the mobile tracking device. Rather, the government will rely solely on order 08–90330–MISC–RS as the warrant that justified use of the mobile tracking device.

Third, Defendant argues that he needs this information because "there is a 'possibility' that the government used passive eavesdropping in addition to interrogation in order to locate the aircard." Doc. 592–1 at 68. As noted above, however, Defendant must make a threshold showing of materiality in order to obtain discovery under Rule 16(a)(1)(E)(i). *Santiago*, 46 F.3d at 894; *Mandel*, 914 F.2d at 1219. A mere "possibility" is not sufficient.

Fourth, Defendant claims that he needs this information to show that the government instructed Verizon Wireless to send messages to the aircard in order to facilitate use of the mobile tracking device. Defendant identifies 11 specific actions that would have been taken as part of this effort. Doc. 592–1 at 69–70. He cites extensively to technical documents to demonstrate that such messages from Verizon would have been necessary. *Id.* To the extent that Defendant seeks such information to show that use of the mobile tracking device constituted a Fourth Amendment search (Doc. 592–1 at 86–87), such proof is unnecessary given the government's concession that a Fourth Amendment search occurred. To the extent Defendant seeks such information to argue that the search exceeded the scope of the relevant warrants and court orders, he has alternative means for making this argument. As demonstrated by his extensive technical citations, Defendant has ample evidence with which to assert that Verizon sent messages to the aircard that required the aircard to engage in various functions. Doc. 592–1 at 68–70. Because Defendant already possesses such alternative information as a result of the substantial resources made available to him in this case, the Court concludes that production of such information from the government is not necessary. *See Harley*, 682 F.2d at 1020.

Fifth, Defendant argues that he needs this information to prove that the government used cell site emulation, aircard emulation, and forced registration to locate the aircard. Doc. 592–1 at 71. Citing several sources, including a publicly available government manual, Defendant argues that cell site emulation and forced registration were used. Alternatively, Defendant asserts that the government may have used a man-in-the-middle attack.

Defendant claims that forcing the aircard to register constituted an unreasonable search of the aircard and the computer, and took over the computer in other ***1001** ways. Doc. 592–1 at 71–72, 85–87. To the extent Defendant seeks this information to show that a search occurred under the Fourth Amendment, that need is eliminated by the government's concession that such a search occurred.

Moreover, the government has conceded that the mobile tracking device simulated a cell site (Doc. 602 at 3) and that use of the equipment resulted in a brief disruption of the aircard's service (Doc. 674 at 2). To the extent Defendant wishes to argue that the government also engaged in a man-in-the-middle attack—a fact denied by the government (Doc. 674–1 at 2–3)—he clearly has alternative means for making the argument. *See* Doc. 592–1 at 71–72; Doc. 698 at 4–6. Because Defendant possesses ample alternative evidence from which to make this argument, he has not made a sufficient showing to overcome the privilege. *Harley*, 682 F.2d at 1020.

Sixth, Defendant argues that this information will show that the government sent interrogation signals to the aircard, that these interrogation signals penetrated the walls of Defendant's apartment, and that use of the mobile tracking device therefore constituted a Fourth Amendment search. Doc. 592–1 at 72–73, 89–90. But the government has already conceded the use of the mobile tracking device constituted a search under the Fourth Amendment. Moreover, the government has stipulated that the mobile tracking device simulated a Verizon cell tower, sent signals to the aircard, and received signals in response. Docs. 602 at 3; 644 at 2–3. The government has also conceded that agents made phone calls to the aircard during the tracking operation. Doc. 697 at 10 n. 8. These concessions, as well as the substantial body of technical information compiled by Defendant, clearly enable him to make arguments that the mobile tracking operation exceeded the scope of the relevant warrants and orders.

Seventh, Defendant argues that this information will allow him to show that the government used time-of-flight, power-distance, angle-of-arrival, statistical functions, and data fusion in order to triangulate the aircard's location. Doc. 592–1 at 73–77. Defendant argues that these are standard geolocation measurement techniques used by companies that manufacture equipment used by the government. *Id.* Defendant contends that these techniques, which constitute triangulation, violate one of the orders from the Northern District of California that specifically prohibited triangulation. *See* Doc. 470–2 at 8. The Court concludes that Defendant has ample information from which to make this argument. His motion cites patents, legislative documents, documents produced by the government, and textbooks to support his triangulation arguments. *See* Doc. 592–1 at 73–77.

Eighth, Defendant argues that he needs this information to show that the government changed locations as it used the mobile tracking device in order to take measurements in multiple locations. Doc. 592–1 at 77–78. The government has conceded this fact. *See* Docs. 602 at 3, 644 at 2.

Finally, Defendant argues that he needs this information to show that the government caused an increase in power consumption by the aircard, an interruption in aircard service, and aircard transfer rates to fall. The government has conceded that the mobile tracking device caused a brief interruption in the aircard's service. Doc. 674 at 2

(as clarified at the October 28, 2011 hearing). To the extent Defendant wishes to contend that the tracking device caused an increase of power usage or a decrease in transfer rates, he has ample alternative evidence with which to make this argument. *See* Doc. 592–1 at 78–80.

***1002 E. Path of Movement Information.**

[18] Defendant seeks disclosure of information showing the geographical paths of the wireless device locators while searching for the aircard. Doc. 592–1.

On the basis of testimony provided by Supervising Agent Morrison at the *ex parte* hearing, the Court concludes that the precise techniques used by agents to locate the aircard, including their path of movement, is subject to the *Roviaro* privilege. Disclosure of such techniques would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection. For reasons that follow, the Court also concludes that the arguments provided by Defendant for overcoming the privilege are not sufficient.

Defendant seeks this information to prove that the government located the aircard within Unit 1122. As noted above, however, the government has conceded for purposes of Defendant's Fourth Amendment argument that the aircard was located precisely within Unit 1122. Defendant also seeks the information to prove that triangulation techniques were used. Doc. 592–1 at 96. As noted above, Defendant has ample alternative sources from which to argue that triangulation occurred.

F. Evidence Related to Specific Devices.

[19] Defendant seeks production of all evidence relating to the specific mobile tracking device used by the government, including user manuals, test data, and related software. Doc. 592–1 at 97. Defendant states that he needs this information because "the requested evidence may reveal additional Fourth Amendment violations the defendant is currently unaware of." *Id.* As noted above, however, Rule 16(a)(1)(E)(i) does not authorize a fishing expedition. Defendant must make a threshold showing of materiality before disclosure is required. *Santiago,* 46 F.3d at 894; *Mandel,* 914 F.2d at 1219.

[20] On the basis of testimony provided by Supervising Agent Morrison at the *ex parte* hearing, the Court concludes that this information is subject to the *Roviaro* privilege. Disclosure of the specific equipment used by the government to locate the aircard would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection. For reasons that follow, the Court also concludes that the arguments provided by Defendant for overcoming the privilege are not sufficient.

Defendant seeks this information to show that the equipment runs afoul of various federal statutes. Doc. 592–1 at 98–100. As his very argument demonstrates, however, Defendant has ample alternative information with which to make this argument. *Id.*

Finally, Defendant asserts that this information will permit his expert to determine how the equipment operated and, therefore, to show that it located the aircard precisely within Unit 1122. The government has conceded, however, that the Court may assume the aircard was located precisely within Unit 1122.

G. Pen/Trap Network Architecture.

[21] Defendant seeks disclosure of all evidence related to the Pen/Trap Network Architecture in place between July 16, 2008 and August 1, 2008. Doc. 592–1 at 105. Defendant asserts that this information will permit him to show that the government did not comply with the "after receipt and storage" requirement of order 08–90331–MISC–RS. *Id.* He also asserts that this information will bear upon the good faith exception to the warrant requirement.

***1003** On the basis of testimony provided by Supervising Agent Morrison at the *ex parte* hearing, the Court concludes that this information is subject to the *Roviaro* privilege. Disclosure of the specific equipment and techniques used by the government to locate the aircard would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection. The Court also concludes that the reasons provided by Defendant for overcoming the privilege are not sufficient. Defendant has ample alternative information with which to make this argument. He cites information from the Telecommunications Industry Association, court orders in other cases, technical information, and federal statutes to assert that the provisions of the court order were violated in this case. Doc. 592–1 at 105–110.

H. Production of Original Storage Devices.

[22] Defendant seeks production of the original storage devices used to log the aircard related messages and to create various data files produced to Defendant by the government. Defendant seeks to have his mobile telecommunications expert conduct a forensic analysis of the original storage devices so that he may determine if

data was deleted or altered by government agents. Doc. 592–1 at 110.

On the basis of testimony provided by Supervising Agent Morrison at the *ex parte* hearing, the Court concludes that this information is subject to the *Roviaro* privilege. Disclosure of the specific devices used by the government to locate the aircard would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection. For reasons that follow, the Court also concludes that the arguments provided by Defendant for overcoming the privilege are not sufficient.

[23] Defendant has not made the threshold showing of materiality required for production of these devices under Rule 16(a)(1)(E)(i). Moreover, the government has conceded that all data generated during the efforts to locate the aircard were destroyed shortly after Defendant's arrest on August 3, 2008. This concession enables Defendant to construct legal arguments arising from the destruction of such evidence.

I. Communication Documents.

[24] Defendant seeks production of all communications between the government and private entities associated with Verizon Wireless and various companies that manufacture electronic surveillance equipment. Doc. 592–1 at 111. Defendant seeks this information "because it will provide further information on all other categories of withheld evidence being requested through this motion." *Id.* Defendant asserts that this "is a reasonable assumption considering the government is withholding the requested communications based on the same claim of privilege asserted over the other withheld evidence." *Id.* Defendant has not made the threshold showing of materiality required for production under Rule 16(a)(1)(E)(i). *Santiago,* 46 F.3d at 894; *Mandel,* 914 F.2d at 1219.

Moreover, the Court concludes on the basis of testimony provided by Supervising Agent Morrison at the *ex parte* hearing that this information is subject to the *Roviaro* privilege. These communications would concern equipment and techniques used by the government to locate the aircard, and disclosure of such equipment and techniques would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection. Defendant's generic argument that disclosure would provide "further information" is not sufficient to overcome the privilege.

***1004 J. Unredacted Documents.**

[25] Defendant seeks "unredacted and unsummarized documents related to the government's motion to search for and locate the aircard." Doc. 592–1 at 111. Defendant seeks this information "because it will provide further information on all other categories of withheld evidence being requested through this motion." *Id.* The possibility of "further information" does not satisfy the threshold showing of materiality required for production under Rule 16(a)(1)(E)(i). *Santiago,* 46 F.3d at 894; *Mandel,* 914 F.2d at 1219.

[26] Moreover, the Court concludes on the basis of testimony provided by Supervising Agent Morrison at the *ex parte* hearing that this information is subject to the *Roviaro* privilege. These documents concern equipment and techniques used by the government to locate the aircard, and disclosure of such equipment and techniques would hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection. Defendant's generic argument that disclosure would provide "further information" is not sufficient to overcome the privilege.

VI. Defendant's Motion for Additional Discovery.

As noted, Defendant filed a motion for additional discovery on November 10, 2011. Doc. 697. The Court will rule on some issue raised in this motion.

A. Text Messages.

Defendant seeks production of all text messages sent to or from FBI agents regarding the aircard locating mission. The Court will await the response and reply before ruling on this issue.

B. FBI Destruction of Evidence Policy.

[27] Relying on an article in The Wall Street Journal regarding this case, Defendant asserts that the government possesses a written policy regarding the destruction of data in connection with efforts to locate the aircard. Defendant seeks a copy of that policy, but he has not made the threshold showing of materiality required for disclosure under Rule 16(a)(1)(E)(i). *Santiago,* 46 F.3d at 894; *Mandel,* 914 F.2d at 1219.

Defendant candidly notes that the government's concession that the aircard was located precisely within his apartment "*may* have eliminated the defendant's need for the destroyed evidence." Doc. 697 at 4 (emphasis in

original). Defendant goes on to argue, however, that *even if there is no prejudice to his defense* in light of the government's concession, he will argue "for suppression of secondary evidence based on *United States v. Flyer,* 633 F.2d [F.3d] 911, 916 (9th Cir.2011)." Doc. 697 at 4. *Flyer,* however, states that the suppression of secondary evidence turns, among other things, on "the degree of prejudice to the accused." 633 F.3d at 916. *Flyer* thus provides no basis for disclosure of the policy, in the absence of prejudice, under Rule 16.

Defendant also asserts that the FBI policy likely resulted in the violation of constitutional rights of other individuals, a fact that warrants dismissal of this case as "a strong deterrent of this government practice in the future." Doc. 697 at 4. But Defendant cites no authority for the proposition that this case may be dismissed as a sanction for violating the constitutional rights of others. This argument thus provides no basis for disclosure of the policy under Rule 16.

C. Copies of Proposed Orders.

Defendant asks for production of any proposed orders submitted to judges in the Northern District of California, arguing that such proposed orders will demonstrate ***1005** that government agents knew they were acting in bad faith. Doc. 697 at 5–6. The Court will await the government's response and Defendant's reply before ruling on this issue.

D. Calls to the Aircard.

[28] Defendant seeks production of evidence regarding the FBI's need to call the aircard over a six-hour period while using the mobile tracking device. Doc. 697 at 6. Specifically, Defendant has asked the government to question FBI agents for an explanation of various issues, including the degree of interruption with the aircard, whether the mobile tracking device was forwarding signals to Verizon Wireless, whether the device was denying the aircard Internet access, and why the agents needed to call the aircard repeatedly over a six hour period. Defendant then asks the government to compile the answers and forward them to him.

As previously noted, Rule 16(a)(1)(E)(i) only requires the government to produce documents and tangible things in its possession. Defendant's demand "sound[s] more like civil interrogatories under Civil Rule 33 than document requests under Criminal Rule 16(a)(1)(E)." *United States v. Cameron,* 672 F.Supp.2d 133, 137 (D.Me.2009). "The Court is unaware of any authority that would require the Government to manufacture a document in order to respond to a Rule 16(a)(1)(E) document request[.]" *Id.* Stated differently, the government has no obligation under Rule 16 to interview agents, compile information, and forward the information to Defendant. *Id.*

Defendant asserts that he needs the information to establish that a Fourth Amendment seizure of the aircard occurred in this case. The government has conceded, however, that the aircard locating mission constituted a search and seizure for purposes of the Fourth Amendment.

Moreover, for reasons discussed above, the Court concludes that Defendant has ample information from government disclosures and his extensive command of technical information to construct whatever arguments he wishes to assert concerning the Fourth Amendment implications of the aircard locating mission.

VII. Next Steps.

For reasons set forth above, the Court will deny Defendant's motion for discovery and deny in part his motion for additional discovery. The Court concludes that Defendant has ample information with which to construct his Fourth Amendment arguments. Because nearly two years have been devoted to this discovery effort, including numerous letters, motions, memoranda, and court hearings, the Court will not entertain further discovery motions. Defendant must construct his Fourth Amendment argument on the basis of information currently in his possession.

The Court will require that Defendant file his Fourth Amendment motion to suppress by **February 17, 2012.** The Court views this as a reasonable deadline given Defendant's full-time access to a laptop computer and the fact that he already has largely compiled relevant information and constructed relevant legal arguments.

Defendant's motion to suppress shall not exceed 50 pages in length.[7] The Court imposes this page limitation because of Defendant's tendency to file extremely long documents, such as his motion for production which exceeded 100 pages. ***1006** Moreover, Defendant at one time suggested that his motion to suppress could range up to 400 pages. Fifty pages will allow Defendant ample opportunity to present all of his Fourth Amendment arguments. In preparing his motion, Defendant shall not incorporate by reference arguments or factual assertions made in any other motions or memoranda as he often has done in past.

This case has been pending since July of 2008. Defendant has been incarcerated for more than three years awaiting trial. The Court has afforded Defendant significant resources and extensive time to prepare his Fourth Amendment arguments because the Court recognizes that those arguments are critical to his defense. The time has come to resolve Defendant's motion to suppress and, if the government's case survives, to move on to trial.

IT IS ORDERED:

1. Defendant's motion for discovery (Doc. 592) is **denied.**

2. Defendant's motion for additional discovery (Doc. 697) is **denied** in part as set forth above. The Court will rule on the remaining portions of this motion after the government responds and Defendant replies.

3. Defendant's motion for disclosure based on the government's failure to properly invoke claims of privilege (Doc. 715) is **denied.**

Excludable delay pursuant to U.S.C. § 18:3161(h)(1)(D) is found to commence on 8/12/11 to 1/4/12.

Footnotes

1 Defendant has filed a number of other motions related to his discovery disagreement with the government. *See* Docs. 593, 595, 596, 597, and 605. The Court will enter a separate order resolving those motions.

2 The government argued in its initial response to Defendant's discovery motion that a criminal defendant must show a "compelling need" for information before the privilege gives way. Doc. 602. This clearly is not the test. *Roviaro* held that where the information "is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the privilege must give way." *Id.* at 60–61, 77 S.Ct. 623. This is the test the Court will apply throughout this order.

3 After the aircard locating efforts had been completed, the government obtained a search warrant for Defendant's apartment. The Court understands the government will seek to introduce evidence obtained from that search, including Defendant's laptop computer, during trial. While the search of the apartment may have been illegal if it was the fruit of an illegal search for the aircard, that question will be decided at the suppression hearing. If Defendant's motion to suppress is not successful, there will be no need to present evidence from the aircard locating mission during trial.

4 The government has acknowledged as much: "for the purpose of defendant's pending motions to compel discovery and his prospective motion to suppress, the United States does not expect to present facts in an *in camera* proceeding that it would then request the Court to consider for the purpose of rebutting any of defendant's claims without disclosing those facts to the defendant." Doc. 674 at 2.

5 Citations in this order are to page numbers applied at the top of each document by the Court's CMECF system, not to page numbers on the original documents.

6 While making this concession, the government states that it is reserving its right to assert that Defendant lacks standing to make certain Fourth Amendment arguments. Doc. 674 at 1 n. 1. As Defendant notes, such a reservation of rights can be viewed as inconsistent with the government's concession. Typically, courts hold that a defendant lacks standing when he has no subjective and reasonable expectation of privacy in the area searched or the evidence seized. *See, e.g., Minnesota v. Carter,* 525 U.S. 83, 91, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (no reasonable expectation of privacy and thus no standing to challenge the admissibility of drug evidence seized on the premises); *Rawlings v. Kentucky,* 448 U.S. 98, 104–05, 100 S.Ct. 2556, 65 L.Ed.2d 633 (1980) (no subjective expectation of privacy and thus no standing to challenge admissibility of drugs seized from acquaintance's purse). At the same time, whether a Fourth Amendment search occurs depends, in part, on whether the defendant had a subjective and reasonable expectation of privacy in the place or thing searched. *See, e.g., United States v. Ziegler,* 474 F.3d 1184, 1189 (9th Cir.2007). Thus, if the government is conceding that the search which located Defendant's aircard constituted a search and seizure for purposes of the Fourth Amendment, it necessarily must be conceding that Defendant had a reasonable expectation of privacy in the aircard. The Court understands this to be the government's concession. If the government is not making this concession—a concession that would seem to defeat any standing arguments that might be asserted by the government—then the premise for this order may well be incorrect. The Court will proceed on the assumption that the government is conceding, for purposes of Defendant's Fourth Amendment arguments, that the search for the aircard was a search within the meaning of the Fourth Amendment.

7 The 50–page limitation does not include exhibits. Defendant may submit exhibits in support of his motion. The exhibits should not contain additional legal arguments, and should be cited specifically in Defendant's motion.

End of Document