# Table of Contents

I. INTRODUCTION..................................................................................................................1

II. Technical Explanations........................................................................................................4

A. Electromagnetic radiation in the radio frequency band.........................................................5

B. The 1xEV-DO cellular communications system deployed by Verizon Wireless...........8

1. Origins of the 1xEV-DO cellular communications system..............................................8

2. Basic hardware elements of a 1xEV-DO Rel. 0 compatible cellular data network.............14

   a. The Access Terminal (AT)..............................................................................................14

   b. The Access Network (AN)............................................................................................17

   c. Access Networks (a.k.a. cell sites) in the geolocation context..................................19

3. How relevant 3GPP2 technical standards dictate communications between a 1xEV-DO Rel. 0 Access Terminal and a 1xEV-DO Rel. 0 Access Network............................21

   a. Over-the-Air Service Provisioning (OTASP) and Over-the-Air Parameter Administration (OTAPA)...............................................................21

   b. Access Terminal Initialization State procedures: identifying and acquiring a 1xEV-DO Rel. 0 Access Network after initial power-on...............................26

      i. Network Determination Substate...............................................................................26

      ii. Pilot Acquisition Substate.......................................................................................28

      iii. Synchronization Substate......................................................................................31

   c. Access Terminal Idle State procedures: preparing to open a connection and opening a connection with a 1xEV-DO Rel. 0 Access Network.........................32

      i. Receiving, processing, and storing to internal storage the Access Network's Overhead Messages.................................................................33

      ii. Transmission of Access Probes to the Access Network to initiate session establishment and open a connection......................................................35

      iii. Establishing an open session with the Access Network.........................................39

      iv. Application of encryption and authentication keys for use in the security layer........42
v. Obtaining identifying information from Access Terminal hardware using the HardwareIDRequest message..........................49

vi. Opening a connection with the Access Network..........................49

d. Using the Default Route Update Protocol to scan for additional pilots, facilitate sector Route Updates, and send Route Update messages............54

i. Operations of the Default Route Update Protocol specific to the Idle State........................................................................56

ii. Operations of the Default Route Update Protocol specific to the Connected State......................................................58

e. Open-loop and closed-loop power control of Access Terminal transmissions....................................................................60

i. Reverse Access Channel power control...........................................61

ii. Reverse Traffic Channel power control...........................................62

f. Synchronization and timing of transmitted signals..........................64

g. Relevant miscellaneous 1xEV-DO Rel. 0 cellular data network operations..............................................................................65

i. Signal interference........................................................................65

ii. Hybrid Access Terminal operations for non-telephones, e.g., aircards..............................................................................67

C. Explanation of the term “triangulation” applicable to geolocation of radio frequency (RF) signals.......................................................70

D. Cell site information and its use in geolocating wireless devices............74

1. Explanation of the term “cell site information.”..................................74

2. Use of statistical databases containing historical cell site location information to determine a wireless device location signature..........................75

3. Cell site triangulation of a wireless device using cell site location information........................................................................77

E. Global Positioning System (GPS)...........................................................80

F. Explanation of the term “mobile tracking device.”.................................81

G. Air interface surveillance equipment with an emphasis on geolocation of wireless devices..............................................................83

1. Detailed description of the Harris RayFish line of portable/transportable wireless device locators, i.e., the StingRay, KingFish, and related equipment........................................................................86

a. Geolocation measurement techniques used by the StingRay and KingFish while triangulating the location of a wireless device.........................91
i. Signal time-of-flight (TOF) measurements to calculate distance (a.k.a. range).......................................................... 91

ii. Signal strength measurements to calculate distance (a.k.a. range).. 93

iii. Signal angle-of-arrival (AOA) measurements to calculate direction (via a phased array antenna).......................................................... 95

iv. Weighting collected geolocation data and using statistical functions (e.g., average, mean, median, mode, etc.)............................... 98

v. Data fusion of calculated geolocation measurements.......................... 98

b. Radio signal and data collection methods used by the StingRay and KingFish while triangulating the location of a wireless device........... 100

i. Base station surveys........................................................................................................... 100

ii. Cell site emulation and forced connection handoff......................................................... 100

iii. Downloading data from wireless device internal storage............................................ 102

iv. Transmitting interrogation signals in order to force reply signals. 103

v. Approach method for triangulation.............................................................................. 104

vi. Forced transmission power increase........................................................................... 105

H. The FBI Digital Collection Program.............................................................................. 106

1. Digital Collection Systems.......................................................................................... 107

2. DCSNET.................................................................................................................. 108


4. Digital Collection System 3000 (DCS-3000) server.................................................. 113

5. DCS-3000 CDNRS Files.......................................................................................... 116

6. Telephone Applications System.................................................................................. 117

7. FBI Cell Site Database .............................................................................................. 118

8. FBI Wireless Intercept and Tracking Team (WITT)................................................... 120

III. PROCEDURAL HISTORY.......................................................................................... 123

A. D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615 relating to identification of the aircard and destination IP addresses...................... 123

B. D.Ariz. order No. 08-3286MB-LOA, i.e., the destination IP address retroactive order....................................................................................... 125

C. D.Ariz. order No. 08-3298MB-LOA, i.e., historical cell site information order.. 127

D. D.Ariz. order No. 08-7273MB-ECV, i.e., historical cell site information order... 128
E. N.D. Cal. order No. 08-90330MISC-RS, i.e., use and monitor a mobile tracking device order

F. N.D. Cal. order No. 08-90331MISC-RS, i.e., pen register and trap and trace order

G. D. Ariz. Grand Jury subpoena No. 07-03-709 relating to Domicilio electronic gate key access records

H. N.D. Cal. warrant No. 08-70460-HRL (the original unexecuted and amended versions)

IV. GENERAL FACTS

A. Prerequisite background information

1. General background information on the aircard, host laptop computer, aircard account, and aircard service

2. Basis for concluding that the government used the Harris StingRay, KingFish, and related equipment to locate the aircard and the defendant
   a. The government admitted that FBI technical agents used the Harris StingRay to locate the aircard
   b. Heuristics and process of elimination confirms that FBI technical agents used the Harris StingRay, KingFish and AmberJack to locate the aircard

B. The government's mission to locate the aircard and the defendant within his private home residence

1. The government identified the aircard and seized destination IP addresses relating to the defendant's Internet activity

2. The government seized aircard historical cell site location information and conducted historical triangulation / location signature techniques

3. The primary case agents flew from Arizona to California to triangulate the precise location of the aircard and the defendant

4. The FBI technical agents began the real-time portion of the aircard locating mission by conducting base station surveys of all cell sites located in the area covered by the cell tower range chart/map

5. The FBI technical agents had Verizon Wireless reprogram and write data to the aircard so that it would be compatible with the Harris StingRay and KingFish

6. The FBI used the SF-Martinez DCS-3000 Pen/Trap device to obtain real-time cell site sector location information to narrow the geographical area of where to use the StingRay, KingFish, and related equipment

7. The FBI obtained additional real-time aircard data from Verizon Wireless through means other than the SF-Martinez DCS-3000 Pen/Trap device
8. The FBI's surreptitious phone calls booted the aircard off the Internet so that the FBI's StingRay and related equipment could hijack the aircard's signal from Verizon Wireless.

9. The FBI technical agents used the Harris StingRay, KingFish, and related equipment to locate the aircard precisely inside apartment No. 1122.
   a. Cell site emulation and forced connection handoff.
   b. The FBI repeatedly wrote data to the aircard using its StingRay.
   c. The StingRay deactivated 1xEV-DO Rel. 0 security layer encryption during session establishment causing the aircard's signals to be transmitted in plaintext and exposed to third-parties.
   d. The FBI used its StingRay to download data stored on the aircard's internal storage device (i.e., the aircard's Electronic Serial Number (ESN)).
   e. The FBI used the StingRay to send location finding interrogation signals into the defendant's home and into the defendant's aircard in order to search out the location of the aircard and the defendant.
   f. The FBI collected the aircard's signal transmissions sent in response to the location finding interrogation signals sent to the aircard by the FBI via the StingRay.
   g. In order to determine the location of the aircard and the defendant, the FBI conducted triangulation techniques on the aircard's location finding response signals collected by the StingRay.
   h. The FBI technical agents used the KingFish within the Domicilio apartment complex to pinpoint the exact location of the aircard and the defendant within apartment No. 1122.
   i. Whenever the aircard was connected to either the StingRay or KingFish, the FBI denied the aircard access to the Internet (i.e., a denial-of-service attack).
   j. The FBI's StingRay and KingFish relied upon the electricity provided to the aircard by the defendant via his home.
   k. The FBI's StingRay and KingFish sent the aircard commands instructing it to increase its signal transmission power to facilitate more effective geolocation.

10. The government's plan to conceal the real-time portion of the aircard locating mission.

11. The government's failed attempts to visually observe the defendant or anyone entering or leaving apartment No. 1122.

12. The government obtained and used the defendant's historical geolocation.
information via his Domicilio electronic gate key access records..................184
13. The FBI's August 3, 2008 sighting of the defendant within the Domicilio
apartment complex and his subsequent arrest by Santa Clara, CA city police
officers.........................................................187
14. The FBI's August 3, 2008 keyhole search of apartment No. 1122........189
15. The government's destruction of the seized/collected real-time aircard
data..................................................................................................................190
16. The government seized evidence from apartment No. 1122 by executing the
previously returned N.D.Cal. 08-70460-HRL search warrant......................191
17. IRS-CI Agent Daun continues to execute the N.D.Cal. 08-70460-HRL/PVT
search warrant more than three years after the defendant's arrest...............192
18. The government failed to serve the defendant with copies of the aircard
locating mission orders or with receipts of what was seized....................195
V. ARGUMENT................................................................................................195
A. The defendant's property/possessory interests in his home, aircard, host laptop
computer, and electricity provided through his utility account................196
1. The defendant had a property and possessory interest in his home
at apartment No. 1122.................................................................196
2. The defendant had a possessory interest and continues to maintain a property
interest in the aircard.................................................................197
3. The defendant had a possessory interest and continues to maintain a property
interest in the host laptop computer used with the aircard...............198
4. The defendant had a property and possessory interest in his home electricity
purchased from Silicon Valley Power.............................................199
5. The defendant had a property and possessory interest in his Internet access
bandwidth purchased from Verizon Wireless....................................200
B. The defendant's liberty interest in using his aircard, host laptop computer, and
aircard service to access the Internet for the purpose of satisfying his own personal
and political interests, etc.................................................................201
C. The defendant's reasonable expectation of privacy in various places, objects,
records, resources, and combinations thereof.....................................202
1. The defendant had a reasonable expectation of privacy in his home residence,
i.e., apartment No. 1122.................................................................203
   a. The defendant's reasonable expectation of privacy in his home as a
      baseline matter........................................................................203
   b. The defendant's use of an alias does not act to destroy his reasonable
      expectation of privacy in his home...........................................205
c. The defendant's reasonable expectation of privacy in his home encompasses all effects contained therein and all geolocation records related to those effects.................................................................207

2. The defendant had a reasonable expectation of privacy in his aircard and host laptop computer..........................................................................................................................208
   a. The defendant's reasonable expectation of privacy in his aircard and host laptop computer as a baseline matter.................................................................208
   b. The defendant's use of aliases does not act to destroy his reasonable expectation of privacy in his aircard and host laptop computer........210

3. The defendant had a reasonable expectation of privacy in the aircard account..............................................................................................................................212

4. The defendant had a reasonable expectation of privacy in his historical cell site location information seized from Verizon Wireless.................................................215
   a. The defendant's reasonable expectation of privacy is grounded by the government's search by inference.................................................................215
   b. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in his historical cell site location information seized from Verizon Wireless.................................................................217
      i. The government's reliance on Miller fails because Verizon Wireless was not party to the defendant's communications and his cell site location information does not constitute routine business records.................................................................218
      ii. The government's reliance on Smith fails because the defendant did not knowingly or voluntarily convey his location information to Verizon Wireless.................................................................221
      iii. In any event, the Court should find an exception to the third-party disclosure rule considering Verizon Wireless is a service provider intermediary and location information is objectively recognized as highly private.................................................................222

5. The defendant had a reasonable expectation of privacy in his real-time cell site sector location information seized from Verizon Wireless.........................................224
   a. The defendant's reasonable expectation of privacy in his real-time cell site sector location information based on its necessary use in pinpointing the defendant within his home.................................................................224
   b. The defendant's reasonable expectation of privacy in his real-time cell site sector location information is supported by various statutes establishing his privacy interests.................................................................225
   c. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in his real-time cell site sector location sector location
information seized from Verizon Wireless.........................226

i. The government's reliance on Smith fails because the defendant correctly knew that Verizon Wireless did not have network infrastructure in place to obtain real-time cell site sector location information for aircard data connections.........................227

ii. The government's reliance on Smith fails because the FBI was pinging the aircard in order to force it to generate real-time cell site sector location information.........................228

6. The defendant had a reasonable expectation of privacy in his encrypted and encoded aircard signals sent over the air interface.........................................................230

a. The defendant's reasonable expectation of privacy in his “sealed” aircard signals is supported by an Ex Parte Jackson analogy..........................230

b. The defendant's reasonable expectation of privacy in his “sealed” aircard signals vis-a-vis signaling data showing the location of the aircard and the defendant within his home.........................................................230

c. The defendant's reasonable expectation of privacy in his “sealed” aircard signals is supported by FCC regulations banning the operation of cellular networks without an FCC license..........................231

d. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in his “sealed” aircard signals seized by the FBI.........................................................233

7. The defendant had a reasonable expectation of privacy in the data contained on the storage device within his aircard.........................................................234

a. The ESN data stored on a wireless device is considered to be highly private..........................235

b. The FBI obtaining the aircard's stored ESN using cell site emulators does not amount to using a pen register or trap and trace device..............236

c. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in the ESN stored on his aircard........238

8. The defendant had a reasonable expectation of privacy in his historical electronic gate location information seized from Quality Alarm Service......239

a. The defendant's reasonable expectation of privacy is grounded by the government's search by inference..........................239

b. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in his historical electronic gate location information seized from Quality Alarm Service..........................240

i. Miller does not apply because Quality Alarm Service was not party to the defendant's transactions and his electronic gate location

- viii -
information does not constitute routine business records............241

ii. Miller does not apply because the defendant did not knowingly or
voluntarily convey his location information to anyone............242

9. The defendant had a reasonable expectation of privacy in his aircard
destination IP addresses seized from Verizon Wireless...............243
   a. The 1.8 million destination IP addresses reveal communications content
      and other Fourth Amendment protected information............243
   b. The third-party disclosure rule does not vitiate the defendant's reasonable
      expectation of privacy in his 1.8 million destination IP addresses.......249

10. The defendant had/has a reasonable expectation of privacy in his data
    contained on his hard drives, encrypted virtual drives, and the forensic images
    created therefrom—as they are in the possession of the government.......250

D. Explanation of five different types of searches and/or seizures and why they are
    relevant to the defendant's arguments...........................................251
    1. Non-trespassory search that violates privacy resulting in the obtaining of
       information; [Katz reasonable-expectation-of-privacy analysis]..........252
    2. Trespassory search resulting in the obtaining of information; [Jones trespass-
       to-obtain-information analysis]......................................................253
    3. Search that violates privacy by way of seizure of records containing private
       information; [Katz reasonable-expectation-of-privacy analysis]..........256
    4. Seizure that interferes with property/possessory interest in an “effect”;[Jacobsen
       meaningful-interference-with-possessory-interest analysis].............256
    5. Seizure that interferes with an individual's liberty interest in a protected
       activity; [Soldal meaningful-interference-with-liberty-interest analysis].....257

E. Identification and classification of the government's Fourth Amendment searches
    and seizures.....................................................................................257
    1. The government's unauthorized and otherwise illegal Fourth Amendment
       searches and seizures relating to the aircard locating mission............257
       a. The government obtaining the defendant's 1.8 million destination IP
          addresses relating to his use of the aircard was a Fourth Amendment
          search and seizure.................................................................259
       b. The government obtaining the defendant's historical cell site location
          information relating to his use of the aircard was a Fourth Amendment
          search and seizure.................................................................260
       c. The FBI using triangulation and location signature techniques on the
          defendant's historical cell site location information was a Fourth
          Amendment search and seizure.............................................261
       d. Verizon Wireless writing data to the aircard via OTAPA was a Fourth
Amendment seizure……………………………………………………………...262
e. Verizon Wireless reprogramming the aircard via OTAPA, or flashing its firmware over-the-air, was a Fourth Amendment seizure………………263
f. The FBI using the SF-Martinez DCS-3000 Pen/Trap device to obtain the defendant's real-time cell site sector location information relating to his use of the aircard was a Fourth Amendment search and seizure…….264
g. The FBI forcing Verizon Wireless to obtain and provide real-time geolocation information relating to the location of the aircard was a Fourth Amendment search and seizure………………………………266
h. The FBI using surreptitious phone calls to deny the defendant access to the Internet for six hours (i.e., denial-of-service attack) was a Fourth Amendment seizure………………………………………………….269
i. The FBI forcing the aircard to handoff its 1xEV-DO Rel. 0 connection to the emulated cellular network broadcast by the StingRay and KingFish was a Fourth Amendment seizure………………………………270
j. The FBI repeatedly writing data to the aircard using the StingRay and KingFish was a Fourth Amendment seizure………………………………272
k. The FBI using the StingRay and KingFish to disable standard 1xEV-DO Rel. 0 air interface encryption for aircard signals was a Fourth Amendment seizure…………………………………………………..273
l. The FBI using the StingRay and KingFish to remotely access and download data from the aircard was a Fourth Amendment search and seizure………………………………………………………………………………….274
m. The FBI using the StingRay and KingFish to send location finding interrogation signals into the defendant's home and aircard was a Fourth Amendment search and seizure…………………………………………………..276
n. The FBI using the StingRay and KingFish to collect the aircard's signal transmissions sent in response to the location finding interrogation signals was a Fourth Amendment search and seizure…………………………………………………..277
o. The FBI using the StingRay and KingFish to conduct triangulation techniques on aircard signals transmitted in response to interrogation was a Fourth Amendment search and seizure…………………………………………………..279
p. The FBI using the StingRay and KingFish to deny the defendant access to the Internet for ten hours (i.e., denial-of-service attack) was a Fourth Amendment seizure…………………………………………………..280
q. The FBI using the defendant's electricity provided to his aircard and forcing the aircard to transmit at the highest possible power was a Fourth Amendment seizure…………………………………………………..282
r. The government obtaining the defendant's historical geolocation
information via his Domicilio electronic gate key access records was a Fourth Amendment search and seizure ........................................ 283
s. FBI Agent Nguyen using the defendant's key to verify that it unlocked apartment No. 1122 was a Fourth Amendment search and seizure...... 284

2. The government's unauthorized and otherwise illegal Fourth Amendment searches and seizures relating to the in-person search of apartment No. 1122........................................................................................................................................ 285
a. Various agents entering the defendant's home to seize his possessions was a Fourth Amendment search and seizure........................ 285
b. IRS-CI Agent Daun continuing to search the forensic images of the defendant's encrypted virtual drives was/is a Fourth Amendment search and seizure.................................................................................. 286

F. The searches and seizures identified in Section V(E), supra, were conducted in violation of the defendant's Fourth Amendment rights due to unreasonableness and lack of proper judicial authority........................................................................................................ 288
1. The N.D.Cal. 08-90330MISC-RS order did not render any of the applicable searches and seizures reasonable.................................................................................. 289
a. The FBI's searches and seizures conducted during execution of the N.D.Cal. 08-90330MISC-RS order exceeded the scope of the issued order........................................................................................................ 292
b. The N.D.Cal. 08-90330MISC-RS order does not authorize the installation, use, or monitoring of a "mobile tracking device"—whatever that device may be........................................................................................ 295
c. Even if a "mobile tracking device" was authorized by the N.D.Cal. 08-90330MISC-RS order, the aircard locating mission did not involve use of one........................................................................................................ 296
d. In any event, the "mobile tracking device" term contained in the N.D.Cal. 08-90330MISC-RS order fails for lack of particularity........ 297
e. Even if the N.D.Cal. 08-90330MISC-RS order authorized a place to be searched, the description of the place fails for lack of particularity...... 299
f. None of the actions authorized by the N.D.Cal. 08-90330MISC-RS order were supported by an applicable finding of probable cause............ 301
g. The "all data, information, facilities, and technical assistance" term contained in the N.D.Cal. 08-90330MISC-RS order fails for lack of particularity........................................................................................................ 302
h. The N.D.Cal. 08-90330MISC-RS order fails for facial unreasonableness.................................................................................. 304
i. The N.D.Cal. 08-90330MISC-RS order is facially unreasonable
because it is not a warrant

ii. The N.D.Cal. 08-90330MISC-RS order is facially unreasonable because it expressly omits compliance with Rule 41 inventory and return requirements.

iii. The N.D.Cal. 08-90330MISC-RS order is facially unreasonable because it expressly omits compliance with Rule 41 receipt and service requirements.

iv. The N.D.Cal. 08-90330MISC-RS order is facially unreasonable because it commanded destruction of evidence obtained via the order.

v. The N.D.Cal. 08-90330MISC-RS order is facially unreasonable because it authorized the government to serve redacted versions of the order.

i. Additional reasons as to why the N.D.Cal. 08-90330MISC-RS order was executed in an unreasonable manner.

i. The N.D.Cal. 08-90330MISC-RS order was unreasonably executed because agents violated the limitation to “monitoring.”

ii. The N.D.Cal. 08-90330MISC-RS order was unreasonably executed because agents failed to comply with receipt and service requirements.

iii. The N.D.Cal. 08-90330MISC-RS order was unreasonably executed because agents failed to comply with inventory and return requirements.

iv. The N.D.Cal. 08-90330MISC-RS order was unreasonably executed because agents destroyed all evidence seized during execution of the order.

j. Neither the N.D.Cal. 08-90330MISC-RS order application nor supporting affidavit act to cure defects in the issued order.

2. The N.D.Cal. 08-90331MISC-RS (Pen/Trap) order do not render any of the applicable searches and seizures reasonable.

a. The searches and seizures conducted during execution of the N.D.Cal. 08-90331MISC-RS order were not backed by anything resembling a probable cause warrant.

b. The FBI's searches and seizures conducted during execution of the N.D.Cal. 08-90331MISC-RS order exceeded the scope of the issued order.

c. Additional reasons as to why the N.D.Cal. 08-90331MISC-RS order was executed in an unreasonable manner.
i. The N.D.Cal. 08-90331MISC-RS order was unreasonably executed because agents violated the limitation to “recording.”

ii. The N.D.Cal. 08-90331MISC-RS order was unreasonably executed because agents violated the “after receipt and storage” provision of the order.

d. Neither the N.D.Cal. 08-90331MISC-RS order application nor supporting affidavit act to cure defects in the issued order.

3. The D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders do not render any of the applicable searches and seizures reasonable.

a. The searches and seizures conducted during execution of the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders were not backed by anything resembling a probable cause warrant.

b. The FBI's searches and seizures conducted during execution of the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders exceeded the scope of the issued orders.

4. The D.Ariz. 07-03-609 and 07-03-615 Grand Jury subpoenas and/or 08-3286MB-LOA order do not render any of the applicable searches and seizures reasonable.

a. The searches and seizures conducted during execution of the D.Ariz. 07-03-609 and 07-03-615 Grand Jury subpoenas and 08-3286MB-LOA order were not backed by anything resembling a probable cause warrant.

b. The description of “destination IP addresses” contained in the D.Ariz. 07-03-609 and 07-03-615 Grand Jury subpoenas and 08-3286MB-LOA order fails for lack of particularity.

5. The D.Ariz. 07-03-709 Grand Jury subpoena does not render any of the applicable searches and seizures reasonable.

a. The searches and seizures conducted during execution of the D.Ariz. 07-03-709 Grand Jury subpoena were not backed by anything resembling a probable cause warrant.

G. The good-faith exception to the exclusionary rule does not apply to the government's various illegal Fourth Amendment searches and seizures.

1. Consolidated “no good-faith” argument RE: lack of probable cause findings; [applicable to all orders and subpoenas]

2. Consolidated “no good-faith” argument RE: scope violations; [applicable to various orders]

3. Consolidated “no good-faith” argument RE: particularity violations; [applicable to various orders and subpoenas]
4. Consolidated “no good-faith” argument RE: violating terms and limitations contained in orders; [applicable to various orders].................................337

5. Consolidated “no good-faith” argument RE: Rule 41 violations; [applicable to all orders and subpoenas]......................................................................................338

6. Consolidated “no good-faith” argument RE: lack of candor in order applications; [applicable to various orders].................................................................340
   a. Lack of candor in the N.D.Cal. 08-90330MISC-RS order application relating to the government's true intentions..................................................341
   b. Lack of candor in the N.D.Cal. 08-90331MISC-RS order application relating to “general geographical location” claim......................................................341
   c. Lack of candor in the N.D.Cal. 08-90330MISC-RS and 08-90331MISC-RS order applications relating to failure to advise of prior orders seeking related information........................................................................342
   d. Lack of candor in the D.Ariz. 08-3286MB-LOA order application relating to failure to advise of extensive use of illegally obtained destination IP addresses........................................................................342

7. Consolidated “no good-faith” argument RE: mistaken understanding of the law; [applicable to all orders and subpoenas].................................................................343
   a. Mistaken understanding of the law relating to 18 U.S.C. § 2703 et seq. (i.e., the Stored Communications Act) as cited and/or relied upon by various orders and subpoenas.................................................................345
   b. Mistaken understanding of the law relating to the retroactive nature of the D.Ariz. 08-3286MB-LOA “retroactive order.”.........................................................346
   c. Mistaken understanding of the law relating to the hybrid use of the Pen/Trap statutes and the SCA in support of the N.D.Cal. 08-90331MISC-RS order.................................................................................................347

VI. [Conclusion:] Exclusion is an appropriate remedy for the various Fourth Amendment violations and all illegally obtained evidence and derivative evidence must be suppressed..............................................................................................................349
I. INTRODUCTION

As a result of a joint investigation by the Internal Revenue Service, Federal Bureau of Investigation, United States Postal Inspection Service, and the United States Attorneys Office into an alleged fraudulent IRS tax return bulk e-filing scheme, Daniel David Rigmaiden (hereafter “the defendant”) was charged with Conspiracy, 18 U.S.C. §§ 371 and 2 (Count 1), Wire Fraud, 18 U.S.C. §§ 1343 and 2 (Counts 2-36), Aggravated Identity Theft, 18 U.S.C. §§ 1028A(a)(1) and 2 (Counts 37-71), Unauthorized Access of a Computer With the Intent to Defraud, 18 U.S.C. §§ 1030(a)(4), 1030(c)(3)(A) and 2 (Count 72), and Mail Fraud, 18 U.S.C. §§ 1341 and 2 (Counts 73-74). See Superseding Indictment (Dkt. #200).[1]

The government charged the defendant in relation to the alleged scheme after the FBI used sophisticated geolocation techniques to locate the defendant within his private home residence: 431 El Camino Real, Apartment No. 1122, Santa Clara, CA 95050 (hereafter “apartment No. 1122”). The defendant was subsequently arrested and transferred to Arizona for prosecution. The defendant denies the government's allegations and maintains his innocence.

The defendant is filing the accompanying motion to raise various constitutional challenges pertaining to the FBI's efforts to locate his UTStarcom PC5740 mobile broadband access card (hereafter “aircard”) used with his home computer to access the Internet through the Verizon Wireless[2] 1xEV-DO Rel. 0 cellular data network. The government alleges that the defendant e-filed numerous fraudulent tax returns using his aircard by routing his Internet


connection through proxy computers in an attempt to hide his true IP addresses. Prior to identifying and indicting the defendant, the government claims to have analyzed a log of source IP addresses responsible for e-filing various fraudulent tax returns.\[3\] Through the analysis, the government claims it was able to identify a few of the aircard's true IP addresses assigned to it by Verizon Wireless. Suspecting that the aircard was the end-source node responsible for e-filing all of the tax returns, the government issued subpoenas to Verizon Wireless requesting two month's worth of the aircard's destination IP addresses and the billing/identity information for the aircard account. After Verizon Wireless fully complied, an analysis of the aircard's destination IP addresses indicated that the aircard was accessing the proxy IP addresses at the same approximate times the proxy computers were used to e-file the allegedly fraudulent tax returns. Based on the above, the government concluded that the aircard user was responsible for perpetuating the alleged scheme by routing the aircard connection through numerous proxy computers during the e-filing process. The government then attempted to identify and locate the owner of the aircard through aircard account billing records but failed because the defendant used an alias and a PO Box to sign up for his aircard account.

In order to identify and indict the aircard user, the government began a locating mission aimed at pinpointing the exact location of the aircard and its owner. The government's “aircard locating mission” began on July 10, 2008 and ended July 17, 2008 with the FBI locating the aircard within the defendant's private home residence, i.e., apartment No. 1122. Before the start of the aircard locating mission, the government had no information on the location of the aircard and the government had no information on who the defendant was or where he was located. During the aircard locating mission, the government used a barrage of high-tech investigative techniques to locate the defendant within his home including: (1) obtaining destination IP addresses and web communications content for the aircard, (2) obtaining historical cell site location information for the aircard, (3) obtaining

---

3. The log of proxy IP addresses was created from records provided by the authorized IRS e-file providers responsible for operating websites used by individuals and businesses to e-file their tax returns.
real-time cell site sector location information for the aircard, (4) using portable/transportable wireless device locators (i.e., the Harris StingRay, KingFish, and related equipment) to pinpoint the exact location of the aircard, and (5) obtaining the defendant's electronic gate key access records for apartment No. 1122. All of the Fourth Amendment searches and seizures related to the government's investigative techniques were conducted in violation of the defendant's Fourth Amendment rights. The government infringed upon the defendant's Fourth Amendment protected interests through a combination of the following: (1) violating the defendant's reasonable expectation of privacy, (2) meaningfully interfering with the defendant's property and/or possessory interests, (3) meaningfully interfering with the defendant's liberty interests, and (4) trespassing upon the defendant's property and chattel for the purpose of obtaining information.

Instead of obtaining a proper probable cause warrant in compliance with Rule 41, the government violated the defendant's constitutional rights by using a hobo stew of inapplicable authorities, vague and convoluted court orders, unreasonable subpoenas, and an unheard of authority to destroy evidence. While locating the aircard, the government relied upon four statutes cited across five court orders spanning three magistrate judges over two federal districts. The government also avoided judicial oversight by using Grand Jury subpoenas to obtain the defendant's electronic gate key geolocation records for his home and web communications content for his aircard Internet connection. There were no probable cause findings that applied to any of the government's actions and most actions were based on mere findings of “specific and articulable facts” while others were entirely unauthorized or specifically forbidden by court order. As icing on the cake, the FBI (1) failed to provide the defense notice on any order until nine months after the aircard had been located, (2) failed to file any type of return, and (3) destroyed evidence in an attempt to circumvent Brady and its progeny.

In the Argument section of this memorandum (Section V, infra), the defendant shows how the government's efforts to locate the aircard and the defendant within his private home residence are plagued with constitutional violations. Beginning with intrusive long term
surveillance via historical cell site location information and ending with the pinpoint accuracy of the FBI's cell site emulators, the defendant shows how each of the government's warrantless investigative techniques violated his constitutional rights. At the conclusion of the Argument section, the defendant explains why suppression of destination IP addresses, geolocation data, and all derivative evidence is an adequate remedy and why the good faith exception to the exclusionary rule does not apply. Prior to arguing for suppression, the defendant outlines various facts through separate factual sections labeled (1) Technical Explanations (Section II, infra), (2) Procedural History (Section III, infra), and (3) General Facts (Section IV, infra). The three factual sections provide necessary background information in support of the defendant's arguments challenging the government's illegal searches and seizures.

II. Technical Explanations

Prior to reading the Procedural History (Section III, infra) and the General Facts (Section IV, infra), obtaining a full technical understanding of how the government locates 1xEV-DO Rel. 0 wireless devices is beneficial. The proceeding subsections provide detailed technical information on communications protocols, geolocation techniques, surveillance equipment, surveillance programs, and investigative methods used by the government to locate wireless devices. All technical explanations are backed by citations to credible public sources of information, case discovery provided by the government, and admissions made by the prosecution. The purpose of providing technical explanations is to support various technical claims made in the General Facts section of this memorandum. For example, the proceeding subsections support Section IV(B)(9), infra, explaining the

4. The facts contained in this section are meant to reflect a “snapshot” of how the technology existed at the time the aircard was located (July of 2008)—even while some newer technical sources are cited.

5. The Argument section of this memorandum is primarily founded by claims made in the General Facts which are in turn supported by the Technical Explanations section. However, some technical explanations have a very precise purpose and are only referenced directly in the Argument section.

6. The noted General Facts subsection is labeled, “The FBI technical agents used the Harris StingRay, KingFish, and related equipment to locate the aircard precisely inside apartment No. 1122.”
activities of the FBI technical agents while they operated their surveillance equipment to pinpoint the exact location of the aircard. In the *General Facts*, all claims are presented as numbered paragraphs and may cite back to the detailed technical explanations outlined in this section. If the reader questions the legitimacy or accuracy of any technical claim made in the *General Facts*, the subsections immediately below should be referenced and studied until sufficient knowledge is obtained allowing for corroboration.

A. **Electromagnetic radiation in the radio frequency band.**

Radio waves are one type of electromagnetic radiation within the electromagnetic spectrum. “The electromagnetic spectrum contains radio waves, microwaves, light, x-rays, and gamma rays.”[7] “Every wave has three different properties: (1) wavelength (a spatial measurement), (2) frequency (a temporal measurement), and (3) energy (or equivalently mass).”[8] “We can always find the frequency of a wave if we know its wavelength. Or, if we know the frequency, we can find its wavelength. The reason is that the frequency multiplied by the wavelength of a wave must always give a product equal to the velocity of light. This is true of all electromagnetic waves.”[9] In radio communications, electromagnetic waves are classified in terms of frequency.[10] For example, the specific radio frequencies licensed to Verizon Wireless for its cdma2000 based cellular network (e.g., 1xRTT, 1xEV-DO, etc.) in the San Jose, CA market area are (1) 835 - 845 MHz paired with 880 - 890 MHz and 846.5 - 849 MHz paired with 891.5 - 894 MHz;[11] and (2) 1850 - 1865 MHz.


10. For a “spectrum activity” chart showing some electromagnetic frequencies used by modern day radio communication systems, see Thales [PDF presentation], “New solutions for massive monitoring”, *ISS World Europe*, p. 4 (Oct. 3, 2008), available at http://wikileaks.org/spyfiles/files/0/40_200810-ISS-PRG-THALES.pdf (last accessed: Apr. 10, 2012); see also EXHIBIT 058 of 2nd Consolidated Exhibits (Dkt. #821-3) (“spectrum activity” chart attached).

11. See FCC [website], *ULS License - Cellular License - KNKA211 - GTE MOBILNET OF CALIFORNIA LIMITED PARTNERSHIP*,
Radio waves, as well as all other electromagnetic radiation, “propagate at the speed of light: 186,282 miles per second.” Radio wave propagation can be in the form of either omnidirectional radio waves or directional radio waves. “Omnidirectional ('all directions') radio-frequency propagation can be compared to the waves created by throwing a pebble into a pond. The waves made by the pebble emanate in all directions equally.” Directional radio frequency propagation by contrast have more gain (i.e., signal coverage area) in certain directions and less in others. Directional radio frequency propagation can therefore be thought of as a “ray” or “beam” of radio waves directed at a certain area.


13. Although Verizon Wireless' license data indicates a small number of listed cell site locations, “[a] licensee may operate additional transmitters at additional locations on the same channel or channel block as its existing system without obtaining prior Commission approval provided: [] (1) The interfering contours of the additional transmitter(s) must be totally encompassed by the composite interfering contour of the existing station (or stations under common control of the applicant) on the same channel...” 47 CFR § 22.165 et seq.

14. Although Verizon Wireless' cdma2000 based mobile network operates on both the “Cellular” spectrum (KNKA211) and “PCS” spectrum (WQIQ264), the network itself remains constant with the only difference being the range of frequencies used over the air interface. For simplicity purposes, Verizon Wireless' cdma2000 based mobile network will be referred to as a cellular network regardless of any possible spectrum in use.


16. See Bedell, Cellular/PCS Management: A Real World Perspective, p. 38.

17. See United States Army, Communications-Electronics Fundamentals: Wave Propagation, Transmission Lines, and Antennas, Training Circular 9-64 (Washington, DC: July 2004), available at http://www.cbtricks.com/miscellaneous/tech_publications/neets/tc9_64.pdf (last accessed: April 10, 2012), p. 4.11 (PDF, p. 177) (“Some antennas are highly directional; that is, more energy is propagated in certain directions compared to the energy that would be propagated if the antenna were not directional is known as its gain. When a transmitting antenna with a certain gain is used as a receiving antenna, it will also have the same gain for receiving.”).
In addition to wave like properties, radio waves also have particle like properties.\(^{[18]}\)

“Light rays, heat radiation, radio waves, X rays, cosmic rays, and gamma rays produced by splitting atoms are all streams of photons.”\(^{[19]}\) Electromagnetic radiation can therefore be visualized as a stream of photons\(^{[20]}\) traveling at the speed of light. A photon is an atomic particle\(^{[21]}\) produced when an electron changes from a high energy level to a low energy level.\(^{[22]}\) Although a photon cannot be weighed, streams of photons still exhibit an observable mass. “For one thing, light produces a definite pressure when it falls on an object. As a comet moves around the sun, its great gaseous tail is always streaming out away from the sun. This can be satisfactorily explained only by assuming that the light from the sun pushes the tail away.”\(^{[23]}\) Photons also carry energy which is directly proportional to frequency.\(^{[24]}\) This photon energy can be converted into electricity for practical applications. For example, when transmitted radio waves reach a receive antenna,\(^{[25]}\) the photon energy...
induces a voltage in the antenna producing a current of electricity which transfers the radio
signals from the antenna to the receiver.\[26\] The photon energy produced by radio waves is
small when compared to other electromagnetic radiation but it is still strong enough to
power, for example, an AM radio receiver and speaker—without a separate power source—if
close enough to an AM transmitter.\[27\]

B. The 1xEV-DO cellular communications system deployed by Verizon Wireless.

1. Origins of the 1xEV-DO cellular communications system.

The 1xEV-DO cellular communications system is defined within the cdma2000
family of standards developed by the 3rd Generation Partnership Project II (3GPP2).\[28\]
These standards define a set of specifications that cellular device manufacturers and cellular
service providers must follow to ensure compatibility across hardware and networks.\[29\] The
cdma2000 family of standards, including 1xEV-DO, is based on a communications
protocol\[30\] called code division multiple access (CDMA) originally designed for military

\[26\] "The RF energy is transmitted into space in the form of an electromagnetic field. As
the traveling electromagnetic field arrives at the receiving antenna, a voltage is induced into
the antenna (a conductor). The RF voltages induced into the receiving antenna are then
passed into the receiver and converted back into the transmitted RF information." Id., p. 4.4
(PDF, p. 170).

(Chicago, IL: Field Enterprises Educational Corporation, 1962), p. 88, Diagram labeled “A
Simple Radio Set” (“A Crystal Set is a simple radio that does not use electricity.”); Tymony,
Cy, Sneaky Uses for Everyday Things (Kansas City, MO: Andrews McMeel Publishing,
2003), p. 60 (“Even now, many parents show their kids how to make a radio at home that
doesn't require AC power or batteries.”).

\[28\] See Etemad, Kamran, cdma2000 Evolution: System Concepts and Design Principles
(Hoboken, NJ: John Wiley & Sons, Inc., 2004), p. xiii, 4 and 9. See also
http://www.3gpp2.org.

\[29\] See Telecommunications Industry Association, TIA-2000.1-E, Introduction to

\[30\] “Protocol: A standard set of definitions governing how communications are formatted
in order to permit their transmission across networks and between devices.” CTIA [website],
Wireless Glossary of Terms N-P,
http://www.ctia.org/media/industry_info/index.cfm/AID/10407 (last accessed: Aug., 30,
use due to it being nearly impossible to intercept a CDMA signal. In the United States, there are various CDMA cellular service providers including “Alaska Communications System, Carolina West, CellCom/nSight, Bluegrass Cellular, Leap Wireless, Sprint, U.S. Cellular, and Verizon Wireless.”

“CDMA employs what is known as wideband spread spectrum technology to carry digitized voice and data transmissions.” Spread spectrum technology spreads “the radio signal over a wide frequency range by modulating it with a code word unique to the radio.” The receiver “distinguishes [the] sender's signal from other signals by examining the wide spectrum band with a time synchronized duplicate of the spreading code word.” In simple terms, CDMA in cellular telephony is “[a] technology used to transmit wireless calls by assigning them codes[]” allowing for each CDMA transmitter to transmit calls.


32. See Bedell, Cellular/PCS Management: A Real World Perspective, p. 225 (“CDMA was originally deployed as a battlefield communications system because it is very hard if not completely impossible to intercept CDMA transmissions.”).


35. Issued in 1942, “[t]he U.S. patent for spread-spectrum technology was held jointly by actress Hedy Lamarr and music composer George Antheil.” Muller, Nathan J., Bluetooth Demystified (New York, NY: McGraw-Hill, Sept. 8, 2000), p. 61 (figure note omitted). “Spread spectrum has two modes of operation: frequency hoping and direct sequencing. Frequency hoping spreads its signals by ‘hoping’ the narrowband signal over the entire radio band as a function of time. Direct sequencing spreads its signal by expanding the signal all at once over the entire radio band.” Id., p. 63. CDMA uses direct sequencing.

36. Katz, Randy H., Professor at U.C. Berkeley, CS 294-7: Media Access—TDMA and CDMA, p. 13 (1996), available at http://www.sss-mag.com/pdf/1tdmacdma.pdf (last accessed: Aug. 31, 2010); see also Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 11 (“The basic idea of spread spectrum communications is based on transmitting information over channels much wider than required by the original signal bandwidth. The spread spectrum term is used to reflect the fact that the system spreads the energy of the information signal over a much wider band channel, allowing signal transmission at very low power spectral densities.”).

37. Id.

38. CTIA [website], Glossary of Terms C-D,
simultaneously to a single cell site without having the signals conflict with each other.\[39\] On the reverse link, “[t]his process is analogous to each mobile speaking a different language and the base station interpreting each of the languages it receives.”\[40\] In all CDMA based cellular systems, the term “reverse link” refers to the signal path leading from the wireless device to the cell site and the term “forward link” refers to the signal path leading from the cell site to the wireless device.\[41\]

CDMA was first introduced in cellular systems in the early 1990s with the cdmaONE family of standards.\[42\] Cellular communications systems based on cdmaONE began with “voice only” services (see IS-95A) with limited data services added later (see IS-95B).\[43\] After commercial use of cdmaONE throughout the 1990s, the cellular communications industry developed cdma2000 beginning with the IS-2000 Release 0 technical standard, which is also referred to as 1xRTT.\[44\] 1xRTT, first commercially deployed in the year 2000, provides both voice and data services\[46\] with performance increases over cdmaONE technology. Later that year, 3GPP2 set out to improve upon 1xRTT by drafting and publishing the cdma2000 High-Rate Packet Data (HRPD) standard referred to as IS-856 or 1xEV-DO (an acronym for EVolution Data-Optimized).\[47\]\[48\] The original release of 1xEV-DO provided both voice and data services with performance increases over cdmaONE technology. Later that year, 3GPP2 set out to improve upon 1xRTT by drafting and publishing the cdma2000 High-Rate Packet Data (HRPD) standard referred to as IS-856 or 1xEV-DO (an acronym for EVolution Data-Optimized).\[47\]\[48\] The original release of 1xEV-DO provided both voice and data services with performance increases over cdmaONE technology. Later that year, 3GPP2 set out to improve upon 1xRTT by drafting and publishing the cdma2000 High-Rate Packet Data (HRPD) standard referred to as IS-856 or 1xEV-DO (an acronym for EVolution Data-Optimized).\[47\]\[48\] The original release of 1xEV-DO provided both voice and data services with performance increases over cdmaONE technology. Later that year, 3GPP2 set out to improve upon 1xRTT by drafting and publishing the cdma2000 High-Rate Packet Data (HRPD) standard referred to as IS-856 or 1xEV-DO (an acronym for EVolution Data-Optimized).\[47\]\[48\] The original release of 1xEV-
DO, first commercially deployed in the year 2002,[^49] is referred to as “Release 0” (or “Rel. 0”) and subsequent releases are referred to as “Revision A,” “Revision B,” and “Revision C” with each revision adding features and increasing data rates[^50] All versions of 1xEV-DO use cellular networks to provide broadband Internet access to Access Terminals such as aircards. Unlike 1xRTT, 1xEV-DO does not allow for placing voice calls and is strictly limited to data services.[^51]

The remainder of the technical explanations contained in this section are presented in the context of 1xEV-DO Rel. 0—the version of 1xEV-DO used by the defendant's aircard. All cell sites, including FBI cell site emulators, that wish to send or receive radio signals to/from a 1xEV-DO Rel. 0 based Access Terminal must follow the detailed instructions outlined in the cdma2000 technical standards applicable to 1xEV-DO Rel. 0. “The technical requirements contained in cdma2000 form a compatibility standard for CDMA systems. They ensure that a mobile station can obtain service in a system manufactured in accordance with the cdma2000 standards.”[^52] The primary technical standards relevant to 1xEV-DO Rel. 0 are listed below:

1. Telecommunications Industry Association, TIA/EIA/IS-856-1 (Addendum No. 1 to TIA/EIA/IS-856), cdma2000 High Rate Packet Data Air Interface Specification (Arlington, VA: Jan. 2002); **Note:** IS-856-1 sets forth standards dictating the technical requirements for HRPD “Release 0” (i.e., 1xEV-DO Rel. 0) systems and is primarily oriented toward requirements necessary for the design and implementation of Access Terminals. The original cdma2000 HRPD technical standard is IS-856, released by 3GPP2 in November of 2000.

[^49]: See id.

[^50]: See eogogicsinc (website), cdma2000 Technologies: 1xRTT, EVDO, UMB, and EVDV.

[^51]: See Chuah, Mook Choo and Zhang, Qingqing, Design And Performance Of 3G Wireless Networks And Wireless LANs (New York, NY: Springer Science+Business Media, Inc., 2006), p. 66 (“The network architecture of 1xEV-DO is very similar to the 3G1x network architecture except that the components associated with voice traffic are absent.”).

2000. However, in January of 2002, 3GPP2 released IS-856-1[54] and in March of 2004, IS-856-2[E][55]—all of which expanded upon the original IS-856 specification as applicable to 1xEV-DO Rel. 0.[56] For the technical explanations outlined in this section, the defendant references IS-856-1.


Note: IS-878-2 sets forth standards dictating Access Terminal authentication, handoffs, Hybrid Access Terminal (HAT) operations, etc. in an HRPD system. The original cdma2000 HRPD Interoperability standard is IS-878, released by 3GPP2 in December of 2001.[57] However, in May of 2003, 3GPP2 released IS-878-1[58] and IS-1878,[59] and in May of 2008, IS-878-2[60] and IS-1878-1[61]—all of which expanded upon the original IS-878
specification as applicable to 1xEV-DO.[62] For the technical explanations outlined in this section, the defendant references IS-878-2.

3. Telecommunications Industry Association, TIA-683-D (Revision to TIA-683-C), Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, (Arlington, VA: May 2006); Note: IS-683-D sets forth standards dictating the Over-the-Air Service Provisioning (OTASP) of Mobile Station and HRPD (i.e., 1xEV-DO) Access Terminal operational parameters. The original Over-the-Air Service Provisioning standard is IS-683, which was subsequently updated by 3GPP2 via IS-683-A in June of 1998.[63] However, in December of 2001, 3GPP2 released IS-683-B,[64] in March of 2003, IS-683-C,[65] and in May of 2006, IS-683-D.[66] For the technical explanations outlined in this section, the defendant references IS-683-D.

The remainder of this section will cite to the above 3GPP2 technical standards and to other relevant technical references. Some technical references will be specific to older cellular technology (e.g., 1xRTT or IS-95A/B) but are only cited to the effect they provide information that remains constant through later CDMA technology, i.e., 1xEV-DO Rel. 0.[67]

[68] In those cases, the term “Mobile Station” should be read as “Access Terminal,” and the

62. Considering the differences between these standards are negligible in the context of the defendant's arguments, IS-878-2 (May 2008) will be used as the primary technical reference in this section.


67. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, Forward, p. xlix (“This standard is evolved from and is a companion to the cdma2000 standards.”); Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 264 (“The network architecture in HRPD is similar to the IS2000 system with some variations in network elements, functionalities, and interface protocols.”).

68. Proceed with caution if references addressing older CDMA technology are pulled and
term “Base Station” should be read as “Access Network.”

2. Basic hardware elements of a 1xEV-DO Rel. 0 compatible cellular data network.

   a. The Access Terminal (AT).

   The basic hardware elements of a 1xEV-DO Rel. 0 cellular data network have both similarities and differences when compared to a 1xRTT cellular voice network. A 1xEV-DO Rel. 0 data network begins with the Access Terminal (AT), which consists of a radio transmitter/receiver (transceiver), antenna, and other hardware used for communicating with Access Networks. [69] The Access Terminal is the equivalent of a Mobile Station (MS) (i.e., cellular telephone) in 1xRTT. [70] The Access Terminal “may be a self-contained data device such as a personal digital assistant (PDA) or a detachable module that is connected to a computing device such as a laptop personal computer.” [71] From a legal perspective, the difference between an Access Terminal and a Mobile Station is that the former facilitates the sending/receiving of electronic communications [72] while the later facilitates the sending/receiving of wire communications. [73] However, most 1xEV-DO Rel. 0 based

   studied for further information. 1xEV-DO, being a pure data network, does not adopt the majority of the subject matter specific to IS-95A/B, 1xRTT, etc.

69. See EXHIBIT 11 of 1st Consolidated Exhibits (Dkt. #587-1) (example of an Access Terminal).

70. See id., p. 264.

71. Id.

72. See 18 U.S.C. § 2510(12) (“‘electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce, but does not include—(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title [18 USCS § 3117]); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;”).

73. See 18 U.S.C. § 2510(1) (“‘wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.;”).
wireless devices are “Hybrid mobile stations / Access Terminals (HATs),”[74] i.e., they support both 1xRTT wire communications and 1xEV-DO Rel. 0 electronic communications. [75] “Hybrid mode device[s]... support cdma20001x and HRPD by periodic[ly] monitoring the paging channel of cdma20001x[] [(i.e., 1xRTT)][][76] but cannot maintain 1xEV-DO and 1xRTT traffic channels simultaneously. If a Hybrid Access Terminal lacks the hardware required to place voice calls,[77] such as a PCMCIA broadband Internet access card (i.e., aircard), the 1xRTT service only facilitates SMS text messages[78] and a low rate data service as a backup to the 1xEV-DO Rel. 0 data service.

Each 1xEV-DO Rel. 0 Access Terminal has either an Electronic Serial Number (ESN) or Mobile Station Equipment Identifier (MEID) that uniquely identifies it among other

---


76. Id., § 1.2, p. 1.1.


Access Terminals and Mobile Stations. The ESN consists of a unique 32-bit number assigned to the wireless device by the manufacturer. The ESN is stored on the Access Terminal's internal storage as a Permanent Access Terminal Indicator and cannot be changed absent physical access to internal hardware. Each Access Terminal has one or more internal electronic storage devices in the form of either an integrated memory chip or Removable User Identity Module (R-UIM). A section of the Access Terminal's internal storage is called the Number Assignment Module (NAM) used to store a copy of the ESN.

---

79. See Telecommunications Industry Association, TIA-2000.5-D (Revision to TIA/IS-2000.5-C), Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems (Arlington, VA: Mar. 2004), § 2.3.2, p. 2.6 (“The ESN or MEID is used to uniquely identify a mobile station in a wireless system.”).


82. See id., p. 12 (“The ESN shall be factory set...”).


84. See TIA, Electronic Serial Number Manufacturer's Code Assignment Guidelines And Procedures, Ver. 2.0, p. 7 (“The manufacturer will exercise due diligence in the design and manufacture of the MS to ensure that alteration of the factory set ESN is not possible outside of an authorized service center.”); TIA-683-D, Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, Notes, p. xviii (“Each mobile station is assigned either a single unique 32-bit binary serial number (ESN) or a single unique 56-bit binary serial number (MEID) that cannot be changed by the subscriber without rendering the mobile station inoperative.”).


and the Mobile Identification Number (MIN).\(^{[87]}\) In addition to storing the ESN and MIN, the NAM also stores other numeric indicators and parameters used for Access Terminal operation.\(^{[88]}\) For example, among other categories of data, each Access Terminal NAM also stores: (1) the Preferred Roaming List,\(^{[89]}\) (2) the Extended Preferred Roaming List,\(^{[90]}\) (3) Shared Secret Data (SSD),\(^{[91],[92]}\) and (4) manufacturer-specific NAM parameters.\(^{[93]}\) The numeric indicators and parameters stored on the NAM can be updated by the wireless carrier by writing and/or deleting data on the NAM via Over-the-Air Parameter Administration (OTAPA) or other similar methods.\(^{[94]}\) See Technical Explanations, Section II(B)(3)(a), \textit{infra}, for a full explanation of OTAPA. The four categories of NAM data listed above are further explained in proceeding subsections.

\textbf{b. The Access Network (AN).}

In order to provide data services to Access Terminals, a 1xEV-DO Rel. 0 cellular data

---

87. See TIA-683-D, \textit{Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems}, § 1.2.1, p. 1.3 (“Mobile Identification Number (MIN). The 34-bit number that is a digital representation of the 10-digit number assigned to a mobile station.”); compare also id. (“Mobile Directory Number. A dialable directory number which is not necessarily the same as the mobile station’s air interface identification, \textit{i.e.}, MIN, IMSI\_M or IMSI\_T.”).

88. See \textit{id.}, § 3.1, p. 3.1 (“The NAM indicators are parameters that can be assigned values using Over-the-Air Service Provisioning are specified in 4.5.2, 4.5.3, 4.5.4 and 4.5.6.”).

89. See \textit{id.}, § 4.5.3, p. 4.38 \textit{et seq.} (explaining the NAM Preferred Roaming List and Extended Preferred Roaming List parameter blocks); \textit{id.}, § 3.5.5, p. 3.93 (Explaining the Preferred Roaming List and Extended Preferred Roaming List stored on the NAM).

90. See fn. No. 89, \textit{supra}.

91. See \textit{id.}, § 3.1, p. 3.1 (“The standard NAM indicators, stored in the mobile station’s permanent and semi-permanent memory, are defined in F.3 of [1, 7].” (referring to TIA-2000.5-D)); See TIA-2000.5-D, \textit{Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems}, Annex F, § F.3, p. F.4 (Listing A-Key, Shared Secret Data A, and Shared Secret Data B as NAM indicators.).


93. See \textit{id.}, § 3.1, p. 3.1 (“Manufacturer-specific NAM parameters may be defined within a Parameter Block Type reserved for manufacturer-specific parameter definitions.” (internal table references omitted)).

94. See \textit{id.}, § 1.2.1, p. 1.4 (“Over-the-Air Parameter Administration (OTAPA). Network initiated OTASP process of provisioning mobile station operational parameters over the air interface.”).
network uses a set of hardware and software called the Access Network (AN). The Access Network is responsible for providing “data connectivity between the packet-switched data network (typically the PDSN and Internet) and the ATs.”[95] The Access Network is the equivalent of a Base Station (BS) in a 1xRTT network.[96] Both Access Networks and Base Stations are more commonly known as cell sites.[97][98] The Access Networks belonging to a 1xEV-DO Rel. 0 data network communicate with Access Terminals via radio waves transmitted through the air, i.e., over the air interface. The radio waves sent between Access Terminals and Access Networks consist of signals that communicate data to/from the Access Terminal users and the Internet. A 1xEV-DO Rel. 0 Access Network consists of two main hardware/software elements: (1) the Base Transceiver Station (BTS),[99] and (2) the Base Station Controller (BSC) which is sometimes “referred to as the radio network controller, or RNC.”[100] “The BTS is an entity, composed of radio devices, antenna, and equipment, that provides transmission capabilities across the air interface (Um).”[101] In a 1xRTT network, “[t]he BSC is an entity that provides control and management for one or more BTSs and exchanges messages with its connected BTSs and the MSC [(i.e., Mobile Switching Center)].”[102] In a 1xEV-DO network, the Base Station Controller (i.e., the

96. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 1.11, p. 1.12 (“An access network is equivalent to a base station...”).
97. In basic terms, a cell site is defined as “[t]he location where a wireless antenna and network communications equipment is placed in order to provide wireless service in a geographic area.” CTIA [website], Glossary of Terms C-D, http://www.ctia.org/media/industry_info/index.cfm/AID/10321.
98. The remainder of the technical explanations contained in this section will refer to 1xEV-DO Rel. 0 cell sites as Access Networks when used in the context of 1xEV-DO Rel. 0 cellular data networks.
99. See Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 264, Fig. 10.23, “Basic network structure for 1X-EV DO.”
100 See id.
101. Id., p. 265.
103. Id. (“The MSC switches circuit-mode MS-originated or MS-terminated traffic and provides processing and control for calls and services.”).
Radio Network Controller) performs the same function but instead of exchanging messages with a Mobile Switching Center, which is absent in a 1xEV-DO data network,[104] the BSC/RNC exchanges messages with (1) the “Access Network-Authentication, Authorization, and Accounting” (AN-AAA) server, and (2) the Packet Data Serving Node (PDSN).[105]

The first primary function performed by the BSC/RNC, exchanging messages with the AN-AAA server, is done to authenticate the Access Terminal to the Access Network and to collect data used for billing the wireless customer.[106] The AN-AAA authentication process, further explained in Section II(B)(3)(c)(vi), infra, prevents unauthorized wireless devices (e.g., cloned wireless devices) from accessing data service through Access Networks while service is not authorized. Once the authentication process is complete, the BSC/RNC performs its second primary function, i.e., exchanging data between the Access Network and the Packet Control Function (PCF),[107] which in turn relays the data to/from the Packet Data Serving Node[108] providing connectivity to the Internet.[109]

c. Access Networks (a.k.a. cell sites) in the geolocation context.

From a geolocation perspective, a 1xEV-DO Rel. 0 cellular data network provides service through a series of “cells” with each designating a geographical area located within the network coverage area.[110] Each cell, which is served by multiple cell sites (i.e., Access

---

104. See Mishra, Ajay R., *Cellular Technologies for Emerging Markets: 2G, 3G and Beyond* (West Sussex, England: John Wiley & Sons, 2010), p. 113 (“...EV-DO uses an IP network and does not require a SS7 network and complex network switches such as a mobile switching center (MSC).”).

105. See Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 266, Fig. 10.24, “Radio and core network interfaces protocols in 1X-EV DO.”

106. See id., p. 205 (“This function of AAA involves collecting and storing the billing-related data concerning the offered services...”).

107. See id., p. 204 (“The PCF is an entity... that manages the buffering and relay of packets between the BS and the PDSN.... The PCF also collects radio link (air interface)-related accounting information to be used by the AAA.”).

108. See id., p. 264, Fig. 10.23, “Basic network structure for 1X-EV DO.”

109. See id., p. 265 (The PDSN is “the network equipment providing data connectivity between the radio access network and a packet-switched data network. The PDSN provides connectivity to the Internet independent of the type of radio access network.”)

110. See Chuah et al., *Design And Performance Of 3G Wireless Networks And Wireless LANs*, p. 1 (“Today, the cellular systems consist of a cluster of base stations with low-power radio transmitters. Each base station serves a small cell within a large geographic area.”).
pointing inward from the cell's borders, “is usually depicted as a hexagon, but in reality the actual shape varies according to the geographic environment and radio propagation."[111] A cell site in 1xEV-DO typically consists of three sets of multiple antennas, referred to as sectors, positioned atop an antenna tower, rooftop, or other structure allowing the antennas to operate across the earth's surface.[112][113] Cell site sectors “are created by installing multiple antenna sets at the base location, each with shielding on the 'back.' Each set of antennas is directional rather than omnidirectional.”[114] The geographical signal coverage area of each sector depends on various factors such as power output of antenna amplifiers, antenna design,[115] and physical obstructions within the signal path area.[116] Sectors belonging to the most common type of cell site are positioned in a

111. Id., p. 2.

112. Although these “typical” cell sites are designed to cover relatively large sections of populated areas, other types of cell sites are becoming more common—even ones “designed to serve very small areas, such as particular floors of buildings or even individual homes and offices.” Hearing Before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the Committee On The Judiciary, House Of Representatives: ECPA Reform and the Revolution in Location Based Technologies and Services, 111th Cong. 2nd sess. (Jun. 24, 2010) (Prepared Statement of Matt Blaze, Associate Professor, University of Pennsylvania), p. 25, available at http://judiciary.house.gov/hearings/printers/111th/111-109_57082.PDF (last visited: Jan. 5, 2012 ), p. 29.

113. The Verizon Wireless cell sites that were being accessed by the defendant's aircard while inside apartment No. 1122 were the typical tri-sectored type. See EXHIBIT 22 of 1st Consolidated Exhibits (Dkt. #587-2) (cell tower range chart/map of cell sites accessed by the aircard). Therefore, the remainder of this subsection will focus on the antenna design applicable to the actual Verizon Wireless cell sites accessed by the aircard.

114. Levine, Digital Switching: Cellular & PCS Lectures April 17 & 24, 2001, p. 11 ("Sected cells have two advantages over omnidirectional cells. First, by limiting the radio reception/transmission to the 'front' of the angular sector and not transmitting or receiving a signal from the 'back' they reduce the level of interference by a ratio of 3/1 or 6/1 for 3 and 6 sectors, respectively. This improves the signal quality, which is manifested as a lower BER in a digital system.").

115. See Bedell, Cellular/PCS Management: A Real World Perspective, p. 38 (“Actual RF coverage is mainly determined by three key factors: the height of the cellular antenna (tower) at the base station, the type of antenna used at the cell base station, and the RF power level emitted.").

116. See, e.g., CTIA [website], How Wireless Works Pg 2, http://www.ctia.org/consumer_info/index.cfm/AID/10539 (last accessed: Dec. 13, 2011) ("Since the shape and size of cells vary, there might also be empty spaces between the coverage areas of two or more cells. These gaps or dead spots can also be caused by trees, tall buildings or other obstructions that block your wireless signal from reaching a nearby antenna.").
360° circular formations with each sector covering an approximate 120° signal path area across the earth's surface.\textsuperscript{117} The horizontal antenna angles designate the direction of each sector's 120° signal path area. In addition to having a physical location address (street address plus latitude and longitude), each cell site sector also has its own identification number. “This arrangement essentially divides the carrier's coverage area into a mosaic of local 'sectors', each served by an antenna at the nearest base station [(\textit{i.e.,} cell site serving a cell)].”\textsuperscript{118}

3. \textbf{How relevant 3GPP2 technical standards dictate communications between a 1xEV-DO Rel. 0 Access Terminal and a 1xEV-DO Rel. 0 Access Network.}

\textbf{a. Over-the-Air Service Provisioning (OTASP) and Over-the-Air Parameter Administration (OTAPA).}

As explained in Section II(B)(2)(a), \textit{supra}, each Access Terminal NAM stores various data parameters such as the Preferred Roaming List, Extended Preferred Roaming List, Shared Secret Data (SSD), and manufacturer-specific NAM parameters.\textsuperscript{119}—all of which can be surreptitiously updated by the wireless carrier through Over-the-Air Service

\textsuperscript{117} See Levine, \textit{Digital Switching: Cellular & PCS Lectures April 17 & 24, 2001}, p. 11 (diagram showing 120° tri-sectored cell site radiation pattern); \textit{see also} O’Connor, Terrence P., \textit{Provider Side Cell Phone Forensics}, Small Scale Digital Device Forensics Journal, Vol. 3, No. 1, June 2009 ISSN# 1941-6164, p. 1 (“The [][various] directional antennas on the cell tower nominally divide the 360 degree circumference around the tower into three 120 degree areas, one area for each antenna.” (technical correction added in brackets)).

\textsuperscript{118} \textit{ECPA Reform and the Revolution in Location Based Technologies and Services}, 111th Cong. 2nd sess. (Jun. 24, 2010) (Prepared Statement of Matt Blaze), p. 23 (PDF, p. 27) (“Network based location enables a cellular provider to identify the sector in which a user's [][wireless device] is located, and, in some cases, to pinpoint their location within a sector.”).

\textsuperscript{119} The Preferred Roaming List, Extended Preferred Roaming List, and Shared Secret Data (SSD) are further explained in this subsection and in proceeding subsections.
Provisioning (OTASP)\(^{120}\)[\(^{121}\)] OTASP is the process of reading,\(^{122}\) writing,\(^{123}\) and/or deleting\(^{124}\) data to/from the internal storage device (e.g., NAM) of an Access Terminal using commands sent by the Access Network to the Access Terminal over the air interface.\(^{125}\) OTASP “allows a potential wireless service subscriber to activate (i.e., become authorized for) new wireless service, and allows an existing wireless subscriber to make changes in existing services without the intervention of a third party [(i.e., physical access to the user’s device by a human)].”\(^{126}\) OTASP can be initiated by either the Access Terminal or Access Network.\(^{127}\) When initiated by the Access Network, the wireless carrier conducts Over-the-Air Parameter Administration (OTAPA)\(^{128}\) to update the NAM or other.

120. See TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, § 1.1, p. 1.1 (listing features that can be provisioned over-the-air); *id.* § 3.3, p. 3.12 (listing programming procedures for OTASP).

121. Another method used by wireless carriers to update wireless devices over-the-air is IP Based Over-the-Air Device Management (IOTA-DM) using the Open Mobile Alliance Device Management (OMA DM) protocol. See 3rd Generation Partnership Project 2, 3GPP2 C.S0064-0, *IP Based Over-the-Air Device Management (IOTA-DM) for cdma2000 Systems, Release 0* (Sept. 6, 2012). “OMA DM provides an integrated and extensible framework for the OTA management needs of 3G mobile devices and beyond. The standard includes the OMA DM protocol specification, which is based on the SyncML DM protocol.” *Id.*, § 1, p. 1.1 (internal citation omitted). “A method for updating firmware over the air (FOTA) based on OMA DM is also specified.” *Id.* (citation omitted). “Firmware over-the-air (FOTA) is the process of updating mobile station firmware over-the-air.” Primary use of firmware update capability is to rectify critical defects, that may compromise the end user safety, through updating firmware. It may be used to update new version of firmware to the mobile station.” *Id.*, § 8, p. 8.1 (emphasis added). OMA DM is intended to replace OTASP but it is still backward compatible with the OTASP standard. See *id.*, § 1.4, p. 1.6 (“For backward compatibility with OTASP/OTAPA, the mobile and the server shall support converting IOTA-DM data to OTASP/OTAPA data.” (internal citation omitted)).

122. See TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, § 3.5, p. 3.48 et seq. (explaining the data sent to Access Networks by Access Terminals via reverse link messages during OTASP).

123. See *id.*, § 4.5, p. 4.9 et seq. (explaining the data sent to Access Terminals by Access Networks via forward link messages during OTASP).

124. See *id*.

125. See *id.*, § 1.2.1, p. 1.4 (“Over-the-Air Service Provisioning (OTASP). A process of provisioning mobile station operational parameters over the air interface.”).


127. TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, § 3.2, p. 3.2 (“Over-the-air service provisioning (OTASP) can be initiated in two ways: by the user and by the network.”).

128. See *id.*, § 1.2.1, p. 1.4 (“Over-the-Air Parameter Administration (OTAPA). Network
operational parameters in the Access Terminal over-the-air. "OTAPA sessions are initiated autonomously by the network, and proceed without any subscriber involvement or knowledge and with no limitation on the subscriber’s ability to receive telecommunications services." In order to read data from a specific NAM, the Access Network transmits a Configuration Request Message to the Access Terminal. In response to the Configuration Request Message, the Access Terminal transmits a Configuration Response Message providing the Access Network with its stored NAM parameters. In order to write data to an Access Terminal NAM, the Access Network transmits a Download Request Message containing the NAM parameter blocks sought to be written. In order to cause the Access Terminal to commit the parameter blocks to permanent NAM memory, the Access Network transmits a Commit Request Message to the Access Terminal. A newly purchased Access Terminal will receive an initial NAM provisioning and, throughout the course of service, the Access Network will periodically update the data stored on the NAM via OTAPA according to relevant protocols.

Prior to reading, writing, and/or deleting data to/from an Access Terminal NAM, the Access Network must first complete SPC/SPL and SPASM security procedures to unlock and gain access to the NAM. The Service Programming Code (SPC) and Service initiated OTASP process of provisioning mobile station operational parameters over the air interface.”; id. § 3.2, p. 3.2 (“The network-initiated procedure... is also built upon the over-the-air programming protocol and procedures that support the OTASP feature.”).

See id. § 3.2, p. 3.2 (“OTAPA provides a tool for the wireless service provider to update NAM indicators and parameters.”).

See TIA-41.000-E-4[E], Introduction to Mobile Application Part (MAP), § § 3.1, p. 000.21.


See id.

See id., § 3.3.1, p. 3.13-3.14.

See id., § 3.3.1, p. 3.14-3.16.

See id., § 4.2.1, p. 4.1.

See id., § 1.2.1, p. 1.5 (“Service Programming Code (SPC). A secret code assigned to the mobile station and known to the authorized network entity.”)
Programming Lock (SPL) parameter[^137] contained on the NAM “prevents the over-the-air provisioning of certain mobile station parameters by an unauthorized network entity.”[^138] The SPL parameter contains the SPC, taking a numeric value of 1 to 999,999[^139], “used for unlocking the mobile station parameters for programming or reprogramming.”[^140] Due to the weak security of the SPC/SPL “combination lock” type mechanism,[^141] an Access Terminal NAM also uses the Subscriber Parameter Administration Security Mechanism (SPASM). SPASM serves the same purpose as SPC/SPL[^142] but, instead of a simple numeric code, SPASM utilizes the Shared Secret Data (SSD) stored on the NAM and known only to the Access Terminal and home AN-AAA server.[^143] SPASM uses cryptographic keys and mathematical equations to conduct a type of challenge-response between the Access Terminal and Access Network so that the Access Terminal can verify that it is having its NAM provisioned by an authorized entity.[^144]

Most commonly, the wireless carrier uses OTAPA to set the NAM’s Preferred Roaming List and Extended Preferred Roaming List with values that (1) designate which radio frequencies to scan in order to acquire a system (i.e., groups of wireless carrier cell sites), and (2) designate which systems are authorized for providing service.[^145]

[^137]: See id. (“Service Programming Lock (SPL). A protection provided for preventing the over-the-air provisioning of certain mobile station parameters by unauthorized network entity by way of verifying the Service Programming Code (SPC).”)

[^138]: Id., § 1.1, p. 1.1.

[^139]: Id., § 3.3.6, p. 3.43, Table 3.3.6-1 (Service Programming Code Values).

[^140]: Id., § 3.3.6, p. 3.42.

[^141]: A numeric security code or combination having only 999,999 possible values is susceptible to a “brute force” attack, i.e., a security code “guessing” attack.

[^142]: See id., § 1.2.1, p. 1.5 (“Subscriber Parameter Administration Security Mechanism (SPASM). Security mechanism protecting parameters and indicators of active NAM from programming by an unauthorized network entity during the OTAPA session.”)

[^143]: See id., § 3.3.7, p. 3.43 (explaining how SPASM works).

[^144]: See id.

[^145]: “Two categories of the preferred roaming list are defined: The Preferred Roaming List and the Extended Preferred Roaming List.” Id., § 3.5.5, p. 3.93. When accessing 1xEV-DO Access Networks, a High Rate Packet Data (HRPD) (i.e., 1xEV-DO) Access Terminal uses its Extended Acquisition Records and Extended System Records contained in its Extended Preferred Roaming List. See id., § 3.5.5.3.2, p. 3.114-3.120 and 3.5.5.2.2.11, p. 3.112. However, because the Extended Preferred Roaming List is considered a category of the...
preferred roaming list consists of two tables: the system table and the acquisition table."[146] The Acquisition Table lists Acquisition Records consisting of “parameters that the mobile station can use to acquire a system. Each type of acquisition record is tailored for use in acquiring a particular kind of system.”[147] The System Table lists System Records containing “parameters that the mobile station can use for identifying an acquired system, for determining whether an acquired system is the optimal system on which to operate and for determining the mobile station’s roaming status.”[148] In basic terms, the Acquisition Table contains a list of radio frequencies[149] the Access Terminal may scan in order to locate transmitting Access Networks, and the System Table contains a list of HRPD IPv6[150] subnets[151] acting as unique identification numbers for groups of Access Networks (i.e., systems) authorized for providing service.[152] In addition to the subnet information identifying a system, each record in the System Table also contains “an indicator of whether the system is preferred or negative, the roaming status that should be indicated by the mobile

Preferred Roaming List (see id., § 3.5.5, p. 3.93), the “Extended” prefix will be omitted and the terms “Preferred Roaming List,” “Acquisition Table,” “Acquisition Record,” “System Table,” and “System Record” will be used from this point forward for sake of simplicity.

147. Id., § 3.5.5.2, p. 3.98.
148. Id., § 3.5.5.3, p. 3.112.
149. See id., § 3.5.5.2.11, p. 3.112 (Generic Acquisition Record for HRPD (i.e., 1xEV-DO Rel. 0) containing band-class and channel number).
150. In 1xEV-DO Rel. 0, Access Network sectors are identified by 128-bit Internet Protocol Version 6 (IPv6) addresses. See TIA-856-2[E], cdma2000 High Rate Packet Data Air Interface Specification – Addendum 2, § 10.9, p. 10.11 (section from more recent version of IS-856 covering “SectorID Provisioning”); see also IETF RFC 2373, IP Version 6 Addressing Architecture. The subnet corresponding to any given Access Network IPv6 address identifies the system to which the Access Network belongs. In other words, the 1xEV-DO subnets take the place of the System Identification numbers (SIDs) and Network Identification numbers (NIDs) used to identify groups of cell sites.
151. See id., § 3.5.5.3.2-3.5.5.3.2.1, p. 3.118-3.20 (indicating that the system ID record for HRPD (i.e., 1xEV-DO Rel. 0) System Table contains the following data fields used to deduce the IPv6 subnet identifying the 1xEV-DO system: SUBNET_COMMON_INCLUDED, SUBNET_LSB_LENGTH, SUBNET_LSB, SUBNET_COMMON_OFFSET, SUBNET_COMMON_LENGTH, and SUBNET_COMMON.).
152. See Technical Explanations, Section II(B)(3)(c)(i), infra (explaining use of the System Table).
station, the relative priority of the system and its geographic region.”[153] “The records in the acquisition table are in order of priority (highest priority first) according to desired mobile station system selection scan order.”[154]

b. Access Terminal Initialization State procedures: identifying and acquiring a 1xEV-DO Rel. 0 Access Network after initial power-on.

The first step of identifying and acquiring an Access Network is to place the Access Terminal into the Initialization State by powering it on.[155] In the case of an aircard, this is accomplished by plugging the device into the PCMCIA slot of a host laptop computer. Once plugged in, the Access Terminal receives power from the laptop's power source and its radio transceiver is automatically initiated. Once powered on, the Access Terminal is considered to be in the Inactive Substate of the Initialization State.[156] Prior to any interaction by the human user, the Access Terminal begins the process of identifying radio signals belonging to available Access Networks[157] authorized to provide 1xEV-DO Rel. 0 data service. In order to accomplish this task, the Access Terminal hardware transitions out of the Inactive Substate and into the Network Determination Substate.[158]

i. Network Determination Substate.

While in the Network Determination Substate, “the access terminal selects a CDMA Channel on which to try and acquire the access network.”[159] Considering Access Networks

---

154. Id.
155. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 6.2.6.1.2.1, p. 6.12 (“The access terminal shall enter the Initialization State when the Default Air-Link Management Protocol is instantiated. This may happen on events such as network redirection and initial power-on.”).
156. See id., § 6.3.1, p. 6.18 (“In this state the protocol waits for an Activate command.”).
157. See id., § 6.2.6.1.2, p. 6.11 (“In the Initialization State the access terminal has no information about the serving access network. In this state the access terminal selects a serving access network and obtains time synchronization from the access network.”).
158. See id., § 6.3.1, p. 6.18 (“Network Determination State: In this state the access terminal chooses an access network on which to operate.”).
159. See id., § 6.3.6.1.3, p. 6.22 (internal reference omitted).
can transmit on any number of radio frequencies, the Access Terminal must first select a frequency to monitor using its Preferred Roaming List (stored on the Access Terminal NAM) through a process called System Selection for Preferred Roaming (SSPR). “The goal of System Selection for Preferred Roaming (SSPR) is for the mobile station to acquire the most preferred system using the information from the preferred roaming list stored in the mobile station[].” As previously explained, “[t]he preferred roaming list consists of two tables: the system table and the acquisition table.” While in the Network Determination Substate, the Access Terminal initiates System Selection for Preferred Roaming (SSPR) by reading from the Acquisition Table to obtain either CDMA frequency blocks or specific CDMA channels within frequency blocks of which to scan for available Access Networks.

In the case of 1xEV-DO Rel. 0 or other High Rate Packet Data (HRPD) service, the Acquisition Table will have one or more “Generic Acquisition Record for HRPD” consisting of a “Band Class number corresponding to the frequency assignment of the channel” and a “channel number corresponding to the Band Class[].” The various Preferred Roaming List “Generic Acquisition Record for HRPD” entries are listed according to selection preference. The Access Terminal will begin by selecting the entry having the highest preference and then it will copy the relevant channel(s) to be scanned into a temporary Channel Record maintained on its internal storage. Once the Access Terminal makes a

---

160. See id., § 9.2.1.1.1, p. 9.6 et seq. (Channel Spacing and Designation).
161. See TIA-683-D, Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, § 1.2.2, p. 1.7 (“PR_LIST s-p - Preferred Roaming List. Contains information to assist the mobile station system selection and acquisition process. Retained by the mobile station when the power is turned off.”).
162. See id., § 3.3.5, p. 3.42 (internal reference and NAM indicator name omitted).
164. See id., § 3.5.5.2.2.11, p. 3.112.
165. See id., § 3.5.5.2.1, p. 3.100 et seq. (listing Acquisition Record Formats).
166. See id., § 3.5.5.2, p. 3.100 (“If ACQ_TABLE contains more than one acquisition record, these records should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.”).
167. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 6.3.6.1.3, p. 6.22 (“In the Network Determination State the access terminal selects a CDMA Channel (see 10.1) on which to try and acquire the access network.”); § 10.1, p. 10.1
Channel Record, it transitions from the Network Determination Substate to the Pilot Acquisition Substate.\footnote{168}

\section*{ii. Pilot Acquisition Substate.}

“In the Pilot Acquisition S[ubs]tate the access terminal acquires the Forward Pilot Channel of the selected CDMA Channel.”\footnote{169} The pilot channel is an “unmodulated direct sequence spread spectrum signal continuously transmitted at a fixed power”\footnote{170} by each Access Network sector. The pilot channel “is continually transmitting an all zero signal, which is covered by a Walsh code 0,”\footnote{171} and is only identifiable because the “all-zero baseband stream is [] multiplied by a pair of quadrature PN sequences.”\footnote{172} Because of the all-zero baseband stream, “the pilot channel has very good SNR [(Signal to Noise Ration)] making it easy for mobiles to find it.”\footnote{173} “The pilot is the first broadcast physical channel that is searched and acquired by the mobile stations immediately after the mobile is powered on.”\footnote{174} “The main functions of the pilot channel [in 1xEV-DO Rel. 0] are the same [as] those of forward common pilot channels in cdma2000 or IS95.”\footnote{175} The pilot channel is used to broadcast a unique signature (etymologically referred to as a PN sequence, short code, PN offset, or PN code) used by Access Terminals to identify and differentiate between

\footnote{168}{See id., § 6.3.6.1.3, p. 6.23 (“Upon selecting a CDMA Channel the access terminal shall enter the Pilot Acquisition State.”).}

\footnote{169}{Id., § 6.3.6.1.4, p. 6.23.}

\footnote{170}{See Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 38.}


\footnote{172}{See Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 39.}

\footnote{173}{Langton, CDMA Tutorial: Intuitive Guide to Principles of Communications, p. 12; see also Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 39 (“As a result, the pilot is an easy-to-capture signal, which mainly reflects the phase of the PN sequence used as the base station's short code.”).}

\footnote{174}{Id., p. 38.}

\footnote{175}{Id., p. 235.}
all Access Network sectors in a given area. “The PN sequence, with a specific offset, forms
a short code, which uniquely identifies the pilot and thereby the particular sector that is
transmitting that pilot signal.”[176] Each CDMA transmit frequency, corresponding to a band
class CDMA channel number, supports a total of 512 unique PN sequences of which short
codes can be derived for any given area.[177]

In addition to using the short code to identify the Access Network, the Access
Terminal also uses the short code to identify and decode all other forward link radio channels
transmitted by the Access Network. This is required because the Access Network uses the
short code “to spread [(i.e., encode)] the composite signal (containing all code channels) that
is transmitted to the users in a cell.”[178] “[T]he base station-specific short codes serve as the
base stations' signatures, allowing differentiation and de-spreading of desired base stations'
signals in the presence of other-cell interference.”[179] Aside from physical layer
identification and decoding, the Access Terminal also uses the “power and timing of the pilot
channel”[180] to simplify the determination of the best serving Access Network[181] and to
help in “acquiring the system timing and fast synchronization.”[182][183] Although the pilot

176. Id., p. 39.

177. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 9.3.1.3.4, p. 9.90 (“Pilot Channels shall be identified by an offset index in the range from 0 through 511 inclusive.”).

178. Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 18; see also TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 9.3.1.3.1, p. 9.60 fig. 9.3.1.3.1-1, “Forward Channel Structure” (showing composite Walsh
channels labeled “A” and “B” being fed into the Quadrature Spreading block prior to output
of Forward Modulated waveform).


180. Id., p. 235.

181. See id., p. 249 (“The AT uses the measured SINR [(Signal to Interference and Noise Ration)] of the strongest pilot and the thresholds defined by the AN to determine the highest
data rate it can reliably decode as well as the identity of the corresponding best serving sector.”).

182. Id.

183. “An additional function of the pilot [(specific to 1xEV-DO)] is to provide the access
terminal with a means of predicting the receive C/I for the purpose of access-terminal-
directed forward data rate control (DRC) of the Data Channel transmission.” TIA/EIA/IS-
856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 9.3.1.3.1, p. 9.56 fn. 54.
channel does not transmit system time, the nature of the PN sequence transmission allows the Access Terminal to synchronize its clock ticks to the clock ticks of the Access Network. This synchronization is required because all forward link channels are placed into time slots “aligned to the PN rolls of the zero-offset PN sequences and... to system time on even-second ticks.”

“Upon entering the Pilot Acquisition State, the access terminal shall tune to the selected CDMA Channel and shall search for the pilot.” If the Access Terminal is unable to acquire at least one pilot signal from the selected CDMA channel within a set amount of time, the Access Terminal makes a new channel record using the next highest priority entry from the Preferred Roaming List Acquisition Table. For example, assume a scenario where the highest priority entry in the Acquisition Table contains a band class and channel number equating to 880.020–880.650 MHz radio frequency for the Access Network and the second highest priority entry in the Acquisition Table contains a band class and channel number equating to 891.510–893.370 MHz radio frequency for the Access Network. Under this scenario, the Access Terminal will first monitor 880.020–880.650 MHz for a pilot signal and if no pilot is detected, the Access Terminal will then monitor 891.510–893.370 MHz for a pilot signal. This process will continue for each entry in the Acquisition Table of the Preferred Roaming List until an initial Access Network pilot signal is detected. Once

184. See id., § 9.3.1.3.4, p. 9.90 (“The chip rate for the pilot PN sequence shall be 1.2288Mcps. The pilot PN sequence period is 32768/1228800 = 26.666… ms, and exactly 75 pilot PN sequence repetitions occur every 2 seconds.”); id. (“The zero-offset pilot PN sequence shall be such that the start of the sequence shall be output at the beginning of every even second in time, referenced to access network transmission time.”).

185. In other words, the noted synchronization causes the “second hand” of the Access Terminal's internal clock to tick in unison with the “second hand” of the Access Network's internal clock but the absolute system time is still unknown to the Access Terminal.

186. Id., § 9.3.1.3.1, p. 9.57; see also id., § 9.3.1.3.6.1, p. 9.93 (“Each sector shall use a time base reference from which all time-critical transmission components, including pilot PN sequences, slots, and Walsh functions, shall be derived.”).

187. Id., § 6.3.6.1.3, p. 6.23.

188. See id. (“If the access terminal fails to acquire the pilot within [a specified amount of] seconds of entering the Pilot Acquisition State, it shall enter the Network Determination State.”).

189. Through the Route Update Protocol, additional pilot signals for additional Access
the Access Terminal has acquired the pilot channel, derived the short code, and synchronized its clock ticks to the system timing, it transitions out of the Pilot Acquisition Substate and into the Synchronization Substate.\footnote{190}

\section*{iii. Synchronization Substate.}

In the Synchronization Substate, “the access terminal synchronizes to the Control Channel cycle, receives the Sync message, and synchronizes to system time.”\footnote{191} In 1xEV-DO Rel. 0, the Sync message is transmitted on the Control Channel,\footnote{192} a forward link traffic channel, which takes the place of the Sync Channel used in 1xRTT and in other earlier CDMA communications systems.\footnote{193} “The access network broadcasts the Sync message to convey basic network and timing information.”\footnote{194} The “broadcast” addressing for the Sync message means all Access Terminals are sent the same Sync message at the same time.\footnote{195} The Access Network uses the Sync message to write network specific data to the internal storage devices of all Access Terminals attempting to acquire the network. In 1xEV-DO, the Sync message contains five parameters (\textit{i.e.}, data fields) sent to the Access Terminal: (1) MessageID, (2) MaximumRevision, (3) MinimumRevision, (4) PilotPN, and (5) SystemTime.\footnote{196}[\footnote{197}] Upon receiving the Sync message, the Access Terminal “reads and

Network sectors are detected and logged after the Access Terminal acquires the initial Access Network. The details of this process are explained in the \textit{Technical Explanations}, Section II(B)(3)(d)(i), infra.

\footnote{190. See id., § 6.3.6.1.4, p. 6.23 (“If the access terminal acquires the pilot, it shall enter the Synchronization State.”) (footnote omitted)).

\footnote{191. See id., § 6.3.1, p. 6.18.

\footnote{192. See id., § 6.3.6.1, p. 6.22 (“The access network shall broadcast the Sync message periodically in a synchronous Control Channel capsule.”)).


\footnote{194. TIA/EIA/IS-856-1, \textit{cdma2000 High Rate Packet Data Air Interface Specification}, § 6.3.6.2.1, p. 6.23.

\footnote{195. See id. (the “addressing” table entry is set to “broadcast” for the Sync message) & § 6.3.6.1, p. 6.22 (“The access network shall broadcast the Sync message periodically in a synchronous Control Channel capsule.”)).

\footnote{196. Unlike the pilot signal that provides clock tick synchronization, the SystemTime parameter of the Sync message provides the Access Terminal with an absolute system time value.

\footnote{197. See id. § 6.3.6.2.1, p. 6.24.}
stores all the parameters in the message that are defined in the mobile protocol revision and ignores the rest.”[198] After storing the data contained in the Sync message, the Access Terminal checks to see if its protocol revision number is between the MinimumRevision and MaximumRevision fields of the Access Network.[199] If the Access Terminal's revision number is not within the specified range then the Access Terminal and Access Network are not compatible and the Access Terminal transitions back to the Network Determination Substate.[200] If the Access Terminal's revision number is within the specified range then the Access Terminal and Access Network are compatible and the Access Terminal sets its “time to the time specified in the message[.]”[201] At this point, the Access Terminal has acquired the network and transitions out of the Initialization State[202] and into the Idle State.

c. Access Terminal Idle State procedures: preparing to open a connection and opening a connection with a 1xEV-DO Rel. 0 Access Network.

While in the Idle State, the Access Terminal's actions are primarily dictated by the Default Idle State Protocol, which “provides the procedures and messages used by the access terminal and the access network when the access terminal has acquired a network and a connection is not open.”[203] There are seven primary functions performed by the Access Terminal while in the Idle State:[204] (1) receiving, processing, and storing to internal storage the Access Network's Overhead Messages, (2) transmission of Access Probes to the Access Network to initiate session establishment and open a connection, (3) establishing an open session with the Access Network, (4) application of encryption and authentication keys for

199. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 6.3.6.1.5, p. 6.23.
200. See id.
201. Id., § 6.3.6.1.5, p. 6.23.
202. Inactive, Network Determination, Pilot Acquisition, and Synchronization were all substates of the Initialization State.
204. There are other functions relevant to this state but, unless otherwise noted in later subsections, they are immaterial to the operation of the FBI's cell site emulators (as used to locate the aircard) and will not be addressed.
use in the security layer, (5) obtaining identifying information from Access Terminal
hardware using the HardwareIDRequest message, and (6) opening a connection with the
Access Network. The above listed functions are fully explained in the subsections
immediately below.

i. Receiving, processing, and storing to internal storage
the Access Network's Overhead Messages.

Upon entering the Idle State, the Access Terminal is in an Inactive Substate and
proceeds into the Monitor Substate. “When the access terminal is in the Monitor S[ubs]tate,
it continuously monitors the Control Channel.”[205] In this substate, “[t]he access terminal
shall monitor the overhead messages as specified in the Overhead Messages Protocol
[].”[206] The Overhead Messages are the QuickConfig message and the SectorParameters
message.[207] “These messages are broadcast by the access network over the Control
Channel.”[208] The “broadcast” addressing for the Overhead Messages means all Access
Terminals are sent the same Overhead Messages at the same time.[209] The QuickConfig and
SectorParameters messages contain numerous categories of essential data communicated to
Access Terminals.[210][211] “The QuickConfig message is used to indicate a change in the
overhead messages’ contents and to provide frequently changing information.”[212] “The

205. Id., § 6.4.6.1.5, p. 6.35.
206. Id., § 6.4.6.1.5.1, p. 6.35.
208. Id.
209. See 6.8.6.1.5, p. 6.118.
210. See id., § 6.8.6.2.1, p. 6.120 (Listing the following data fields for the QuickConfig
    message: MessageID, ColorCode, SectorID24, SectorSignature, AccessSignature, Redirect,
    RPCCount, ForwardTrafficValid, and a Reserved field.).
211. See id., § 6.8.6.2.2, p. 6.122 (Listing the following data fields for the
    SectorParameters message: MessageID, CountryCode, SectorID, SubnetMask,
    SectorSignature, Latitude, Longitude, RouteUpdateRadius, LeapSeconds, LocalTimeOffset,
    ReverseLinkSilenceDuration, ReverseLinkSilencePeriod, ChannelCount, Channel,
    NeighborCount, NeighborPilotPN, NeighborChannelIncluded, NeighborChannel,
    NeighborSearchWindowSizeIncluded, NeighborSearchWindowSize,
    NeighborSearchWindowOffsetIncluded, NeighborSearchWindowOffset, and a Reserved
    field.).
212. Id., § 6.8.6.2.1, p. 6.120.
SectorParameters message is used to convey sector specific information to the access terminals.\[213\] The Access Network uses the Overhead Messages to write network specific data to the internal storage devices of all Access Terminals that have acquired the network but are yet to establish a connection. “When a mobile station receives an overhead message, it should update all of its related stored information accordingly.”\[214\] The Access Terminal will also “store the signature associated with the message for future comparisons.”\[215\] By comparing the signature of the previous Overhead Message to the signature of the new Overhead Message, the Access Terminal can determine if it needs to update its stored data sent to it by the Access Network.\[216\] The Overhead Message parameters written to the Access Terminal by the Access Network are “essential parameters” that are “shared by protocols in the Connection Layer as well as protocols in other layers.”\[217\]

Immediately after receiving the SectorParameters message, the Access Terminal uses the SectorID and SubnetMask\[218\] data parameters to determine the subnet of the system to which the Access Network belongs. The SectorID of the SectorParameters message contains a 128-bit Internet Protocol Version 6 (IPv6) address that identifies the sector.\[219\] The SubnetMask of the SectorParameters message contains “the number of consecutive 1's in the subnet mask of the subnet to which th[e] sector belongs.”\[220\] In order to calculate the IPv6 subnet from the SectorParameters message, the Access Terminal conducts a mathematical

\[213\] Id., § 6.8.6.2.2, p. 6.121.
\[215\] TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 6.8.6.1.6, p. 6.119.
\[216\] See id., § 6.8.6.1.6, p. 6.118 (explaining the signature comparison process).
\[217\] Id., § 6.1.1, p. 6.2.
\[218\] See id., § 1.11, p. 1.15 (Explaining the IPv6 SubnetMask to be “[a] 128-bit value whose binary representation consists of \(n\) consecutive ‘1’s followed by 128-\(n\) consecutive ‘0’s.’”).
\[219\] See id., § 6.8.6.2.2, p. 6.123 (Defining the SectorID as the “Sector Address Identifier[]” and that “[t]he access network shall set this field to the 128-bit IPv6 address of th[e] sector.” (internal citation omitted)); see also IETF RFC 2373, IP Version 6 Addressing Architecture.
bitwise logical AND using the SectorID and the SubnetMask.\(^{[221]}\) As explained in Section II(B)(3)(a), \(supra\), the subnet of the serving sector acts as the unique identification number identifying the particular 1xEV-DO system being accessed by the Access Terminal. No two 1xEV-DO systems have the same subnet and all Access Networks belonging to any given system will have identical subnet values as calculated using the SectorID and SubnetMask. Once the Access Terminal deduces the subnet of the serving system, it checks its locally stored Preferred Roaming List System Table\(^{[222]}\) to determine if the subnet is listed as corresponding to a group of Access Networks (\(i.e.,\) a system) authorized for providing wireless service. If the subnet is not authorized, the Access Terminal ignores the Access Network and transitions back to the Network Determination Substate. If the subnet is authorized, the Access Terminal begins the access probe process to initiate session establishment with the Access Network.

\[\text{ii. Transmission of Access Probes to the Access Network to initiate session establishment and open a connection.}\]

Prior to the initial Access Probe process explained in this subsection, all radio signal transmissions are broadcast by the Access Network to the Access Terminal. Immediately after network acquisition, the Access Terminal is yet to transmit signals and the Access Network is yet to be made aware of the Access Terminal's presence.\(^{[223]}\) In order to establish a session and open a connection with the Access Network, the Access Terminal initiates an Access Attempt over the Reverse Access Channel belonging to the sector serving the Access Terminal.\(^{[224]}\) “Each access attempt may consist of one or more sub-attempts, each


\(^{[222]}\) See Technical Explanations, Section II(B)(3)(a), \(supra\) (explaining the Preferred Roaming List System Table and its purpose).

\(^{[223]}\) See id., p. 52 (“When the mobile first attempts to access the system, the base station has no information about the location of the mobile...”).

\(^{[224]}\) See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification,
consisting of repeated transmissions of the same message. Each message transmission is
called an **access probe**.[225] All Access Channel transmissions are spread (i.e., encoded)
using a long code created from stored data received via the Overhead messages.[227]
[228] A 1xEV-DO Access Probe transmission “consist[s] of a preamble followed by one or
more access channel physical layer packets.”[229] “During the preamble transmission, only
the Pilot Channel is transmitted.”[230] “During the Access Channel physical layer packet
transmission, both the Pilot Channel and the Data Channel are transmitted.”[231] The
physical layer packet transmissions contain higher layer Protocol Data Units[232] used for

§ 9.2.1.3.2, p. 9.33 (“The Access Channel is used by the access terminal to initiate
communication with the access network...”);

225. See Korowajczuk, Leonhard *et al.*, *Designing cdma2000 Systems*, John Wiley & Sons,
Concepts and Design Principles*, p. 247 (“The transmissions on the access channel are in the
form of access probes, each consisting of a preamble followed by one or more access
channel physical layer packets.” (internal figure note omitted));

226. See TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*,
§ 8.3.6.1.4.1.1, p. 8.25 (“The access terminal shall use the Access Channel long codes to
cover the entire probe.”).

227. See *id.*, § 8.3.6.1.4.1.2, p. 8.26, Table 8.3.6.1.4.1.2-1, Access Channel Long Code
Masks (showing that the long code mask for the Access Channel is comprised, in part, by the
ColorCode and SectorID); *id.*, § 8.3.6.1.4.1.2, p. 8.27 (“SectorID is given as public data of
Overhead Messages Protocol and corresponds to the sector to which the access terminal is
sending the access probe. [] ColorCode is given as public data of Overhead Messages
Protocol and corresponds to the sector to which the access terminal is sending the access
probe.”).

228. The entire forward link channel, which includes the Access Channel spread by the
Access Channel long code, is also collectively spread by the Access Network short code as
explained in the *Technical Explanations*, Section II(B)(3)(b)(ii), *supra*.

(internal figure note omitted).

230. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, §
9.2.1.3.2, p. 9.33; see also Etemad, *cdma2000 Evolution: System Concepts and Design
Principles*, p. 33 (“The preamble does not carry any m[e]ssages and it is transmitted to help
[the] base station capture the phase and timing of [the] user's transmission in the uplink.
Once the preamble is detected the base station can demodulate the message capsule and
process [the] MS's request.”).

231. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, §
9.2.1.3.2, p. 9.33-9.34.

232. See *id.*, § 8.3.3, p. 8.18 (defining the Protocol Data Unit for the Default Access
Channel MAC Protocol).
establishing a session and opening a connection with the Access Network.\[233\] A transmission sent on the Access Channel by the Access Terminal is always part of an Access Attempt dictated by the Access Probe process.

In 1xEV-DO, \[t\]he access procedure performed by the access channel MAC protocol is similar to that used in basic access mode of IS-2000.\[234\] “Namely, the AT keeps transmitting access probes at increasing power levels until it gets an acknowledgement back from the AN.”\[235\] The 1xEV-DO Access Probe process adopted from earlier CDMA technology solves the power control\[236\] problem inherent with initial reverse link transmissions: “When the mobile first attempts to access the system, the base station has no information about the location of the mobile and thus the power at which the mobile should access the system.”\[237\] An Access Attempt involves transmitting Access Probes “starting with a low initial power estimated by open-loop power control followed by power increments on every successive probe within an access attempt.”\[238\] “Similar to IS95 and cdma2000, the access terminal sends a series of access probes until it receives a response from the access network or the timer expires.”\[239\] “The transmission of request or response

233.  See id., § 8.3.6.1, p. 8.21 and Fig. 8.3.6-1. Access Channel MAC Packet Structure.


235.  Yang, 3G CDMA2000: Wireless System Engineering, p. 229; see also Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 52 (“The mobile attempts to access the system by transmitting a series of access probes. The first access probe is transmitted at a relatively low power and is followed by a series of successive probe transmissions of progressively higher power until an acknowledgment is received.”).

236.  1xEV-DO and other CDMA based technologies are dependent on strict power control across the various transceivers making up the network. See, e.g., Levine, Digital Switching: Cellular & PCS Lectures April 17 & 24, 2001, p. 58 (“When multiple transmitters send signals with different PN codes to a common receiver, the RSSI of all the signals must be very close to equal, or the strongest one will dominate all the others and only it can be decoded without errors. This was a major problem which caused malfunctions of a trial CDMA system used in tests by the Groupe Spécial Mobile in 1986 in Paris. Qualcomm revived the idea of CDMA for cellular in 1989 with an improved closed- loop feedback power control to keep all the received signals from deviating in individual power levels.”).


238.  Id., p. 247.

239.  Id.
messages through the air interface does not assure successful access to the system. The
process is only complete after the same message is sent a certain number of times or when
the MS receives a reception acknowledgement (ACK).”[240] In other words, the Access
Terminal transmits the same message over and over, each time increasing the transmission
power, until the Access Network responds with an acknowledgement that the message was
received. Once the Access Terminal receives the acknowledgement, it will begin
transmitting the next message using the same Access Probe process. As long as the Access
network continues to respond to Access Probes, the process will continue until the Access
Attempt is successfully completed (i.e., a session is established and a connection is open).

Before the Access Terminal can begin transmitting Access Probes, it first needs to receive and process the AccessParameters message[241] broadcast by the Access Network.
[242] The “broadcast” addressing for the AccessParameters message means all Access Terminals are sent the same message at the same time. The Access Network uses the AccessParameters message to write network specific data to the internal storage devices of all Access Terminals that are attempting to access the network after network acquisition.[243] The AccessParameters message contains numerous categories of essential data communicated to Access Terminals for use in power control and formatting of Access Probe transmissions.[244] Upon receiving the AccessParameters message, the Access Terminal reads and stores all data fields contained in the message. The Access Terminal uses the

---

240. Korowajczuk, Designing cdma2000 Systems, p. 254; see also TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 8.3.6.1.4.1.1, p. 8.25 (“The access terminal shall not change the probe data contents in between probes.”).

241. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 8.3.6.1.4.1.1, p. 8-25 (“Prior to sending the first probe of the probe sequence, the access terminal shall verify that the last AccessParameters message it received is current...”).

242. See id., § 8.3.6.2.6, p. 8-33 (the “addressing” table entry is set to “broadcast” for the AccessParameters message).

243. See id., § 8.3.6.2.6, p. 8-31 (“The AccessParameters message is used to convey Access Channel information to the access terminals.”).

244. See id., § 8.3.6.2.6, p. 8-31 (Listing the following data fields for the AccessParameters message: MessageID, AccessCycleDuration, AccessSignature, OpenLoopAdjust, ProbeInitialAdjust, ProbeNumStep, PowerStep, PreambleLength, CapsuleLengthMax, Apersistence, and a Reserved field.).
stored data fields, along with stored data fields from the Overhead Messages, to configure Access Probe transmissions and to facilitate Access Attempts.

### iii. Establishing an open session with the Access Network.

As noted in Section II(B)(3)(c)(ii), supra, the access channel physical layer packets initially sent by the Access Terminal during the Access Probe process contain data used to establish a session. Prior to establishing a session, “there are no communications between the access terminal and the access network.” The Access Network “may be unaware of the access terminal’s existence within its coverage area.” “Other than to open a session, an access terminal cannot communicate with an access network without having an open session.” “An HRPD session refers to a shared state between the access terminal and the access network. This shared state stores the protocols and protocol configurations that were negotiated and are used for communications between the access terminal and the access network.” A session should not be confused with a connection. In order to communicate with the Access Network over the air interface, the Access Terminal opens a session. In order to communicate with the Internet, the Access Terminal uses the established session.

---

245. See, e.g., id., § 8.3.6.1.4.1.1, p. 8-25 (using the OpenLoopAdjust and ProbeInitialAdjust data fields of the AccessParameters message for Access Probe power control).

246. See, e.g., id., § 8.3.6.1.4.1.1, p. 8-25 (using the SectorID and ColorCode data fields of the Overhead Messages for Access Channel long code mask).

247. During Access Attempts, in addition to configuring transmissions using data fields contained in the AccessParameters message and Overhead Messages, the Access Terminal also uses various well known fall-back data values or data values as designated by the Access Network via ConfigurationRequest messages (sent according to the the Generic Configuration Protocol) containing complex attributes including the InitialConfiguration Attribute and the PowerParameters Attribute (both of which contain numerous data fields and records sent to and stored by the Access Terminal). See id., § 8.3.7, p. 8.36-8.38.

248. Id., § 5.3.7.1.4, p. 5.23.

249. Id.

250. Id., § 1.9, p. 1.12.


252. See id. (“An air interface connection is a particular state of the air-link in which the access terminal is assigned a Forward Traffic Channel, a Reverse Traffic Channel and associated Medium Access Control (MAC) Channels.”).
session to open a connection with the underlying Packet Data Serving Node linked to the Access Network.\footnote{253} “During a single session the access terminal and the access network can open and close a connection multiple times[.]”\footnote{254} For session establishment, a powered-on Access Terminal will automatically initiate a session with a trusted Access Network without intervention or action from the user of the device.\footnote{255}

The first step to establishing a session where no prior session exists is for the Access Terminal to enter the Setup State\footnote{256} of the Default Address Management Protocol.\footnote{257} Once in the Setup State, the Access Terminal requests a Unicast Access Terminal Identifier (UATI) using the UATIRequest message.\footnote{258} For the Access Network, the UATI allows for “distinguishing among the different packets and [for] finding out which packet is from which AT.”\footnote{259} More precisely, the UATI is a unique 32-bit numerical address\footnote{260} used by the Access Terminal and Access Network MAC layer protocols to label and identify

\footnote{253} See Technical Explanations, Section II(B)(3)(c)(vi), infra (explaining the 1xEV-DO Rel. 0 connection establishment process).

\footnote{254} TIA/EIA/IS-856-1, \textit{cdma2000 High Rate Packet Data Air Interface Specification}, § 5.11, p. 5.1.

\footnote{255} The automatic nature of session establishment is unlike connection establishment which requires direct action by the Access Terminal user. See Technical Explanations, Section II(B)(3)(c)(vi), infra (explaining the 1xEV-DO Rel. 0 connection establishment process).

\footnote{256} See TIA/EIA/IS-856-1, \textit{cdma2000 High Rate Packet Data Air Interface Specification}, § 5.3.7.1.5, p. 5.24 (“In this state, the access terminal sends a request to the access network asking for a UATI and waits for the access network’s response.”).

\footnote{257} See \textit{id.}, § 5.3.1, p. 5.17 (“The Default Address Management Protocol provides the following functions: [ ] Initial UATI assignment[, and] Maintaining the access terminal unicast address as the access terminal moves between subnets.”).

\footnote{258} See \textit{id.}, § 5.3.7.1.5.1, p. 5.24 (“Upon entering the Setup State the access terminal shall... send a UATIRequest message.”); 5.3.7.2.1, p. 5.28 (“The access terminal sends the UATIRequest message to request that a UATI be assigned or re-assigned to it by the access network.”).

\footnote{259} Yang, \textit{3G CDMA2000: Wireless System Engineering}, p. 229 (“[W]hen an AN receives an access channel MAC packet, it checks the access terminal identifier record field of the MAC layer header and performs address matching”).

\footnote{260} See TIA/EIA/IS-856-1, \textit{cdma2000 High Rate Packet Data Air Interface Specification}, § 10.2, p. 10.2 (“The Access Terminal Identifier record provides a unicast, multicast, or broadcast access terminal address.”).
transmissions during the current session. When the Access Network receives the
UATIRequest message, it transmits a UATIAssignment message that assigns a UATI to the
Access Terminal for the session. The UATIAssignment message is a unicast
transmission containing numerous data fields that are written to the Access Terminal's
internal storage. The Access Terminal uses the data transmitted via the
UATIAssignment message, to deduce its assigned 32-bit UATI and adds the UATI
to its internally stored ReceiveATIList. Once the Access Terminal adds its assigned
UATI to its ReceiveATIList, it stops using the Default Address Management Protocol and
begins using the Default Session Configuration Protocol. This second protocol is used to
negotiate and configure a set of additional protocols to be used during the session. For
example, the Default Session Configuration Protocol is used to negotiate and configure the
Security Layer protocols discussed in Section II(B)(3)(c)(iv), infra. Once all relevant

261. See, e.g., id., § 8.2.6.1.4.2.4, p. 8.13 (Under a heading titled “Address Matching”
applicable to transmission received from the Forward Control Channel, the standard explains
that the “Access terminal shall forward the Security Layer packet along with the
SecurityLayerFormat and the ConnectionLayerFormat fields to the Security Layer if... the
ATIType field and the ATI field of the ATI Record in the MAC Layer header of a Security
Layer packet is equal to the ATIType and ATI fields of any member of the Address
Management Protocol’s ReceiveATIList.”); id., 8.2.6.2.1, p. 8.14 (All MAC Layer Headers
placed in front of Access Network transmitted Security Layer packets must contain the
Access Terminal’s “ATI Record.”).

262. The UATI is also sent by the Access Terminal to the new Access Network (target)
during a Connected State Route Update so that “the source AN []can lookup] the session
configuration parameters that are requested by the target[]” over the A13 interface.
ANSI/TIA-878-2, Interoperability Specification (IOS) for High Rate Packet Data (HRPD)
Radio Access Network Interfaces with Session Control in the Access Network, § 2.4, p. 2.3;
see also Technical Explanations, Section II(B)(3)(d) et seq., infra (explaining Route Updates,
i.e., handoffs).

263. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification,
§ 5.3.7.1.5.2, p. 5.24-5.25.

264. See id., § 5.3.7.2.2, p. 5.29 (Listing the following data fields for the UATIAssignment
message: MessageID, MessageSequence, Reserved1, SubnetIncluded, UATISubnetMask,
UATI04, UATIColorCode, UATI024, UpperOldUATILength, and a Reserved2 field).

265. See id., § 5.3.7.1.5.1, p. 5.24-5.25.

266. The UATI is unrelated to the Access Terminal's internally stored ESN.

267. See id.

268. See id., § 5.4.1, p. 5.35 (“The Default Session Configuration Protocol provides for the
negotiation and configuration of the set of protocols used during a session.”).
protocols are negotiated and configured, the session is open and “the access terminal and the access network use the negotiated protocols to exchange data and signaling in accordance with the requirements of each protocol.”[269] In other words, once a session is established, the Access Terminal can initiate a connection with the Access Network for the ultimate purpose of gaining access to the Internet. See Technical Explanations, Section II(B)(3)(c) (vi), infra (explaining the connection establishment process).

iv. Application of encryption and authentication keys for use in the security layer.

During session establishment, the Access Terminal and Access Network negotiate and configure the security layer protocols so that a session key may be created for use in data integrity, authentication, and encryption in the MAC layer. The session key is created using a session key exchange process, which “[p]rovides the procedures followed by the access network and by the access terminal to exchange security keys for authentication and encryption.”[270] The authentication keys are used “by the access network and the access terminal for authenticating traffic [(i.e., data)].”[271] Traffic authentication is done through a cryptographic authentication process[272] allowing for the Access Network and Access Terminal to ensure that transmissions being received are not coming from a man-in-the-middle who may be altering data or impersonating either the Access Network or Access Terminal.[273]

269. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 5.4.6.1.6, p. 5.44.
270. Id., § 7.1.1, p. 7.1.
271. Id.
272. “Authentication is a service that is used to establish the origin of information. That is, authentication services verify the identity of the user or system that created information (e.g., a transaction or message). This service supports the receiver in security relevant decisions, such as 'Is the sender an authorized user of this system?' or 'Is the sender permitted to read sensitive information?' Several cryptographic mechanisms may be used to provide authentication services....” National Institute of Standards and Technology, NIST Special Publication 800-57, Recommendations for Key Management -- Part I: General (Revised) (Mar. 2007), p. 30.
273. The type of man-in-the-middle attack protection provided in the 1xEV-DO Rel. 0 security layer is limited to scenarios where the attacker attempts to mimic a party after session establishment. Other types of 1xEV-DO Rel. 0 man-in-the-middle attacks, such as
The encryption keys are used “by the access network and the access terminal for encrypting traffic [(i.e., data)].” Traffic encryption is done through a cryptographic encryption process allowing for the Access Network and Access Terminal to exchange data that cannot be read by third-party eavesdroppers even if they gain full access to all transmissions. The noted encryption keys are used to encrypt all data content and signaling information in the MAC layer payload, which contains all higher layer protocol data units.

In other words, if encryption is invoked by the Access Network, all forward and reverse link data content and signaling information are protected from eavesdroppers over the air interface.

those launched prior to session establishment, are not prevented by the MAC payload authentication provided in the security layer. As explained later in this subsection, the various authentication keys are ultimately derived from Hash-based Key Derivation Function using a shared secret (i.e., the session key or “SKey”) created through the Diffie-Hellman Pair-Wise Key Establishment Scheme. “The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack. In this attack, an opponent Carol intercepts Alice's public value and sends her own public value to Bob. When Bob transmits his public value, Carol substitutes it with her own and sends it to Alice. Carol and Alice thus agree on one shared key and Carol and Bob agree on another shared key. After this exchange, Carol simply decrypts any messages sent out by Alice or Bob, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the other party. This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants.” RSA Laboratories [website], RSA Laboratories - 3.6.1 What is Diffie-Hellman?, http://www.rsa.com/rsalabs/node.asp?id=2248 (last accessed: Mar. 23, 2012).

Applying the above scenario to 1xEV-DO Rel. 0 with its use of Diffie-Hellman without supplementary two-party authentication, Carol operates a cell site emulator to become a man-in-the-middle between Bob's Access Terminal and Alice's legitimate wireless carrier cell site.


275. “Encryption is used to provide confidentiality for data. The data to be protected is called plaintext when in its original form. Encryption transforms the data into ciphertext. Ciphertext can be transformed back into plaintext using decryption. The Approved algorithms for encryption/decryption are symmetric key algorithms: AES and TDEA....” NIST Special Publication 800-57, Recommendations for Key Management -- Part 1: General (Revised), p. 35.

276. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 8.1.2, p. 8.2.8-4, Fig. 8.1.2-1 (“Control Channel MAC Layer Packet Encapsulation”), Fig. 8.1.2-2 (“Access Channel MAC Layer Packet Encapsulation”), Fig. 8.1.2-3 (“Forward Traffic Channel MAC Layer Packet Encapsulation”), and Fig. 8.1.2-4 (“Reverse Traffic Channel MAC Layer Packet Encapsulation”).

277. Although the MAC layer payload is encrypted, the MAC layer header, which is neither encrypted nor authenticated, contains the Access Terminal Identifier (e.g., the UATI) in plaintext. See id., § 8.6.2.1, p. 8.14. However, as explained in the technical Explanations, Section II(B)(3)(c)(iii), supra, the UATI is a randomly assigned value used for MAC layer...
During the session key exchange process, the Access Network and Access Terminal use the DH Key Exchange Protocol outlining “a method for session key exchange based on Diffie-Hellman (DH).”[278] “The Diffie-Hellman (DH) key exchange protocol provides a method for session key exchanges based on the DH key exchange algorithm.”[279] The Diffie-Hellman key exchange algorithm is an asymmetric key algorithm[280] allowing for “two users to exchange a secret key over an insecure medium without any prior secrets.”[281] In Diffie-Hellman, “both parties contribute information to the key agreement process.”[282] The Diffie-Hellman session key created by the Access Network and Access Terminal is referred to as the SKey and is either a 768-bit key or 1024-bit key.[283] After the Skey is created, the Access Network and Access Terminal separately split their SKey copies into “eight sub-fields within the SKey. These sub-fields are of equal length.”[284] The eight sub-fields are then used with Hash-based Key Derivation Functions (HKDFs)[285] to create four addressing purposes and it cannot be used by an eavesdropper to identify Access Terminal hardware.

278. Id., § 7.6.1., p. 7.22.
280. “Asymmetric key algorithms, commonly known as public key algorithms, use two related keys (i.e., a key pair) to perform their functions: a public key and a private key. The public key may be known by anyone; the private key should be under the sole control of the entity that “owns” the key pair. Even though the public and private keys of a key pair are related, knowledge of the public key does not reveal the private key.” NIST Special Publication 800-57, Recommendations for Key Management -- Part 1: General (Revised), p. 35 (footnote omitted).
283. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 7.6.7, p. 7.48, Tab. 7.6.7-1.
284. Id., § 7.6.5.1.3, p. 7.28.
285. “Cryptographic hash functions can be used as building blocks in key derivation functions (KDFs).... KDFs using cryptographic hash functions as their building blocks are called Hash-based Key Derivation Functions (HKDFs). The main purpose of an HKDF is to generate (i.e., derive) secret keys from a secret value (e.g., a shared key, or a shared secret in a key agreement scheme) that is shared between communicating parties. The security strengths of the derived secret keys are limited to the security strength of the secret value. The security strength of the secret value shall meet or exceed the desired security strengths.
pairs of 160-bit authentication and encryption key values for use on each of the forward and reverse link channels transmitted/received by the Access Network and Access Terminal.[286]

Each of the four 160-bit authentication keys are used to authenticate packets on their respective channels[287] via Keyed-Hash Message Authentication Codes (HMACs)[288] derived from the SHA-1 cryptographic hash function.[289] For encryption purposes, each of the four 160-bit encryption keys are truncated into 128-bit AES (based on Rijndael)[290]


286. Id., § 7.6.5.1.3, p. 7.28-7.29 and Fig. 7.6.5.1-1 (“Message Bits for Generation of Authentication and Encryption Keys”).

287. IS-856 only defines procedures “for authentication of access channel MAC layer packets by applying the SHA-1 hash function to message bits (ACPAC - Access Channel MAC Layer Packet Authentication Code).” Korowajczuk, Designing cdma2000 Systems, p. 338. However, data integrity and authentication of packets sent over traffic channels and the control channel can also be implemented by any 1xEV-DO Rel. 0 network considering authentication keys are defined and generated for “the Forward Traffic Channel” (i.e., FACAuthKey), “the Reverse Traffic Channel” (i.e., RACAuthKey), and “the Control Channel” (i.e., FPCAuthKey). TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 7.6.3.2, p. 7.22.

288. “Message authentication codes (MACs) provide data authentication and integrity protection.... MAC algorithms that are based on cryptographic hash functions[] [are] called HMAC algorithms... The HMAC output is generated from the secret key and the string of 'text' to be MACed (e.g., a message to be sent) using the HMAC algorithm. The MacTag is provided to the MacTag verifier, along with the 'text' that was MACed (e.g., the sender transmits both the MacTag and the 'text' that was MACed to the intended receiver). [] The verifier computes an HMAC output on the received 'text' using the same key and HMAC algorithm that was used by the HMAC generator, generates a MacTag (either a full or truncated HMAC output), and then compares the generated MacTag with the received MacTag. If the two values match, the 'text' has been correctly received, and the verifier is assured that the entity that generated the MacTag is a member of the community of users that share the key.” NIST Special Publication 800-107, Recommendation for Applications Using Approved Hash Algorithms, p. 12.

289. SHA-1, as well as SHA-224, SHA-256, SHA-384, SHA512, SHA-512/224 and SHA-512/256, are all “iterative, one-way hash functions that can process a message to produce a condensed representation called a message digest. These algorithms enable the determination of a message’s integrity; any change to the message will, with a very high probability, result in a different message digest. This property is useful in the generation and verification of digital signatures and message authentication codes, and in the generation of random numbers or bits.” National Institute of Standards and Technology, FIPS PUB 180-4, Federal Information Processing Standards Publication: Secure Hash Standard (SHS) (Mar. 2012), p. 3.

290. AES, based on Rijndael, is “a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in [][the AES] standard.” National Institute of Standards and Technology, FIPS PUB 197, Announcing the
encryption keys which are used for encrypting packets on their respective channels via the AES symmetrical key algorithm.

If attempting to crack 1xEV-DO Rel. 0 security layer encryption via cryptanalysis, the 1024-bit Diffie-Hellman asymmetrical keys and the 128-bit AES symmetrical keys are considered secure for the year 2008. In general terms, the protections provided by encryption are primarily based on current computer technology being unable to quickly compute values using factoring algorithms and discrete logarithm attacks. “The first successful factorization of a 768-bit RSA modulus was not reported until December 2009. This effort required six months of computations using highly sophisticated equipment. According to the paper’s authors, factoring a 1024-bit modulus would be 'one thousand times harder' than a 768-bit one. This means that another 6-7 years are likely to pass before 1024-bit numbers could realistically be factored.” The 768-bit number factored in December of 2009 was in the context of RSA—an asymmetrical cryptographic algorithm using integer

---


291. See Telecommunications Industry Association, TIA-925-1 [E] (Addendum to TIA-925), Enhanced Subscriber Privacy for cdma2000 High Rate Packet Data - Addendum I (Arlington, VA: Sept. 2007), § 3, p. 3-1 (“The AES Encryption Protocol uses the AES (a.k.a. Rijndael) procedures defined in [3GPP2 S.S0055-A] in order to encrypt the Connection Layer packets and decrypt the Authentication Protocol packets.”); § 3.5.1.1, p. 3.3-3.6 (“Constructing the Encryption Key”).

292. “Symmetric key algorithms (sometimes known as secret key algorithms) transform data in a way that is fundamentally difficult to undo without knowledge of a secret key. The key is “symmetric” because one key is used for all operations (e.g., encryption and decryption). Symmetric keys are often known by more than one entity; however, the key shall not be disclosed to entities that are not authorized access to the data protected by that algorithm and key.” NIST Special Publication 800-57, Recommendations for Key Management -- Part 1: General (Revised), p. 34.

293. Cryptanalysis: “Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection.” Id., p. 20.


factorization cryptography as apposed to the discrete logarithm cryptography used in Diffie-Hellman.\[296\] However, NIST issues the same key length “comparable strengths” recommendations for Diffie-Hellman as it does for RSA\[297\] and the required computational requirements for cryptanalysis under each cryptographic scheme are similar.\[298\] Therefore, 1024-bit encryption keys in the context of Diffie-Hellman will be uncrackable at least until the year 2017. In comparison to Diffie-Hellman, the 128-bit AES keys used in 1xEV-DO Rel. 0 offer an even less likely entry point for an attacker. Seagate Technology, LLC took a simplistic approach to a difficult cryptanalysis question and determined that it would take 70 billion computers 77,000,000,000,000,000,000,000,000 (77 trillion trillion) years to crack one 128-bit AES encryption key using computer technology and cryptanalysis techniques available in the year 2008.\[299\]

Regardless of available key strengths, 1xEV-DO Rel. 0 encryption will only protect data if it is implemented by the Access Network. At the beginning of session establishment and prior to the session key exchange process, the Access Network and Access Terminal use the Default Encryption Protocol, which provides no encryption for signals transmitted over

\[\begin{align*}

\text{297.} & \quad \text{See NIST Special Publication 800-57, Recommendations for Key Management -- Part 1: General (Revised), p. 63, “Table 2: Comparable strengths.”}

\text{298.} & \quad \text{Pornin, Thomas, “How to calculate the time it’ll take to crack RSA or DH?,” online posting, Oct. 6, 2011, \textit{diffie hellman - How to calculate the time it'll take to crack RSA or DH? - Cryptography - Stack Exchange}, http://crypto.stackexchange.com/questions/913/how-to-calculate-the-time-itll-take-to-crack-rsa-or-dh (last accessed: Apr. 9, 2012) (explaining how cracking discrete logarithm cryptographic keys has the same, or slightly greater, asymptotic complexity as cracking integer factorization cryptographic keys).}

\end{align*}\]
the air interface. The Access Network and Access Terminal will continue to use the Default Encryption Protocol until the Access Network initiates the session key exchange process. However, initiation of the session key exchange process is not required and the Default Encryption Protocol can be used during the entire session if the Access Network chooses to not use encryption. If the Access Network chooses to not initiate the session key exchange, all communications content and signaling information contained in the MAC payload will not be encrypted via the security layer. If security layer encryption is not used, “end-to-end encryption can be provided at the application layer” to protect communications content contained in higher layer protocol data units sent over Traffic Channels. However, the security layer encryption explained in this section is still the only mechanism that will protect Access Channel and Control Channel signaling information from being intercepted over the air interface. An Access Network's failure to initiate the session key exchange process will result in signaling information, such as the Access Terminal's ESN transmitted in response to a HardwareIDRequest message, being exposed to third-party eavesdroppers.

300. TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 7.9, p. 7.68 (“The Default Encryption Protocol does not alter the Security Layer packet payload (i.e., no encryption/decryption) and does not add an Encryption Protocol Header or Trailer; therefore, the Cipher-text for this protocol is equal to the Connection Layer packet.”).


302. See id., § 7.6.5.1.2, p. 7.26 (“The access network shall initiate the key exchange by sending a KeyRequest message.”).

303. If following good security practices, a wireless carrier Access Network will initiate the session key exchange process (in order to “turn on” encryption and authentication) as soon as possible, i.e., after the UATI is assigned to the Access Terminal.

304. See Korowajczuk, Designing cdma2000 Systems, p. 359 (“[E]ven though a single layer may contain multiple protocols, each of them can be individually negotiated to better accommodate network requirements and availability.”).

305. There is no logical reason why a wireless carrier would not implement the encryption procedures provided via the security layer.

306. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 7.9, p. 7.68.

307. Id.
v. Obtaining identifying information from Access Terminal hardware using the HardwareIDRequest message.

Once a session is established, the Access Network can obtain the Access Terminal's identifying information by transmitting a HardwareIDRequest message.\[308\] By transmitting a HardwareIDRequest message, the Access Network asks the Access Terminal to transmit a HardwareIDResponse message\[309\] containing its ESN or other “unique ID that has been assigned to the terminal by the manufacturer.”\[310\] Prior to receiving the HardwareIDResponse message, the Access Network identifies the Access Terminal generically via reverse link PN codes and the Access Terminal's UATI assigned by the Access Network.\[311\] The Access Terminal's HardwareIDResponse message provides its absolute identity, which can be used to determine the customer who's wireless account is associated with the Access Terminal. Although not precisely articulated in the relevant standards, the main purpose served by the HardwareIDRequest message is to provide the Access Network with an initial Access Terminal identity verification mechanism.\[312\] If the ESN or MEID contained in the HardwareIDResponse message does not belong to a device authorized for service then the wireless carrier can direct the Access Terminal away from the Access Network prior to any attempt to open a connection. By severing the air link with the unauthorized Access Terminal during the session but prior to establishing a connection, network resources are conserved.

vi. Opening a connection with the Access Network.

Once a session is established, the user of the Access Terminal can initiate the connection process with the Access Network. In the case of an aircard, the connection

\[308\] See id., § 5.3.7.1.3, p. 5.23; see also id., § 5.3.7.2.4, p. 5.31.

\[309\] See id., § 5.3.7.2.5, p. 5.31 (“The access terminal sends this message in response to the HardwareIDRequest message.”).

\[310\] Id.

\[311\] See Technical Explanations, Section II(B)(3)(c)(iii), supra (UATI used to identify the Access Terminal).

\[312\] See, e.g., Nortel Networks, PN-4875/IS-856 Ballot Comments, AT Authentication in 1xEV-DO, p. 1 (“In this comment, AT hardware authentication is added as a part of the Address Management Protocol (ADMP) in the Session Layer. This allows an operator to perform terminal authentication, based on a hardware identifier (such as the IMSI) over the common channels before the AT is assigned a traffic channel.”).
process is initiated via software installed on the host laptop computer paired with the aircard. For example, an aircard user may initiate the connection process by clicking a “connect” button on companion software bundled with the aircard. Once the user has initiated the connection process, the Access Terminal transitions into the Connection Setup Substate of the Idle State. In this substate, “the access terminal and the access network setup a connection[314] via the previously explained Access Attempt process. Using Access Probes, “[t]he access terminal sends the ConnectionRequest message to request a connection.”[315] Once the ConnectionRequest message is sent, indicating that the Access Terminal “is ready to exchange data on the access stream, the AN shall initiate PPP procedures...”[316] PPP is an acronym for “Point-to-Point Protocol” and provides a standard method for the Access Network and Access terminal to communicate.[317] “PPP also defines an extensible Link Control Protocol, which allows negotiation of an Authentication Protocol for authenticating its peer before allowing Network Layer protocols to transmit over the link.”[318] In basic terms, PPP, as used in the Connection Setup Substate, allows the Access Network to positively authenticate the Access Terminal and determine if it is authorized to access 1xEV-DO Rel. 0 service.[319] In order to accomplish this task, 1xEV-DO Rel. 0

313. See EXHIBIT 11 of 1st Consolidated Exhibits (Dkt. #587-1) (government web research on UTStarcom PC5740 aircard indicating that it is bundled with “VZAccess Manager software for easy connection management.”).
315. Id., § 6.4.6.2.2, p. 6.39.
316. ANSI/TIA-878-2 (Addenda to TIA-878), Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network, § 2.3.1.1, p. 2.2.
318. Id.
319. It was previously explained how the Access Network can identify an Access Terminal by obtaining its stored ESN via a HardwareIDRequest message. See Technical Explanations, Section II(B)(3)(e)(v), supra. However, obtaining an Access Terminal's ESN is only a preliminary identification mechanism and it is not sufficient for authenticating an Access Terminal for receiving service. Because an ESN can be copied by an attacker who has physical access to the Access Terminal, a more secure authentication mechanism using Shared Secret Data (SSD) (i.e., PPP as explained in this subsection) is employed to positively authenticate the Access Terminal prior to receiving service.
employs the Challenge-Handshake Authentication Protocol (CHAP)—an element of PPP.

CHAP is “used to periodically verify the identity of the peer using a 3-way handshake.”[321] In 1xEV-DO Rel. 0, the peer is the Access Terminal and the Access Network is the authenticator ensuring that the peer is authorized to access the cellular data network.[322] CHAP depends on the peer (i.e., the Access Terminal) and the authenticator (i.e., the Access Network) having a previously shared secret that is not transmitted or exchanged during the CHAP process.[323] In 1xEV-DO Rel. 0, the shared secret is the Shared Secret Data (SSD)[324] stored within the Access Terminal's internal storage device (NAM)[325] with an exact copy stored in a database maintained by the Access Terminal's home “Access Network-Authentication, Authorization, and Accounting” (AN-AAA) server within the wireless carrier network.[326]

Once a PPP connection is established between the Access Network and Access Terminal, “[t]he AN generates a random challenge and sends it to the AT in a CHAP Challenge message...”[327] Once the Access Terminal receives the CHAP challenge, it concatenates some of the data contained in the challenge with its stored Shared Secret Data

321. Id.
322. Although CHAP can also be used by the Access Terminal to authenticate the Access Network, this is not done in 1xEV-DO Rel. 0.
323. See id., p. 3 (“This authentication method depends upon a 'secret' known only to the authenticator and that peer. The secret is not sent over the link.”)
324. “Shared Secret Data (SSD) is a 128-bit pattern stored in the MS and readily available to the network. This Shared Secret Data is not passed across the air interface between the MS and the network...” Telecommunications Industry Association, TIA/EIA/IS-2001-A (Revision of TIA/EIA/IS-2001), Interoperability Specifications (IOS) for cdma2000 Access Network Interfaces (Arlington, VA: Aug. 2001), § 4.2.1, p. 290.
325. See TIA-683-D (Revision to TIA-683-C), Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, § 3.5.8, p. 3.141, Table 3.5.8-1 3GPP Parameter Block Types (listing “HRPD Access Authentication CHAP SS Parameters” for the Access Terminal NAM (footnote omitted)); id., § 3.5.8.14, p. 3.158 (showing the “SS” field of the “HRPD Access Authentication CHAP SS Parameters” as containing “Shared Secret Data”).
326. See fn. No. 324, supra.
327. ANSI/TIA-878-2 (Addenda to TIA-878), Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network, § 3.1.1(d), p. 3.2.
and then uses a cryptographic hashing algorithm to create a message digest\(^{328}\) (i.e., a “one-way hash”) of the result.\(^{329}\) The resulting message digest is used in the CHAP challenge response message.\(^{330}\) The “one-way hash” is essentially a unique signature taken of the concatenated data used to create the CHAP response. The Access Terminal then transmits its CHAP response message to the Access Network containing the calculated “one-way hash.”\(^{331}\) When the Access Network receives the CHAP response message, it forwards it to the AN-AAA server connected directly to the Access Network using an Access-Request message over the A12 interface.\(^{332}\) If the AN-AAA server is not the Access Terminal's home AN-AAA, it will be unable to verify the CHAP response because it will not have a stored copy of the Access Terminal's Shared Secret Data. In this case, the visited AN-AAA forwards the CHAP response to the home network AN-AAA.\(^{333}\) Once the appropriate AN-AAA receives the Access-Request message, it retrieves the Access Terminal's Shared Secret Data from its database and concatenates it with some of the data contained in the Access-Request message to create a “one-way hash” in the same fashion explained for the Access Terminal.\(^{334}\) If the “one-way hash” created by the AN-AAA matches the “one-way hash”

\(^{328}\) Cryptographic hashing algorithms and message digests are generally explained in footnotes contained in the Technical Explanations, Section II(B)(3)(c)(iv), supra (MAC payload encryption and authentication in the security layer). However, use of a hashing algorithm for authentication and integrity checks of MAC layer payloads (as explained in the Technical Explanations, Section II(B)(3)(c)(iv), supra) is different from the authentication explained in this section. Previously, it was explained how a hashing algorithm is applied to message bits contained in MAC layer payloads. In this section, a hashing algorithm is employed so that the Access Network will be able to authenticate (i.e., identify and authorize) the Access Terminal prior to providing it service.

\(^{329}\) See RFC 1994, PPP Challenge Handshake Authentication Protocol (CHAP), p. 8 (“The Response Value is the one-way hash calculated over a stream of octets consisting of the Identifier, followed by (concatenated with) the 'secret', followed by (concatenated with) the Challenge Value.”).

\(^{330}\) See id.

\(^{331}\) See id., p. 7 (“Whenever a Challenge packet is received, the peer MUST transmit a CHAP packet with the Code field set to 2 (Response).”).

\(^{332}\) See ANSI/TIA-878-2 (Addenda to TIA-878), Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network, § 3.1.1(e), p. 3.2.

\(^{333}\) See id., § 2.3.3, p. 2.3 (“If the AN-AAA does not have the authority to accept/deny the request, it forwards the request to the home network...”).

contained in the CHAP response message (created by the Access Terminal), the AN-AAA sends the Access Network an Access-Accept message.\[335\] Otherwise, the AN-AAA sends the access Network an Access-Reject message indicating that the Access Terminal is not authorized for 1xEV-DO Rel. 0 service.\[336\]

In the case of an Access-Reject message, “[t]he AN returns an indication of CHAP access authentication failure to the AT[]”\[337\] and “sends a SessionClose message to the AT to close the HRPD session.”\[338\] In the case of an Access-Accept message, “[t]he AN returns an indication of CHAP access authentication success to the AT[]”\[339\] and then begins other steps to register the Access Terminal on the network so that Internet access service can be provided by the Packet Data Serving Node (PDSN). In order to register the Access Terminal for Internet access, the Access Network establishes a connection with the Packet Control Function (PCF).\[340\] The Packet Control Function then “sends an A11-Registration Request message to the PDSN...”\[341\] “The A11-Registration Request message is validated and the PDSN accepts the connection by returning an A11-Registration Reply message with an accept indication...”\[342][343\] Once the Packet Data Serving Node accepts the connection through the registration process, the Packet Control Function notifies the

(“Whenever a Response packet is received, the authenticator compares the Response Value with its own calculation of the expected value.”)

\[335\] See ANSI/TIA-878-2 (Addenda to TIA-878), Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network, § 3.1.1(f), p. 3.2.

\[336\] See id., § 3.1.2(f), p. 3.3.

\[337\] Id., § 3.1.2(g), p. 3.3.

\[338\] Id., § 3.1.2(h), p. 3.3.

\[339\] Id., § 3.1.1(g), p. 3.2.

\[340\] See id., § 3.1.1(j), p. 3.2.

\[341\] Id., § 3.1.1(k), p. 3.2.

\[342\] Id., § 3.1.1(l), p. 3.2.

\[343\] In other words, the “registration” process in 1xEV-DO Rel. 0 occurs between the PCF and PDSN—not between the Access Terminal and Access Network. See also EXHIBIT 055 of 2nd Consolidated Exhibits (Dkt. #821-3) (diagram from ANSI/TIA-878-2 (Addenda to TIA-878) showing 1xEV-DO registration process occurring between PCF and PDSN over the A11 interface, i.e., not between the Access Terminal and Access Network).
Access Network,[344] a “PPP connection establishment procedure is performed between the AT and the PDSN...,”[345] and “the connection is established and packet data [(i.e., Internet traffic)] can flow between the AT and the PDSN.”[346] Once the connection is established, the Access Terminal transitions from the Idle State to the Connected State.[347]

d. Using the Default Route Update Protocol to scan for additional pilots, facilitate sector Route Updates, and send Route Update messages.

In addition to searching for pilots during the Pilot Acquisition Substate,[348] the Access Terminal also searches for pilots to facilitate use of the Default Route Update Protocol. “The Default Route Update Protocol provides the procedures and messages used by the access terminal and the access network to keep track of the access terminal’s approximate location and to maintain the radio link as the access terminal moves between the coverage areas of different sectors.”[349] In order to serve the goals of the Default Route Update Protocol, “[t]he access terminal shall continually search for pilots in the Connected State and whenever it is monitoring the Control Channel in the Idle State.”[350] During the searching process, “[t]he access terminal estimates the strength of the Forward Channel transmitted by each sector in its neighborhood.”[351] “The access terminal shall measure the strength of every pilot it searches.”[352] When the Access Terminal finds additional pilots transmitting in its neighborhood, it stores the pilots in sets according to signal strength.[353]
In addition to searching for pilots in its neighborhood, the Access Terminal “should also be capable of searching for pilots in frequencies and band classes other than its current frequency.”[354] In order to locate the maximum amount of available Access Networks, the Access Terminal will search all listed frequencies in its Preferred Roaming List Acquisition Table for additional pilots and it may also receive additional frequencies to search via channel records provided by the Access Network in real-time.[355] If a transmitted pilot “is on a different frequency assignment from that of the mobile station, this target frequency should be included in the search criteria.”[356]

The Access Terminal maintains the following continuously updated sets of searched pilots: (1) Active Set, (2) Candidate Set, (3) Neighbor Set, and (4) Remaining Set.[357] The Active Set is “[t]he set of pilots [] associated with the sectors currently serving the access terminal.”[358] “When a connection is open [(i.e., in the Connected State)], a sector is considered to be serving an access terminal when there is a Forward Traffic Channel, Reverse Traffic Channel and Reverse Power Control Channel assigned to the access terminal. When a connection is not open [(i.e., in the Idle State)], a sector is considered to be serving the access terminal when the access terminal is monitoring that sector’s control channel.”[359] The remaining three sets of pilots are categorized according to various rules and are maintained for conducting Route Updates where appropriate, i.e., Access Terminal handoffs[360] from one Access Network to another.

355. See, e.g., TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 6.8.6.2.2, p. 6.125 (indicating that the “NeighborChannel” parameter for the SectorParameters message consists of the “Channel record specification for the neighbor channel.”).
358. Id.
359. Id.
360. A handoff is “[t]he act of transferring communication with an access terminal from one sector to another.” Telecommunications Industry Association, TIA-866-A (Revision of TIA-866), Introduction to cdma2000 Spread Spectrum Systems (Arlington, VA: Jan. 2006), § 1.2.1, p. 1.3. In 1xEV-DO, the term “route update” is typically used in place of “handoff.”
i. Operations of the Default Route Update Protocol specific to the Idle State.

While in the Idle State, the Access Terminal maintains the Active Set of pilots on its own without receiving instructions from any Access Network.[361] “The access terminal shall initially keep an Active Set of size one when it is in the Idle State. The Active Set pilot shall be the pilot associated with the Control Channel the access terminal is currently monitoring.”[362] The Access Terminal continuously compares the pilots maintained in the four pilot sets and uses “pilot strengths to decide which sector's Control Channel it monitors.”[363] For example, if the pilot of the Access Network acquired by the Access Terminal after initial power-on has a lower signal strength compared to a newly searched pilot then the Access Terminal will stop monitoring the first Access Network sector Control Channel and it will begin monitoring the new Access Network sector Control Channel.[364]

This process is called an Idle State Route Update (i.e., idle handoff)[365] and is initiated by the Access Terminal without direct involvement from any Access Network.[366]

There are two primary types of handoffs in 1xEV-DO Rel. 0 that occur various states: the “hard handoff” and the “soft handoff.” A hard handoff is “characterized by a temporary disconnection of the Traffic Channel. Hard handoffs occur when the access terminal changes to a new CDMA frequency.” Id., § 1.2.1, p. 1.5. In contrast, a soft handoff is “a handoff occurring while the access terminal is in the Connected State of the Default Route Update Protocol. This handoff is characterized by pointing the DRC from one sector to another on the same CDMA frequency assignment.” Id., § 1.2.1, p. 1.8.

361. See TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 6.6.1, p. 6.55 (“In [][the Idle] State, the access terminal autonomously maintains the Active Set.”).

362. Id., § 6.6.1.5.1, p. 6.69.


364. While monitoring the Control Channel of the new Access Network, the Access Terminal receives and processes the new Access Network's Overhead Messages as explained in the Technical Explanations, Section II(B)(3)(c)(i), supra. As long as the new Access Network belongs to a preferred system, as listed on the Access Terminal's Preferred Roaming List System Table, the Idle State Route Update completes.

365. An idle handoff is “[t]he act of transferring reception of the Control Channel from one sector to another, when the access terminal is in the Idle State of the Default Route Update Protocol.” TIA-866-A (Revision of TIA-866), Introduction to cdma2000 Spread Spectrum Systems, § 1.2.1, p. 1.5.

366. See Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 154 (“During this search, if the mobile station detects a pilot channel signal from another base station that is sufficiently stronger than that of the current base station, the mobile station determines that an idle handoff should occur.”).
Idle State Route Updates occur under two scenarios: (1) before session establishment, and (2) after session establishment but before connection establishment. An Access Terminal conducting an Idle State Route Update prior to session establishment can seamlessly switch to any Access network, even if part of a different system \(\text{(i.e., subnet)}\), without having to send transmissions to any Access Network.\(^{367}\) However, an Access Terminal conducting an Idle State Route Update after session establishment, but before connection establishment, needs to either close the current session and open a new session with the new Access Network or the wireless carrier needs to use the A13 interface to transfer authentication and session configuration parameters similar to what is implemented for Connected State Route Updates.\(^{368}\) While in the Idle State, if a session is established or is being established, the Access Terminal sends the Access Network “RouteUpdate messages to update its location with the access network.”\(^{369}\)\(^{370}\) The Access Terminal transmits RouteUpdate messages either when “the computed value \(r\) is greater than the value provided in the RouteUpdateRadius field of the SectorParameters message transmitted by the sector in which the access terminal last sent a RouteUpdate message[.]”\(^{371}\) or “whenever it transmits on the Access Channel.”\(^{372}\)

367. An Access Terminal can initiate an autonomous Idle State Route Update prior to session establishment because the Default Session Management Protocol is in the Inactive State until the Access Probe process. “In this state there are no communications between the access terminal and the access network. The access terminal does not maintain any session-related state and the access network may be unaware of the access terminal’s existence within its coverage area when the access terminal’s Session Management Protocol is in this state.” TIA/EIA/IS-856-1, \textit{cdma2000 High Rate Packet Data Air Interface Specification}, § 5.2.6.1.4, p. 5.9.

368. \textit{See Technical Explanations}, Section II(B)(3)(d)(ii), \textit{infra}.

369. TIA/EIA/IS-856-1, \textit{cdma2000 High Rate Packet Data Air Interface Specification}, § 6.6.6.1.5.4, p. 6.70. In other words, while in the Idle State, “RouteUpdate messages from the access terminal are based on the distance between the sector where the access terminal last sent a RouteUpdate message and the sector currently in its active set.” \textit{Id.}, § 6.6.6.1.5, p. 6.69.

370. \textit{See id.}, § 6.6.6.2.1, p. 6.76 (Listing the following data fields for the RouteUpdate message: MessageID, MessageSequence, ReferencePilotPN, ReferencePilotStrength, ReferenceKeep, NumPilots, PilotPNPhase, ChannelIncluded, Channel, PilotStrength, Keep, and a Reserved field.).

371. \textit{Id.}, § 6.6.6.1.5.4, p. 6.71.

372. \textit{Id.}, § 6.6.6.1.5.4, p. 6.70.
ii. Operations of the Default Route Update Protocol specific to the Connected State.

While in the Connected State, the Access Network dictates the Access Terminal's Active Set of pilots. The access network determines the contents of the Active Set through TrafficChannelAssignment messages. These messages contain various data fields including the pilots (labeled as PilotPN field) belonging to the Access Networks the Access Terminal must access for receiving Internet access service. “If the access terminal receives a valid TrafficChannelAssignment message, it shall replace the contents of its current Active Set with the pilots specified in the message.” In other words, while a connection is established, the Access Network dictates the list of additional Access Networks the Access Terminal must choose from when conducting Route Updates (i.e., handoffs).

While in the Connected State, and unlike in the Idle State, the Access Terminal sends “RouteUpdate message[s] to the access network... to request addition or deletion of pilots from its Active Set.” The Access Terminal transmits RouteUpdate messages when there are “changes in the radio link between the access terminal and the access network, obtained through pilot strength measurements at the access terminal.” “The access network should send a TrafficChannelAssignment message to the access terminal in response to changing radio link conditions, as reported in the access terminal’s RouteUpdate messages.” “The access network should only specify a pilot in the associated sector. This means that the sector specified by the pilot is ready to receive data

373. See id., § 6.6.1, p. 6.55 (“In [[the Connected] state the access network dictates the access terminal’s Active Set.”).
374. Id., § 6.6.6.1.6, p. 6.71.
375. See id., § 6.6.6.2.2, p. 6.78 (Listing the following data fields for the TrafficChannelAssignment message: MessageID, MessageSequence, ChannelIncluded, Channel, FrameOffset, DRCLength, DRCCountGain, AckChannelGain, NumPilots, PilotPN, SofterHandoff, MACIndex, DRCCover, RABLength, RABOffset and a Reserved field.).
376. Id., § 6.6.6.1.6.3.2, p. 6.72.
377. Id., § 6.6.6.1.6.5, p. 6.73.
378. Id., § 6.6.6.1.6, p. 6.71.
379. Id., § 6.6.6.1.6.3.1, p. 6.72.
from the access terminal and is ready to transmit queued data to the access terminal should the access terminal point its DRC at that sector."[380] The process of an Access Terminal selecting a new Access Network is called a Connected State Route Update (i.e., soft and hard handoffs)[381] and requires significant collaboration between the Access Terminal, the serving Access Network, the new Access Network, and the underlying packet data network. [382]

In order to not interrupt the Access Terminal user's Internet connection during a Connected State Route Update, the wireless carrier needs to use the A13 interface to transfer authentication and session configuration parameters from the current Access Network to the new Access Network.[383] The A13 interface is a direct link between the current serving Access Network and the Access Network of which the Access Terminal is having its signal routed over the air interface.[384] The A13 interface is separate from the air interface used by the Access Network and Access Terminal to communicate via radio waves.[385] "The procedure for the A13 interface is a message flow to exchange AT and PDSN information..." [380]. Id.

381. See Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 255 ("In 1X EV-DO the soft handoff is only supported in the reverse link and it follows a procedure very similar to cdma2000. In the forward link, however, there is no soft handoff and the network transmits the data only on the best sector selected by the AT on the DRC channel.").

382. See id., p. 256 (explaining the Connected State Route Update process in the context of the air interface); ANSI/TIA-878-2, Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network (explaining the Connected State Route Update process in the context of the "underlying network," i.e., the A13 interface).

383. See id., p. 265 ("In an enhanced 1X-EV DO system; different access networks can be connected to each other with an IOS-A13 interface defined within IOS [(i.e., IS-878-2 )]. This interface is required to support mobility procedures when the AT moves from one AN to another. The A13 interface allows the transfer of authentication and session configuration parameters from the old AN to the new AN. The interface is based on the UDP/IP and uses messages defined in the IOS.").

384. See ANSI/TIA-878-2, Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network, § 3.6.1, Figure 3.6.1-1, “Inter-PCF/Intra-PDSN Dormant AN-AN HO - Successful Operation,” p. 3.15 (Connected State Route Update diagram showing the A13 interface directly linking two different Access Networks separate from the air interface).

385. See id., § 2.4.1, p. 2.4 ("The IOS application is independent of the underlying physical transport medium, which is left to the discretion of operators and manufacturers.").
between the ANs[386] involved in a Connected State Route Update (i.e., handoff). During a handoff, “[w]hen the target AN receives a packet from an AT that contains a UATI that is not in a subnet that is associated with the target AN, the target AN attempts to retrieve session related information from the source AN for the AT. The target AN sends an A13-Session Information Request message to the source AN to indicate the information requested. The target AN shall include the determined UATI, Security Layer Packet and Sector ID.”[387] “When the source AN receives an A13-Session Information Request message it checks if the session information for the requested AT exists and if it can authenticate the target AN request. After the source AN has successfully authenticated the message contained in the A13-Session Information Request message and has the requested session state information, it sends an A13-Session Information Response message to the target AN with the requested information.”[388][389] Once the target AN receives the A13-Session Information Response message, the handoff is complete when “[t]he AT and the target AN complete the establishment of the HRPD session. Depending on the state of the AT and the target AN, either an existing HRPD session may be re-established, or a new HRPD session may be initiated if required.”[390]

e. Open-loop and closed-loop power control of Access Terminal transmissions.

Regardless of implementation, all “CDMA base stations control the power of all mobiles for interference reduction purposes. All mobile signals must arrive at the base station at the same power level so that the signals can be properly coded. Power control is a required operational parameter of CDMA digital system operations.”[391] In 1xEV-DO Rel.
0, “[t]he access terminal shall provide two independent means for output power adjustment: an open-loop estimation performed by the access terminal and a closed-loop correction involving both the access terminal and the access network.”[392] “In closed-loop power control, based on the measurement of the link quality, the base station sends a power control command instructing the mobile to increase or decrease its transmission power level. In open-loop power control, the mobile adjusts its transmission power based on the received signaling power from the base station.”[393] The proceeding subsections explain the open-loop and closed-loop power control utilized by Access Terminals while sending reverse link transmissions to Access Networks.

i. Reverse Access Channel power control.

When establishing a session and opening a connection using the Access Probe process, open-loop power control is used to determine the power at which the Access Terminal transmits signals to the Access Network. As explained in Section II(B)(3)(c)(ii), supra, each Access Probe is an independent signal sent by the Access Terminal using both a pilot channel and data channel. In this context, the pilot channel and data channel make up the two part Reverse Access Channel with the pilot channel being sent first for a period of time (i.e., the preamble) followed by the pilot channel and data channel being sent together for a period of time.[394] In order to calculate the mean transmit power used for the overall Reverse Access Channel, the Access Terminal measures the mean receive power of forward link signals broadcast by the Access Network and adds the negative of the resulting value to the values contained in the OpenLoopAdjust and ProbeInitialAdjust data parameters.

394. See TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.2.1.3.2, p. 9.34, Figure 9.2.1.3.2-1, “Example of an Access Probe.”
broadcast by the Access Network via the AccessParameters message.[395][396][397] In order to determine the transmit power for each individual Access Probe sent as part of an Access sub-attempt, the Access Terminal multiplies the Access Probe number by the PowerStep value (provided to the Access Terminal via the AccessParameters message) and adds that value to the previously calculated mean transmit power used for the overall Reverse Access Channel.[398][399] During the preamble portion of any given Access Probe, the pilot channel is transmitted at the full calculated transmit power used for the Reverse Access Channel considering no data channel is transmitted.[400] During the data transmission portion of any given Access Probe, the Access Terminal uses the DataOffsetNom and DataOffset9k6 data parameter values (provided as public data of the Access Channel MAC Protocol) to determine the power at which to transmit the pilot channel and data channel.[401] When data is being transmitted, the combined transmit power of the pilot channel and data channel total the full calculated transmit power used for the Reverse Access Channel.[402] While engaging in Access Attempts as explained in Section II(B)(3)(c)(ii), supra, the Access Terminal uses the open-loop power control process explained above.

**ii. Reverse Traffic Channel power control.**

After a connection is open and a Reverse Traffic Channel assigned to the Access

---

395. See id., § 8.3.6.1.4.1.1, p. 8.25, No. 4 (providing mathematical equation).
396. The OpenLoopAdjust value sent to the Access Terminal by the Access Network contains “the nominal power to be used by access terminals in the open loop power estimate...” Id., § 8.3.6.2.6, p. 8.32.
397. The ProbeInitialAdjust value sent to the Access Terminal by the Access Network contains “the correction factor to be used by access terminals in the open loop power estimate for the initial transmission on the Access Channel...” Id.
398. See id., § 8.3.6.1.4.1.1, p. 8.25, No. 4 (providing mathematical equation).
399. The PowerStep designates “the increase in power between probes, in resolution of 0.5 dB.” Id., § 8.3.6.2.6, p. 8.32.
400. See id., § 9.2.1.3.2, p. 9.34 (“The output power of the Pilot Channel during the preamble portion of an access probe is higher than it is during the data portion of the probe by an amount such that the total output power of the preamble and data portions of the access probe are the same as shown in Figure 9.2.1.3.2-1.”).
402. See id.
Terminal by the Access Network, a combination of open-loop and closed-loop power control is used to determine the power at which the Access Terminal transmits signals to the Access Network. “When the access terminal is transmitting the Reverse Traffic Channel, the access terminal transmits the Pilot Channel, the DRC Channel, the ACK Channel when acknowledging received physical layer packets, and the Data Channel when transmitting physical layer packets. These channels shall be transmitted at power levels according to open-loop and closed-loop power control.” For the initial open-loop power estimate, “the initial mean output power of the Pilot Channel of the Reverse Traffic Channel shall be equal to the mean output power of the Pilot Channel at the end of the last Access Channel probe minus the difference in the forward link mean received signal power from the end of the last Access Channel probe to the start of the Reverse Traffic Channel transmission.” “During the transmission of the Reverse Traffic Channel, the determination of the output power needed to support the Data Channel, the DRC Channel, and the ACK Channel is an additional open-loop process performed by the access terminal.”

This process utilizes the DataOffsetNom, DataOffset9k6, DataOffset19k2, DataOffset38k4, DataOffset76k8, DataOffset153k6, DRCChannelGain, and ACKChannelGain data parameter values (provided as public data of the Reverse Traffic Channel). While communicating with the Access Network after a Reverse Traffic Channel is assigned, the Access Terminal configures its transmissions using various well known fallback data values or data values as designated by the Access Network via ConfigurationRequest messages (sent according to the Generic Configuration Protocol) containing attributes including the PowerParameters Attribute and the RateParameters Attribute (both of which contain numerous data fields and records sent to and stored by the Access Terminal). See id., § 8.5.7, p. 8.79-8.84.

See id., § 9.2.1.2.1.2, p. 9.22 (“When the access terminal is transmitting the Reverse Traffic Channel, the access terminal shall control the mean output power using a combination of closed-loop and open-loop power control...”).


Id., § 9.2.1.2.4.1, p. 9.24.

Id.

See also Etemad, cdma2000 Evolution: System Concepts and Design Principles, p. 255 (“The reverse power control is directly applied to the pilot/RRI channel only, and the power levels allocated to the DRC, ACK, and data channels are adjusted by a fixed gain relative to the pilot/RRI channel. The channel gains are defined based on the coding gain, the target reliability, and the data rate for each channel to achieve the desired performance.”).
Channel MAC Protocol) to determine the power at which to transmit the various noted channels relative to the mean output power of the pilot channel. The subsequent mean output power of the reverse link pilot channel is dictated by the Access Network through closed-loop power control. “For closed-loop correction (with respect to the open-loop estimate), the access terminal shall adjust the mean output power level of the Pilot Channel in response to each power-control bit received on the Reverse Power Control (RPC) Channel.” Whenever a connection is open, “the access network continuously transmits ‘0’ (up) or ‘1’ (down) RPC bits to the access terminal, based on measurements of the reverse link signal quality. If the received quality is above the target threshold, a ‘1’ bit is transmitted. If the received quality is below the target threshold, a ‘0’ bit is transmitted.”

Through commands sent to the Access Terminal over the air interface, the Access Network is able to increase or decrease the Access Terminal transmit power at least ±24 dB around the Access Terminal's open-loop transmit power estimate.

f. Synchronization and timing of transmitted signals.

“All sector air interface transmissions are referenced to a common system-wide timing reference that uses the Global Positioning System (GPS) time, which is traceable to and synchronous with Universal Coordinated Time (UTC).” Based on the GPS time maintained by the Access Network, the Access Terminal establishes “a time reference that is

410. Id., § 9.2.1.2.4.2, p. 9.25.
411. Id., § 9.2.1.4, p. 9.53.
413. Id., § 1.14, p. 1.17.
414. See also USDOD, Global Positioning System Standard Positioning Service Performance Standard (4th ed. 2008), Appendix C, p. C-2 (“GPS Time. A continuous time scale maintained by the GPS Control Segment which began at midnight on the night of 5/6 January 1980 on the Coordinated Universal Time (UTC) scale as established by the U.S. Naval Observatory (USNO)”; Smithsonian: National Air and Space Museum [website], How Does GPS Work?, http://www.nasm.si.edu/exhibitions/gps/work.html (last accessed: Dec. 1, 2011) (“GPS operations depend on a very accurate time reference, which is provided by atomic clocks at the U.S. Naval Observatory. Each GPS satellite has atomic clocks on board.”).
used to derive timing for the transmitted chips, symbols, slots, frames, and system timing.”[415] “The access terminal initial time reference shall be established from the acquired Pilot Channel and from the Sync message transmitted on the Control Channel.”[416] In other words, through the Pilot Channel and Sync message, the Access Network instructs the Access Terminal to transmit signals only at specific time intervals. Because the Access Terminal time reference is “used as the transmit time reference of the Reverse Traffic Channel and the Access Channel[,]”[417] the Access Network always knows the time at which the Access Terminal transmits a signal. For example, “The Access Channel Cycle specifies the time instants at which the access terminal may start an access probe.”[418] Similarly, the Access Network transmits to the Access Terminal at specified times.[419] For example, “[t]he AN sends the broadcast and common channel messages on the control channel slots in every 256 slots = 426.67 ms.”[420]

g. Relevant miscellaneous 1xEV-DO Rel. 0 cellular data network operations.

i. Signal interference.

All cellular systems, including those supporting 1xEV-DO Rel. 0, are susceptible to signal interference on the air interface. The FCC defines signal interference as “[t]he effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy.”[421] “Interference usually occurs between two radio signals whose

---

415. TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air InterfaceSpecification, § 9.2.1.6, p. 9.54.
416. Id.
417. Id.
418. Id., § 8.3.6.1.2, p. 8.22.
419. See Korowajczuk, Designing cdma2000 Systems, p. 396 (“The AN (sector) also uses the system time as a reference for all its time-critical transmission components, including pilot PN sequences, slots and Walsh functions.”).
421. 47 C.F.R. § 2.1(c).
Two common types of interference in a cellular network are cochannel interference and adjacent channel interference. “Cochannel interference occurs when there are two or more transmitters within a cellular system, or even a neighboring cellular system, that are transmitting on the same frequency (channel). This type of interference is usually generated because channel sets have been assigned to two cells that are not far enough apart; their signals are strong enough to cause interference to each other.”[423] “Adjacent channel interference is caused by the inability of a mobile phone to filter out the signals (frequencies) of adjacent channels assigned to side-by-side cell sites[].”[424] “There are other types of interference that occasionally plague cellular systems. The most common form of interference, other than cochannel and adjacent channel interference, is intermodulation interference (IM).”[425] “Intermodulation interference describes the effect of several signals mixing together to produce an unwanted signal, or even no signal at all.”[426]

In order to avoid signal interference on the air interface, wireless carriers implement frequency coordination defined as “the effort to assign frequencies to cellular channels in such a way as to minimize interference within your own cellular system and neighboring systems of different wireless carriers.”[427] Wireless carriers use both intramarket and intermarket frequency coordination. Intramarket frequency coordination is done internally by each wireless carrier and “is based on a frequency-reuse growth plan using the hex grid.”[428] “The configuration and planning of [][each cell within the hex grid] is chosen to minimize the interference from another cell and thus maximum capacity can be

---

423. Id.
424. Id., p. 45.
425. Id.
426. Id.
427. Id.
428. Id., p. 42.
Intermarket frequency coordination “is external to a wireless carrier’s cellular system, and involves coordinating frequency assignments with neighboring cellular systems[].”[430] “The FCC dictates that all reasonable actions must be taken to limit and/or reduce interference between two cellular systems.”[431] For example, the FCC requires that “[l]icensees in the Cellular Radiotelephone Service must coordinate, with the appropriate parties, channel usage at each transmitter location within 121 kilometers (75 miles) of any transmitter locations authorized to other licensees or proposed by tentative selectees or other applicants, except those with mutually exclusive applications.”[432] Additionally, the FCC has strict guidelines that must be followed by wireless carriers to prevent and correct network issues that cause interference with 800mhz Public Safety Radio Service,[433] i.e., radios used by ambulances, firefighters, police officers, etc.

ii. Hybrid Access Terminal operations for non-telephones, e.g., aircards.

As explained in Section II(B)(2)(a), supra, most Access Terminals are hybrid Access Terminals (HATs) meaning they are capable of communicating with both 1xEV-DO cellular data networks and 1xRTT cellular data/voice networks. An example of a HAT that supports all connection types across both networks (i.e., 1xEV-DO high speed Internet, 1xRTT low speed Internet, 1xRTT telephone calls, and 1xRTT SMS text messages) is a “smart phone.”[434] An example of a HAT that supports 1xEV-DO data connections and 1xRTT...

---

429. Chuah et al., Design And Performance Of 3G Wireless Networks And Wireless LANs, p. 2.
431. Id.
432. 47 C.F.R. § 22.907; see also 47 C.F.R. § 22.351 (“All applicants for, and licensees of, stations in the Public Mobile Services shall cooperate in the selection and use of channels in order to minimize interference and obtain the most efficient use of the allocated spectrum.”).
433. See 47 C.F.R. § 22.970 et seq.; 47 C.F.R. § 22.971(a) (“Any licensee who, knowingly or unknowingly, directly or indirectly, causes or contributes to causing unacceptable interference to a non-cellular part 90 [(i.e., Public Safety Radio Service)] of this chapter licensee in the 800 MHz band, as defined in § 22.970, shall be strictly accountable to abate the interference, with full cooperation and utmost diligence, in the shortest time practicable.”).
434. “Smart Phone: Wireless phones with advanced data features and often keyboards.
data connections (but not voice connections) is an aircard that plugs into a host laptop computer. In the context of an aircard, support for 1xRTT provides an SMS text message service and low speed Internet access in places where 1xEV-DO High Rate Packet Data (HRPD) service is unavailable. Hybrid Access Terminals should not be confused with SVDO Access Terminals. Hybrid Access Terminals allow for data connections via 1xEV-DO air links or a data and/or voice connection via 1xRTT air links, but not at the same time. In contrast, SVDO Access Terminals allow for simultaneous 1xEV-DO and 1xRTT air links with traffic channels assigned for each link. In the context of an SVDO Access Terminal consisting of hardware capable of supporting voice calls, if a 1xEV-DO data connection is open during the time of an incoming voice page, the Access Terminal stays in the connected state (i.e., no impact on 1xEV-DO data session) while it utilizes separate radio channels to connect the incoming voice call. In contrast, a voice capable Hybrid Access Terminal under the same scenario will drop the 1xEV-DO air link (if the user chooses to answer the call) so that resources are freed to connect the incoming voice call on the 1xRTT system.


435. See EXHIBIT 11 of 1st Consolidated Exhibits (Dkt. #587-1) (government web research on aircard).

436. SVDO Access Terminals were not being marketed in the year 2008.

437. See TIA-1157-A, Signaling Conformance Test Specification for Interworking of CDMA2000 1X and High Rate Packet Data Systems, Revision A, § 1.2, p. 1.1 (A Hybrid Access Terminal is a “[h]ybrid mode device that can support cdma20001x [(e.g., 1xRTT)] and HRPD [(e.g., 1xEV-DO)] by periodic monitoring [of] the paging channel of cdma20001x.”).

438. See id.

439. The simultaneous voice and data operation of an SVDO Access Terminal should not be confused with the “concurrent services” operation of a Hybrid Access Terminal using solely 1xRTT to concurrently access low speed Internet and a voice call.

440. See id., § 3.6, p. 3.4-3.5 (Outlining test guidelines to “verif[y] a voice call termination in active HRPD mode for SVDO capable AT.”).

441. See id., § 3.2, p. 3.1-3.2 (Outlining test guidelines to “verif[y] a voice call termination when in HRPD Active Mode.”).
The technical standard labeled IS-878-2 provides instructions on how a Hybrid Access Terminal handles incoming 1xRTT voice calls (via pages) under various scenarios while in “Active Mode,” i.e., having an open 1xEV-DO data connection.[442][443] Under a scenario applicable to “concurrent services,” if a voice capable Hybrid Access Terminal receives a 1xRTT page from a Base Station (indicating an incoming voice call) while engaged in an open 1xEV-DO data connection with an Access Network, the Access Terminal will (1) stop transmitting to the Access Network, (2) respond to the page by communicating with the Base Station over the air interface, (3) receive an “Alert with Info” message from the Base Station instructing the telephone hardware to ring, and (4) have its 1xEV-DO packet data session handed off to the 1xRTT system for concurrent call/data services (i.e., low speed Internet and voice simultaneously).[444] During the above explained process, the Base Station will establish a 1xRTT packet data session to take the place of the previous 1xEV-DO packet data session so that Internet access will be maintained while the voice call is in progress.[445] Under a similar scenario but applicable to Access Terminals with no support for “concurrent services,” the same first three steps are completed but no request will be made to handoff the 1xEV-DO packet data session to the 1xRTT network.[446] Under this variant, the Access Network starts a “Tairdrop” timer and releases the entire 1xEV-DO session if it does not receive a 1xEV-DO transmission from the Access Terminal within a period of time ranging from 0.1 to 60.0 seconds as set by the wireless carrier.[447] If the user of the Hybrid Access


443. An Access Terminal “is in Active Mode when it has a session established with an HRPD system, a PPP session established and an air-interface connection open with the HRPD system.” TIA-1157-A, Signaling Conformance Test Specification for Interworking of CDMA2000 1X and High Rate Packet Data Systems, Revision A, § 1.6, p. 1.2.

444. See ANSI/TIA-878-2, Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network, § 4.2.1, p. 4.7-4.9 & Fig. 4.2.1-1.

445. See id.

446. See id., § 4.2.2, p. 4.10-4.11 & Fig. 4.2.2-1.

447. See id., § 5.3, p. 5.10 (Showing Tairdrop timer with s default value of 5 seconds and a possible range of 0.1-60.0 seconds); § 5.3.1.1 (Tairdrop is an Access Network timer indicating
Terminal answers the ringing phone, the Access Network's timer eventually runs out and it closes the Access Terminal's PPP session established with the PDSN and its HRPD session established with the Access Network. If the call is not answered by the Access Terminal user, the Access Terminal resumes transmissions over the 1xEV-DO air link and the 1xEV-DO connection resumes.

Regardless of whether concurrent services are supported, none of the above applies to Hybrid Access Terminals that do not support voice calls (e.g., aircards). A factory set Hybrid Access Terminal lacking telephone hardware will ignore 1xRTT pages resulting from typical incoming voice calls and the 1xEV-DO data connection will not be disrupted. Under both scenarios explained above, the IS-878-2 technical standard states that “[t]he MS/AT may ignore this Page Message to continue the HRPD session. If the MS/AT ignores the message, the following steps are not performed.” Because non-telephone Hybrid Access Terminals have no reason to respond to 1xRTT pages for voice calls, let alone issue connect orders for the calls, they ignore all incoming telephone calls and never even reach the first step of ceasing transmissions to the Access Network.

C. Explanation of the term “triangulation” applicable to geolocation of radio frequency (RF) signals.

“In navigation, surveying, and civil engineering, triangulation is a technique for precise determination of a ship's or aircraft's position, and the direction of roads, tunnels, or other structures under construction. It is based on the laws of plane trigonometry, which state that, if one side and two angles of a triangle are known, the other two sides and angle can be readily calculated.” However, in the context of geolocating wireless devices via

when an HRPD connection has been lost. The timer is started by the AN when it determines that it is not receiving any transmissions from the MS/AT and stopped when the AN resumes receiving transmissions from the MS/AT or upon receipt of the A9-Disconnect-A8 message.”

448. See id., § 4.2.2, p. 4.10-4.11 & Fig. 4.2.2-1.
449. See id., § 4.2.1, p. 4.8 (a); id. § 4.2.2, p. 4.10 (a);
radio signals, the meaning of triangulation has evolved into a generically used term encompassing any number of radio signal measurements taken at two or more collection points (simultaneity is not required) where radio signals are received from a wireless device. Triangles, angles, and stationary measurement points (as are needed in traditional triangulation) are not necessary elements of radio signal triangulation. Inventors of wireless device locating technology use the term “triangulation” to generically refer to any number of geolocation measurement techniques used to locate wireless devices. For example, Bromhead et al., inventors of wireless device geolocation technology, applied the term “triangulate” in reference to using signal power levels and signal timing measurements as a way to locate a wireless device. Hildebrand et al. (Harris), inventors of wireless device geolocation technology, explained “triangulation” as using two receivers to determine radio signal angle of arrival and time difference of arrival to locate a cellular device. Dupray

451. “Geolocation of RF signals is defined as the problem of precise localization (or geolocation) of spatially separated sources emitting electromagnetic energy in the form of radio signals within a certain frequency bandwidth by observing their received signals at spatially separated sensors (or array elements) of the geolocation of RF signals system. Geolocation of RF signals is of considerable importance occurring in many fields, including radar, sonar, mobile communications, radio astronomy, seismology, unmanned air vehicle (UAV) for intelligence gathering information, emergency and rescue personnel, mining and agriculture, drilling, aviation, ground transportation, naval, etc.” Progri, Ilir, Geolocation of RF Signals: Principles and Simulations (New York, NY: Springer, 2011), p. 5.

452. See, e.g., ECPA Reform and the Revolution in Location Based Technologies and Services, 111th Cong. 2nd sess. (Jun. 24, 2010), APPENDIX, “Materials Submitted for the Hearing Record” (Written Responses of Matt Blaze), p. 138 (PDF, p. 142) (“‘Triangulation’ in this context refers to a range of techniques for more precisely locating a cellular subscriber handset by comparing the radio signal received from the handset at multiple vantage points.”).


et al., inventors of *Geographic Location Using Multiple Location Estimators*, used the term “triangulation” while explaining GPS.[456][457] Recent technical texts and papers also use “triangulation” to refer to measurements of distance, time, signal power, and signal direction. [458][459] In sum, triangulation refers to use of one or more of the following geolocation techniques: (1) time-of-flight (TOF) (a.k.a time-of-arrival), (2) time-difference-of-arrival (TDOA), (3) angle-of-arrival (AOA), and (4) power-distance.[460] Various geolocation techniques are further discussed *infra*.

For radio wave collection purposes, the traditional triangulation requirement of needing two stationary points taking measurements simultaneously can also be written out of array antenna and a pair of receiver stations to determine angle of arrival and difference in time of arrival for triangulation purposes.” (emphasis added)).


457. Pop-culture fiction novelist, Tom Clancy, also entertains his readers with a generic triangulation concept that encompasses GPS. See Preisler, Jerome, *Tom Clancy's Power Play: Zero Hour*, (New York, NY: Berkley Publishing Group, 2003) p. 239 (“Bottom-of-the-line [GPS] units lock on to three sats and provide a two-dimensional fix on position—latitude and longitude. The coordinates are arrived at by simple triangulation...the travel time of the satellite signals beamed to the receiver times the speed of light [(i.e., time-of-flight)].” (emphasis added)).

458. See, e.g., Dwivedi, Himanshu et al., *Mobile Application Security*, (McGraw-Hill (USA 2010), p. 332 (Explaining “Tower Triangulation” as using the “relative power levels of radio signals between a cell phone and a cell tower of a known location...” (emphasis added)).

459. See, e.g., The House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection and Subcommittee on Communications, Technology, and the Internet, *The Privacy Implications of Commercial Location-Based Services*, 111th Cong. (Feb. 24, 2010) (Statement by John B. Morris, Jr., General Counsel, and Director of CDT’s Internet Standards, Center for Democracy & Technology), available at http://democrats.energycommerce.house.gov/Press_111/20100224/Morris.Testimony.2010.02.24.pdf (last accessed: Apr. 9, 2012), p. 4. (“[I]f two or three cell towers can detect a mobile device at the same time, the carrier can triangulate from the towers to determine the approximate location of the phone... [and] if needed, make calculations based on the strength and direction of a phone’s signal...” (emphasis added)).

460. Other elements of geolocation involve applying received signal measurements, statistical functions, and data fusion to multiple triangulation calculations for increased accuracy; and Doppler measurements for ascertaining velocity of a wireless device. Each of these geolocation elements is further discussed *infra*.
the triangulation equation through use of the “approach” method. Instead of using multiple stationary wireless device locators, such as wireless carrier cell sites, a portable/transportable wireless device locator can use the approach method to take numerous triangulation calculations from multiple vantage points. In referencing this method, the USDOJ Electronic Surveillance Manual states that “[l]aw enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones[, and b]y shifting the location of the device, the operator can determine the phone's location more precisely using triangulation.” Through a different method using multipath signals, a stationary wireless device locator, such as a wireless carrier cell site, can autonomously triangulate the location of a wireless device. A single stationary wireless device locator can triangulate by collecting and measuring multipath signals reflected from proxy receivers such as water towers, hillsides, or other natural or man-made objects. The proxy receiver method is unique in that it allows for a single wireless device locator in a stationary position to conduct triangulation measurements on radio signals as if being done by multiple wireless device locators in stationary positions or by a single portable/transportable wireless device locator engaged in the approach method.

461. The approach method is further explain in the Technical Explanations, Section II(G) (1)(b)(v), infra.

462. U.S. Dep't of Justice, Electronic Surveillance Manual, p. 45 (emphasis added). See also EXHIBIT 052 of 2nd Consolidated Exhibits (Dkt. #821-3) (section on cell site emulators, etc., p. 40-41 and 44-45).


464. See id., p. 4 In. 56-66 (“The system uses a proxy receiver (or passive reflector) for Time of Arrival and/or Time of Difference of Arrival calculations. Throughout the description, the term proxy receiver is used for a reflector/refractor located at a location called a proxy receive site (PRS) and also used to describe any type of passive reflector, such as a building, mountain, or hill, water tower, or any other natural or man-made object that would reflect and/or refract (or diffract) the signal from a transmitting mobile unit or other radio transmitter to a receiver that could be fixed or mobile.”).
D. Cell site information and its use in geolocating wireless devices.

1. Explanation of the term “cell site information.”

Cell site information may be generated by a wireless carrier when a wireless device accesses a cell site over the air interface. The term “cell site information” is an ambiguous catch-all phrase referring to many different subsets of data generated in response to a wireless device accessing a cell site such as a 1xEV-DO Rel. 0 Access Network. The different subsets of data making up cell site information are dictated by various elements such as cellular network infrastructure, service features, wireless device type, and cell site design. In the context of historical cell site information, the subset of cell site information making up location information is not standardized across wireless carriers. “Some providers may collect only information about the nearest tower [(either with or without sector information)]... [and] how revealing that is depends on the density of the area in which the subscriber is located. Other providers, however, may collect more precise information and may collect location records at more frequent intervals, which might reveal, for example, not only a subscriber's individual locations but also his or her direction and rate of travel, travel habits, and other patterns of behavior.”

An analysis of historical cell site information provided by wireless carriers in three separate cases demonstrates the ambiguous, catch-all nature of the term. In United States v. Luis Soto, Sprint Nextel Corporation provided historical cell site information consisting of the following data fields: (1) Date; (2) Time; (3) Duration (sec); (4) FromUrbanArea NetworkCode; (5) FromACGIId; (6) Destination UFMI; and (7) Direct Connect Number. See id., Case No. 3:09-cr-00200-AWT, Doc. #112-1 (D. Conn., Jun. 28, 2010); see also EXHIBIT 110 of 2nd Consolidated Exhibits (Dkt. #821-6) (cell site information record attached). In The Matter Of An Application Of The United States Of America For An Order
Authorizing The Release Of Historical Cell-Site Information, an unknown wireless carrier provided historical cell site information consisting of the following data fields: (1) Customer PTN; (2) Date; (3) Call Initiation Time; (4) Duration (sec); (5) Type; (6) Forwarded; (7) 911; (8) International; (9) Caller / Called PTN; (10) Originating Cell Site; and (11) Terminating Cell Site. See id., Case No. 1:10-mc-00550-RRM-JO, Doc. #004-2 (E.D.N.Y., Aug. 24, 2010); see also EXHIBIT 111 of 2nd Consolidated Exhibits (Dkt. #821-6) (cell site information record attached). Finally, in the present case, Verizon Wireless provided historical cell site information consisting of the following data fields: (1) Details; (2) MDN; (3) MSID; (4) Cell Start Date/Time; (5) Event Stop Date/Time; (6) Duration (seconds); (7) MOU; (8) KBU; (9) SID; (10) Mscid; (11) Cell; (12) Switch; (13) Cell #; (14) LAT; (15) LONG; (16) ADDRESS; (17) CITY; (18) STATE; and (19) ZIP. See EXHIBIT 03 of 1st Consolidated Exhibits (Dkt. #587-1).

2. Use of statistical databases containing historical cell site location information to determine a wireless device location signature.

There are various ways to use statistical databases containing historical cell site location information to determine the past, present, and future location of a wireless device. By using information about the terrain and received signals collected over time (i.e., historical cell site location information), a wireless carrier or law enforcement can use heuristics to ascertain the location signature of a wireless device. “In one embodiment, the PDE [(i.e., Position Determination Entity)] may collect statistical data about the reported PN phases from any [[wireless device], organized within small geographic regions surrounding a [[cell site]... With a sufficient number of phase measurement samples, the PDE can make general assumptions about the multipath environment within a given region, measured by a

467. See also In Re Application For Pen Register And Trap/trace Device With Cell Site Location Authority, 396 F.Supp.2d 747, 749 (S.D.Tex. 2005) (“Smith (mj) 2005 Opinion”) (Defining real-time (i.e., prospective) cell site information as “the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls)…” and “information regarding the strength, angle, and timing of the caller’s signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture.”).
The phase measurement samples (i.e., historical cell site location information) are entered into a statistical database used to divide each cell site coverage area into regions that correspond to the available location signatures. In U.S. Patent No. 6,999,778, DiBuduo provides a diagram showing five regions surrounding a cell site with each region corresponding to a different location signature. If a wireless carrier needs to determine the region where a wireless device is located, it compares cell site location information corresponding to the target wireless device to entries in the statistical database in order to obtain a location signature match.

In another embodiment, Dupray et al. explains a system that collects historical location data to establish location signatures “based on: (a) the terrain area classifications; e.g., the terrain of an area surrounding a target MS, (b) the configuration of base stations in the radio coverage area, and (c) characterizations of the wireless signal transmission paths between a target MS location and the base stations.” Dupray et al. employs a real number confidence value system to weight specific geographic areas according to the

---


469. See id., p. 12, ln. 61-65 (“[T]his statistical database can be generated by considering any information provided to the PDE in the PPM. Over time, the PDE will compile previously reported pilot phase measurements from multiple MSs in a particular region and create the statistical distribution...”).

470. See id., p. 11, ln. 33-38 (“The statistical database compiled by the PDE can be divided into multiple regions for each BS. FIG. 10 is a diagram showing five regions surrounding BS A for which a database consisting of received PPMs from MSs located within those regions is maintained according to the present invention.”).

471. See id., Sheet 9 of 11, Fig. 10; see also EXHIBIT 057 of 2nd Consolidated Exhibits (Dkt. #821-3) (Fig. 10 attached).

472. See id., p. 17, ln. 30-31 (claiming that the invention allows for locating a wireless by “estimating a location of the MS using PN phase offsets previously reported by the MS;”).

473. Dupray, et al., TracBeam, LLC, *Geographic Location Using Multiple Location Estimators*, U.S. Patent No. 7,298,327, p. 43, ln. 41-46 (claim notes omitted); see also id., p. 15 ln. 62-67, p. 16 ln. 1 (“A novel aspect of the present invention relies on the discovery that in many areas where MS location services are desired, the wireless signal measurements obtained from communications between the target MS and the base station infrastructure are extensive enough to provide sufficiently unique or peculiar values so that the pattern of values alone may identify the location of the target MS.”).
probability of containing the target wireless device (i.e., the MS). “That is, confidence values that are larger indicate a higher likelihood that the target MS is in the corresponding MS estimated area, wherein -1 indicates that the target MS is absolutely NOT in the estimated area, 0 indicates a substantially neutral or unknown likelihood of the target MS being in the corresponding estimated area, and 1 indicates that the target MS is absolutely within the corresponding estimated area.”[474] In summary, the invention by Dupray et al., “provide[s] location hypothesis enhancing and evaluation techniques that can adjust target MS location estimates according to historical MS location data and/or adjust the confidence values of location hypotheses according to how consistent the corresponding target MS location estimate is...”[475]

3. Cell site triangulation of a wireless device using cell site location information.

There are various geolocation techniques that can be used to triangulate a wireless device using cell site location information. The most basic form of cell site triangulation uses low resolution angle-of-arrival (AOA) measurements taken from two overlapping cell site sectors belonging to adjacent cell sites:

Triangulation is the process of determining the coordinates of a point based on the known location of two other points. If the direction (but not distance) from each known point to the unknown point can be determined, then a triangle can be drawn connecting all three points. While only the length of one side of the triangle is known at first (the side connecting the two known points), simple trigonometry reveals the lengths of the other sides and so the position of the third point. In the context of cell site information, the two known points are the antenna towers, the third point is the cellular telephone, and the direction from each tower to the phone is discerned from the information about which face of each tower is facing the phone.


For the type of cell site triangulation explained above, the 120° cell site sectors[476] make up
the angles used in the angle-of-arrival (AOA) measurements. Therefore, the minimum amount of cell site location information needed for triangulation is information identifying each sector accessed by the wireless device. Angle-of-arrival (AOA) measurements in this context are considered low resolution because a sector having a radiation pattern oriented at 120° with center azimuth bearing at 60° is only capable of locating a wireless device at a vector angle centered at 60° with a line bearing uncertainty of 120°. Therefore, the line bearing pointing to the location of the wireless device is somewhere along a set 120° arc as part of a 360° circle with the cell site hardware at the center of the circle. However, because line bearings are measured from two separate cell site sectors, the level of location uncertainty is reduced to an area where the two cell site sectors overlap.[477]

More precise forms of cell site triangulation are also employed—mainly in real-time by wireless carriers seeking to “compl[y] with the FCC's 'E911' mandate for more precisely locating cellular callers to emergency services. When a subscriber places a call to 911, many cellular networks automatically employ some form of triangulation and automatically transmit the calculated location of the caller to the 911 call center.”[478] However, high resolution geolocation information may also be continuously compiled by wireless carriers for law enforcement use—even while 911 calls are not involved.[479] In order to conduct high resolution geolocation of a wireless device, wireless carriers use various network-based

II(B)(2)(c), supra (explaining cell sites in the geolocation context); EXHIBIT 22 of 1st Consolidated Exhibits (Dkt. #587-2) (cell tower range chart/map showing three tri-sectored cell sites that were accessed by the aircard).

477. EXHIBIT 22 of 1st Consolidated Exhibits (Dkt. #587-2) (cell tower range chart/map showing how triangulation via cell site sector angle-of-arrival (AOA) measurements in combination with location signature techniques eliminated 93.9% of the location uncertainty); see also General Facts, Section IV(B)(2), infra (explaining the precise techniques used to created the cell tower range chart/map).

478. ECPA Reform and the Revolution in Location Based Technologies and Services, 111th Cong. 2nd sess. (Jun. 24, 2010), APPENDIX, “Materials Submitted for the Hearing Record” (Written Responses of Matt Blaze), p. 138 (PDF, p. 142).

479. For example, TruePosition's network-based geolocation product not only serves E911 purposes, it also serves a law enforcement need for “safe shared and secure access to definitive information relating to the size, detail, location and activity of illegal conduct.” ECPA Reform and the Revolution in Location Based Technologies and Services, 111th Cong. 2nd sess. (Jun. 24, 2010) (Prepared Statement of Michael Amarosa, Senior Vice President, TruePosition, Inc.), p. 44 (PDF, p. 48).
triangulation techniques including time-of-flight (TOF), time-difference-of-arrival (TDOA),
angle-of-arrival (AOA), and power-distance. For network based geolocation, triangulation
calculations are conducted by cell sites in combination with other network hardware and may
also involve handset based measurements of cell site pilot signals as recorded by the wireless
device.\textsuperscript{480-482} According to E911 requirements, network-based geolocation
techniques will have a sufficient resolution if they are accurate to “100 meters for 67 percent
of calls, [and] 300 meters for 95 percent of calls.”\textsuperscript{483-484} However, E911 requirements
set a minimum standard and network-based geolocation techniques have the potential to be
much more accurate and intrusive. For example, TruePosition boasts that its U-TDOA
network-based geolocation product “[l]ocates mobile phones and devices in any environment
(indoors, in-vehicle, urban, suburban, rural, etc.)... with very high accuracy (typically under
50 meters)...”\textsuperscript{485} “Described discretely, TruePosition location security solutions allow for
automatic notifications based on desired criteria, such as the geographic zone of activity,
specific communications patterns or particular users.... U-TDOA technology allows for

\begin{脚注}
\footnotesize
480. See Caffery, James J., Jr. and Stüber, Gordon L., Georgia Institute of Technology,
\textit{Overview of Radiolocation in CDMA Cellular Systems}, IEEE Communications Magazine,

481. The primary technical standard addressing position determining services is the
Telecommunications Industry Association, TIA-801-A (Revision of TIA/EIA/IS-801),
2004).

482. Aside from pilot signals, wireless carriers may employ handset-based geolocation
where the wireless device uses GPS to calculate its location, which is then communicated to
the nearest cell site. “By itself, GPS can be the most accurate (when satellites are
acquired/available), but this technology is often enhanced by the network. Assisted GPS
(AGPS) refers to a PDE system that makes use of additional network equipment that is
deployed to help acquire the mobile device (much faster than non-assisted GPS) and provide
positioning when the A-GPS system is unsuccessful in acquiring any/enough satellites.”
MobileIN.com [website], \textit{Mobile Positioning}, 2001-2004,


484. In contrast, handset-based geolocation techniques are high enough resolution if they
are accurate to “50 meters for 67 percent of calls, [and] 150 meters for 95 percent of calls.”
\textit{Id}.

485. \textit{ECPA Reform and the Revolution in Location Based Technologies and Services}, 111th
43).
\end{脚注}
locating multiple devices in real time with high accuracy. The information obtained can be viewed in a map-based format, also in real time. It includes alerting capability with regard to specific geographic areas and users.”

E. Global Positioning System (GPS).

Global Positioning System (GPS) “is a space-based positioning, navigation and timing system developed by the U.S. Department of Defense (DoD). The U.S. Air Force currently finances and operates the basic system of 24+ satellites and associated ground monitoring stations located around the world. GPS is widely characterized as a satellite navigation or a satellite positioning system, providing signals for geolocation and for safe and efficient movement, measurement, and tracking of people, vehicles, and other objects anywhere from the earth’s surface to geosynchronous orbit in space. A less-known element omitted from many GPS descriptions is the embedded timing that serves an essential role in its navigation services.”\[487][488] “A GPS receiver calculates its position by timing the signals sent by the GPS satellites. Each satellite continually transmits messages containing the time the message was sent, precise orbital information (the ephemeris), and the general system health and rough orbits of all GPS satellites (the almanac). The receiver measures the transit time of each message and computes the distance to each satellite. Geometric trilateration is used to combine these distances with the location of the satellites to determine the receiver’s location.”\[489][490]

---

486. Id., p. 44 (PDF, p. 48).


488. See also USDOD, Global Positioning System Standard Positioning Service Performance Standard (4th ed. 2008), p. 1 (“GPS has provided positioning, navigation, and timing services to military and civilian users on a continuous worldwide basis since first launch in 1978. An unlimited number of users with a civil or military GPS receiver can determine accurate time and location, in any weather, day or night, anywhere in the world.”).


490. Location information is displayed to the user of the receiver as latitude and longitude.
“GPS satellites provide service to civilian and military users.”[^491] The civilian service is called the Standard Positioning Service (SPS)[^492] and the military service is called the Precise Positioning Service (PPS).[^493] “The civilian service is freely available to all users on a continuous, worldwide basis. The military service is available to U.S. and allied armed forces as well as approved Government agencies.”[^494] “Real-world data collected by the FAA show that some high-quality GPS SPS receivers currently provide better than 3 meter horizontal accuracy.”[^495] Because PPS broadcasts on two frequencies as opposed to the one frequency broadcast by SPS, “military users can perform ionospheric correction, a technique that reduces radio degradation caused by the Earth’s atmosphere. With less degradation, PPS provides better accuracy than the basic SPS.”[^496] For additional information on GPS, see Brief of Center For Democracy & Technology, Electronic Frontier Foundation, Matt Blaze, Andrew J. Blumberg, Roger L. Easton, and Norman M. Sadeh as Amici Curiae in Support of Respondent, p. 7-14, United States v. Jones, 556 U.S. ___, 181 L. Ed. 2d 911, No. 10-1259 (2012).

F. **Explanation of the term “mobile tracking device.”**

Mobile tracking devices are surveillance devices that can be attached to a person or values. See nationalatlas.gov, Latitude and Longitude, http://www.nationalatlas.gov/articles/mapping/a_latlong.html (last accessed: Aug. 30, 2011).


[^493]: “Precise Positioning Service (PPS). The GPS broadcast signals based on the L1 P(Y)-codes, L1 C/A-codes, and L2 P(Y)-codes, as defined in the GPS ISs/ICDs, providing constellation performance to authorized users, as established in the PPS Performance Standard (PPS PS), in accordance with U.S. Government (USG) policy.” Id., APPENDIX C, p. C-3.


[^496]: Id., “Is Military GPS More Accurate Than Civilian GPS.”
object sought to be tracked. A federal statute titled “Mobile tracking devices,” 18 U.S.C. § 3117, defines the broader term “tracking device” as “an electronic or mechanical device which permits the tracking of the movement of a person or object.”[497] Although the statutory definition of “tracking device” is not particularized, an analysis of the historical origins of 18 U.S.C. § 3117, enacted in 1986 as part of the Electronic Communications Privacy Act (ECPA), makes clear that legislators understood the term “tracking device” to mean a homing device “which might be placed in an automobile, on a person, or in some other item.”[498] Prior to the wide scale use of GPS, mobile tracking devices were “beepers” or “bird dogs” consisting of “a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver.”[499] The beepers of the 1980s were physically installed by law enforcement in order to track a person or object for the purpose of aiding in visual surveillance.[500] Modern day mobile tracking devices still require physical installation but the tracking is now done through use of GPS satellites. For example, the Daviscomms EaziTRAC 1000 GSM/GPRS/GPS Mobile Tracking Device uses GPS satellites to generate geolocation data that can be stored and transmitted back to law enforcement via SMS messages.[501] Likewise, numerous other modern day mobile tracking devices are of similar design and function.[502]

497. 18 U.S.C. § 3117(b).
500. See id. (beeper installed in a can of chloroform and used to track movement of car); United States v. Karo, 468 U.S. 705 (1984) (beeper installed in a can of ether and tracked into residences).
G. Air interface surveillance equipment with an emphasis on geolocation of wireless devices.

Portable/transportable wireless device locators, virtual base stations, cell site emulators/simulators, and IMSI catchers are all generic names\[503\] used for hardware based surveillance equipment targeted at wireless devices such as cell phones, tablets, aircards, and other devices that communicate via a cellular air interface standard, e.g., GSM, UMTS, 1xRTT, 1xEV-DO, etc. The surveillance devices discussed in this section operate independent from any wireless carrier network by automatically sending and/or receiving radio signals to/from target wireless devices over the air interface. Recording or “catching” IMSIs, ESNs or other identifying data; emulating base stations; locating/tracking wireless devices; conducting denial of service attacks; downloading data from wireless devices; and intercepting communications (either passively or through a man-in-the-middle attack) are all possible functions of the type of surveillance equipment addressed in this section. While specific features vary across manufacturers, surveillance equipment targeted at wireless devices can be classified into one or both of the following general categories: (1) communication interception capabilities, and/or (2) wireless device locating/tracking capabilities. Additionally, each make/model of air interface surveillance equipment is either man-portable (using handheld controls) or vehicle-transportable (using laptop controls).\[504\]

While a cursory glance shows that there are many similar types of off-the-shelf air interface surveillance equipment having geolocation capabilities, a more detailed analysis reveals that the RayFish line by Harris Corporation\[505\] is set apart from all other equipment.

---


504. In theory, either configuration would also allow for stationary operation.

505. “Harris is an international communications and information technology company serving government and commercial markets in more than 150 countries. Headquartered in Melbourne, Florida, the company has approximately $5 billion of annual revenue and more than 16,000 employees — including nearly 7,000 engineers and scientists. Harris is dedicated to developing best-in-class assured communications products, systems, and services.” Harris [website], Harris Corporation - Media Center;
sold by other companies. As an initial matter, Harris’ RayFish product line is within a class of cell site emulator capable surveillance devices—which also includes devices sold by Altron, NeoSoft, and MMI—that are specifically designed to not have integrated communications interception (i.e., man-in-the-middle attack) capabilities. In contrast, all cell site emulator capable devices sold by Ability, Meganet, Shoghi


509. MMI sells its devices through partner companies such as Elaman and Cobham. See [MMI Research Trading as Cobham Surveillance, Tactical Lawful Intercept, PDF presentation provided at ISS World Europe 2008, available at http://wikileaks.org/spyfiles/files/0/43_200906-ISS-PRG-COBHAM.pdf (last accessed: Apr. 5, 2012) (device does not intercept communications); see also EXHIBIT 024 of 2nd Consolidated Exhibits (Dkt. #821-1) (PDF attached.)]; see also [[Elaman, Active Off-Air System 3GN UMTS, Product Brochure, available at http://wikileaks.org/spyfiles/files/0/124_ELAMAN-200805-CATALOGUE-P1.zip (last accessed: May 14, 2012) [Active Off-Air System 3GN UMTS Technical Specification.pdf] (device does not intercept communications); see also EXHIBIT 025 of 2nd Consolidated Exhibits (Dkt. #821-1) (product brochure attached)]; [Elaman, GSM Vehicle Direction
Communications Ltd., Verint and View Systems have integrated communications interception capabilities in addition to wireless device locating/tracking capabilities. Regardless of whether only geolocation or geolocation with communications interception is supported, the Harris RayFish product line is entirely distinguished from all other similar products considering it offers the only cell site emulator capable air interface surveillance equipment supporting cdma2000 based air interface standards. “The Harris RayFish product line includes the StingRay II, StingRay, and KingFish systems, which are

Finder (VDF), Product Brochure, available at http://wikileaks.org/spyfiles/files/0/124_ELAMAN-200805-CATALOGUE-P1.zip (last accessed: May 14, 2012) [GSM Vehicle Direction Finder-VDF.pdf] (device does not intercept communications); see also EXHIBIT 026 of 2nd Consolidated Exhibits (Dkt. #821-1) (product brochure attached)].


compatible with the CDMA2000, GSM, and iDEN (Nextel) protocols.”[516][517][518] In contrast, all other off-the-shelf air interface surveillance equipment having geolocation through cell site emulation capabilities are limited to locating only GSM/UMTS[519] based wireless devices and lack compatibility with cdma2000 based wireless devices (i.e., devices that operate via 1xRTT, 1xEV-DO Rel. 0, etc.).[520]

1. Detailed description of the Harris RayFish line of portable/transportable wireless device locators, i.e., the StingRay, KingFish, and related equipment.

Harris has been manufacturing wireless device locators for law enforcement use since the early 1990s.[521] In February of 2009, one FBI agent testified that he alone used


517.  The Harris RayFish product line (e.g., the StingRay and KingFish) also supports the 3G GSM upgrade referred to as UMTS. See Miami, FL, USA – Legislative Files, Harris Sole Source Letter (Aug. 25, 2008), available at http://egov.ci.miami.fl.us/Legistarweb/Attachments/40003.pdf (last accessed: Mar. 9, 2011), p. 2 (“The Harris StingRay and KingFish systems are compatible with the... UMTS standard...”); see also EXHIBIT 017 of 2nd Consolidated Exhibits (Dkt. #821-1) (letter attached).

518.  Harris is also one of the few companies selling both portable and transportable air interface surveillance equipment that operate cooperatively. “The Harris StingRay and KingFish systems are the only cooperative portable/man-portable standard +12VDC powered/battery powered multiprotocol surveillance systems currently available.” Id.

519.  Although UMTS (the 3G upgrade for GSM) is based on W-CDMA, it is incompatible with the protocols used by cdma2000. See Dornan, Andy, The Essential Guide to Wireless Communications Applications, 2nd ed. (Prentice Hall, May 16, 2002) p. 113-14 (“Until mid-2000, the upgrade path for cdmaOne seemed clear. The end result was supposed to be a system named cdma2000 3XMC, so called because it combines three channels together, resulting in a wider band. Unfortunately, this system was not compatible with the form of W-CDMA favored by Europe and Japan, though its specifications are almost identical. The difference is the chip rate, the frequency at which the transceiver resonates. cdma2000’s chip rate needs to be a multiple of cdmaOne’s, while W-CDMA’s has to fit the GSM framing structure.”).

520.  Other than for equipment sold by Harris, all cell site emulator capable air interface surveillance equipment sold by the companies discussed in this section (i.e., Altron, NeoSoft, MMI, Ability, Meganet, Shoghi Communications Ltd., Verint, and View Systems) lack the ability to locate cdma2000 based wireless devices (e.g., 1xEV-DO Rel. 0 based aircards). See air interface surveillance equipment exhibits referenced in various footnotes immediately above.

such equipment more than 300 times over the last nine years and that “other agencies, U.S. Marshals, Secret Service, any different number of agencies all over the country [use the equipment] every day.” [522] Current era Harris products include the StingRay and KingFish as part of the RayFish line of wireless device locators. The StingRay [523] is a vehicle-transportable (e.g., operational from an automobile, helicopter, airplane, etc.) [524][525] wireless device locator with laptop location determining processor [526] and the KingFish [527]

(last accessed: Apr. 5, 2012) (“The team talked to me a little about the technology they had toted along in the station wagon, especially something called a cell-site simulator, which was packed in a large travel case. The simulator was a technician's device normally used for testing cell phones, but it could also be used to page Mitnick's cell phone without ringing it, as long as he had the phone turned on but not in use. The phone would then act as a transmitter that they could home in on with a Triggerfish cellular radio direction-finding system that they were using.”). The TriggerFish is a first generation wireless device locator manufactured and sold by Harris. See United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [TriggerFish registered by Harris] (registered Jan. 29, 2002), all associated documents available via search at http://tmportal.uspto.gov/external/portal/tow (last accessed Mar. 11, 2011) (documents showing that the TriggerFish “was first used in connection with the goods at least as early as November 26, 1997...”).


524. Miami, FL, USA – Legislative Files, Harris GCSD Price List (Sep. 2008) (Nov. 29, 2006), available at http://egov.ci.miami.fl.us/Legistarweb/Attachments/48000.pdf (last accessed: Mar. 9, 2011), p. 4 (price list having a StingRay accessory named “Airborne DF Kit CONUS” ($9,000), indicating that the StingRay may be used via helicopter, airplane, etc.); see also EXHIBIT 014 of 2nd Consolidated Exhibits (Dkt. #821-1) (price list attached).

525. See Durham, NC, USA - City Council Agenda No. 7503, Harris Sole Source Vendor Letter (Sept. 29, 2010) (“When interfaced with the optional Harris AmberJack DF antenna, supported mapping software, laptop PC controller, and the Harris 25-Watt power amplifier kit, the StingRay can perform vehicular-based operations.”) (emphasis added); see also EXHIBIT 015 of 2nd Consolidated Exhibits (Dkt. #821-1) (letter attached).

526. See id.

is a man-portable\textsuperscript{528} wireless device locator with handheld PDA location determining processor.\textsuperscript{529} As explained above, the Harris RayFish product line is able to conduct surveillance on wireless devices compatible with the cdma2000, GSM, UMTS and iDEN wireless network communication technologies.\textsuperscript{530} The Harris “StingRay and KingFish support 3 technologies simultaneously, additional technologies can be swapped through a hardware flash process (software provided).”\textsuperscript{531} Engineers employed by Harris explain the technology incorporated into the StingRay and KingFish as follows:

\begin{quote}
[T]he wireless device locator may include at least one antenna and a transceiver connected thereto, and a controller for cooperating with the transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among the plurality thereof. The target device may transmit a respective reply signal for each of the location finding signals.
\end{quote}


The location determining system may also include a location determining processor coupled to the receiver to collect, during movement relative to the wireless transmitter, a series of range measurements [(using propagation delays)] and a corresponding series of received signal measurements, and to estimate a location of the wireless transmitter based upon the range.

\textsuperscript{528} See Miami, FL, USA – Legislative Files, \textbf{Harris Sole Source Vendor Letter} (Nov. 29, 2006), \textit{available at} http://egov.ci.miami.fl.us/Legistarweb/Attachments/34768.pdf (last accessed: Mar. 9, 2011), p. 1 (“The \textbf{man-portability} and battery power features of the Harris KingFish product are unique for tactical mission needs, allowing the user to perform passive collection, active interrogation and active location \textbf{while on foot} (\textit{i.e., inside a multi-story building, or outside in rough terrain}).” (emphasis added)); \textit{see also EXHIBIT 016 of 2\textsuperscript{nd} Consolidated Exhibits} (Dkt. #821-1) (letter attached).

\textsuperscript{529} See Miami, FL, USA – Legislative Files, \textbf{Harris KingFish Product Datasheet}, p. 2 (“Wireless remote control from commercially available \textbf{Pocket PC}” (emphasis added)); \textit{see also EXHIBIT 007 of 2\textsuperscript{nd} Consolidated Exhibits} (Dkt. #821-1) (datasheet attached).

\textsuperscript{530} Additionally, “[s]oftware reconfigurable architecture will allow for future software upgrades to support other wireless standards and capabilities[.]” \textit{See United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay registered by Harris] (registered Sep. 9, 2003), \textbf{Harris StingRay Product Datasheet}, all associated trademark documents available via search at} http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 60-61 of 88 page compilation; \textit{see also EXHIBIT 004 of 2\textsuperscript{nd} Consolidated Exhibits} (Dkt. #821-1) (datasheet attached).

\textsuperscript{531} Maricopa County, FL, USA – \textbf{Harris Contract}, Serial No. 09041-SS (May 27, 2010), \textit{available at} http://www.maricopa.gov/materials/Awarded_Contracts/PDF/09041-c.pdf (last accessed: Mar. 9, 2011), p. 14; \textit{see also EXHIBIT 018 of 2\textsuperscript{nd} Consolidated Exhibits} (Dkt. #821-1) (contract attached).
measurements weighted using the received signal measurements.


In certain embodiments, the antenna may comprise a directional antenna. In these embodiments, the location determining processor may cooperate with the directional antenna to collect, during movement relative to the wireless transmitter, a corresponding series of angle of arrival measurements. The location determining processor may also estimate the location of the wireless transmitter further based upon the angle of arrival measurements.


Moreover, the location determining processor may cooperate with the receiver to collect, during movement relative to the wireless transmitter, a corresponding series of received signal strength measurements. The location determining processor may further estimate the location of the wireless transmitter further based upon the received signal strength measurements weighted using the received signal measurements.

*Id.*, p. 2, ln. 52-58.

A Harris wireless device locator records and stores geolocation data and then uses the video display of its location determining processor (e.g., laptop or PDA screen) to superimpose over a digital map the estimated location of the target wireless device.[532][533][534]

McPherson and Lanza further explain that Harris wireless device locators include a GPS receiver as a platform position determining system which provides the wireless device

532. See Miami, FL, USA – Legislative Files, Harris KingFish Product Datasheet, p. 2 (“Provides real-time display of Interrogation and Passive Collection results” (emphasis added)); see also EXHIBIT 007 of 2nd Consolidated Exhibits (Dkt. #821-1) (datasheet attached).


534. See Miami, FL, USA – Legislative Files, Harris Geolocation Product Datasheet, available at http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf (last accessed: Mar. 9, 2011), p. 1 (“Geolocation provides a user-friendly, geospatially accurate mapping routine which shows on-screen the exact location of the tracking vehicle, plus Direction of Arrival (DOA) information and/or estimated range/location information on the targeted phone.... Tracking missions can be stored for post-mission analysis” (emphasis added)); see also EXHIBIT 009 of 2nd Consolidated Exhibits (Dkt. #821-1) (Geolocation Product datasheet attached).
locator with a current geographical location of the platform. The GPS receiver cooperates with the location determining processor so that the target wireless device may be located with longitude, latitude, and elevation coordinates tethered to the accuracy of the GPS coordinates of the platform. When GPS signals are not available, such as when using the handheld KingFish within a building, the location determining processor may also provide for a proximity indicator involving a 3D graphic display of an arrow pointing along the azimuth and elevation angles in the direction of the target wireless device with a distance value designating the distance from the wireless device locator to the target wireless device.

Public information regarding Harris wireless device locators indicates that the Harris products allow for locating wireless devices inside buildings with precision accurate to a single room. In order to achieve such a high precision, the StingRay and KingFish wireless device locators combine numerous geolocation measurement techniques to triangulate wireless devices. The geolocation techniques employed include (1) signal time-of-flight (TOF) measurements to calculate distance (a.k.a. Range), (2) signal strength measurements to calculate distance (a.k.a. range), (3) signal angle-of-arrival (AOA)


536. The term “platform” refers to the person or vehicle transporting the wireless device locator. See *id.*, p. 3, ln. 50-54 (“The location determining system is illustratively carried by a platform movable relative to the wireless transmitter. The platform may comprise an airborne platform, for example, an aircraft, or alternatively a ground based platform, for example, an automobile.” (claim notes omitted)).

537. See *id.*, p. 6, ln. 33-41.

538. See Miami, FL, USA – Legislative Files, *Harris Sole Source Vendor Letter* (Nov. 29, 2006) (the Harris KingFish can be used “while on foot (i.e., inside a multi-story building, or outside in rough terrain.”); see also EXHIBIT 016 of 2nd Consolidated Exhibits (Dkt. #821-1) (letter attached).


540. See Lapin, Lee, *How To Get Anything On Anybody – Book 3* (Mt. Shasta, CA: Intelligence Here, Jan. 15, 2003), p. 123 (Harris products are able to “track a cellular user to an area the size of a hotel room.”).
measurements to calculate direction (via a phased array antenna), (4) frequency-of-arrival (FOA) measurements to calculate velocity, (5) weighting collected geolocation data and using statistical functions (e.g., average, mean, median, mode, etc.), and (6) data fusion of calculated geolocation measurements. Whether the StingRay or KingFish, various radio signal and data collection methods are used in order to obtain signals that are subject to the noted geolocation measurement techniques. These methods include: (1) base station surveys, (2) passive interception, (3) downloading data from wireless device internal storage, (4) transmitting interrogation signals in order to force reply signals, (5) approach method for triangulation, (6) forced transmission power increase, and (7) denial-of-service attacks. The proceeding subsections explain the above listed geolocation measurement techniques and signal/data collection methods used by the StingRay and KingFish while locating/tracking wireless devices.

a. Geolocation measurement techniques used by the StingRay and KingFish while triangulating the location of a wireless device.

i. Signal time-of-flight (TOF) measurements to calculate distance (a.k.a. range).

The StingRay uses “active... ranging techniques...” in order to locate a wireless device. The StingRay's companion Geolocation software “shows on-screen the... estimated range/location information on the targeted phone.” A Harris patent addressing wireless


542. Passive interception and denial-of-service attack via jamming are not explained because such methods are not relevant to the defendant's arguments. Note: the FBI conducted two other types of denial-of-service attacks that are discussed in the General Facts, infra.

543. See Miami, FL, USA – Legislative Files, Harris StingRay Product Datasheet, p. 1; see also EXHIBIT 003 of 2nd Consolidated Exhibits (Dkt. #821-1) (datasheet attached).

544. See Miami, FL, USA – Legislative Files, Harris Geolocation Product Datasheet, p. 1; see also EXHIBIT 009 of 2nd Consolidated Exhibits (Dkt. #821-1) (Geolocation Product datasheet attached).
device locator technology provides detailed examples of mathematical equations used in time-of-flight (TOF) measurements for conducting ranging techniques.\footnote{545} A wireless device locator employing TOF\footnote{546} will measures the propagation delay time of signals received from a target wireless device in order to find the distance between the wireless device locator and the target wireless device.\footnote{547} If the wireless device locator knows the transmission time of a signal,\footnote{548} it can subtract that time from the signal receive time to obtain the time-of-flight. Because all radio waves travel at the speed of light,\footnote{549} multiplying the time-of-flight by the speed of light gives a measurement of distance from the wireless device locator to the target wireless device.\footnote{550} Knowledge of one TOF distance


\footnote{547}{See Kim and Lee, \textit{Apparatus And Method For Tracking Location Of Mobile Station}, U.S. Patent App. No. 2003/0117320, p. 4, ¶ 15.}

\footnote{548}{As previously explained, for 1xEV-DO Rel. 0 cellular data networks, the Access Terminal (\textit{i.e.}, target wireless device) and Access Network (\textit{e.g.}, StingRay or KingFish) establish a common time reference that is used to derive timing for the transmitted chips, symbols, slots, frames, and system timing over the air interface. \textit{See Technical Explanations, Section II(B)(3)(f), supra}. Because of the common timing, the Access Network always knows the time at which the Access Terminal transmits a signal. \textit{See id}. Harris wireless device locators take advantage of the common timing reference in order to obtain a precise transmission time for CDMA based signals transmitted from a target wireless device. \textit{See McPherson and Lanza, Harris, \textit{Wireless Transmitter Location Determining System And Related Methods}, U.S. Patent No. 7,592,956, p. 4 ln. 56-59 (“T]he time of flight measurements may be generated using a time of transmission stamp within the reply signal by differencing the reply signal receipt time with the indicated time of transmission.”).}

\footnote{549}{\textit{See Technical Explanations, Section II(A), supra} (explaining electromagnetic radiation in the radio frequency band); Jandrell, Louis H. M., Pinpoint Communications, Inc., \textit{Communication system and method for determining the location of a transponder unit}, U.S. Patent No. 5,526,357 (Dallas, TX: Jun. 11, 1996), \textit{available at} http://www.freepatentsonline.com/5526357.html (last accessed: Feb. 16, 2011), p. 16, ln. 18-19 (“...radio signals travel at the speed of light, approximately 0.98357 ft. per nanosecond through air...”).}

measurement constrains the location of the target wireless device to any point along the circumference of a circle in a 2D coordinate system, or to any point on the surface of a sphere in a 3D coordinate system—with each scenario having the wireless device locator at the center.\footnote{551} If a second propagation delay can be measured from a second known location, the result is the intersection of two circles in 2D, which in turn constrains the location of the wireless device to two intersecting points, or the result is the intersection of two spheres in 3D, which in turn constrains the location of the wireless device to any point around the circumference of a circle created by the intersecting spheres.\footnote{552} Knowledge of at least three propagation delays measured from three separate known locations will resolve the ambiguity in a 2D coordinate system and constrain the location of the wireless device to one of the two previously discussed intersecting points.\footnote{553} Knowledge of at least four propagation delays measured from four separate known locations will resolve the ambiguity in a 3D coordinate system and constrain the location of the target wireless device to a single point along the circumference of the previously discussed circle.\footnote{554}

\section*{ii. Signal strength measurements to calculate distance (a.k.a. range).}

The StingRay “[i]nterfaces with AmberJack antenna to form a complete target tracking and location solution using active... ranging techniques...”\footnote{555} The AmberJack


\footnote{553}{See references cited in fn. No. 553, \textit{supra}.

\footnote{554}{See references cited in fn. No. 552, \textit{supra}.

\footnote{555}{See Miami, FL, USA – Legislative Files, \textit{Harris StingRay Product Datasheet}, p. 1; \textit{see also EXHIBIT 003 of 2\textsuperscript{nd} Consolidated Exhibits} (Dkt. #821-1) (datasheet attached).}
phased array beam-forming antenna “[d]etermines... received signal strength of a targeted mobile phone's transmission.”[556] Similarly, the KingFish “[d]ynamically updates received signal strength to enable precise location of a target phone.”[557] A Harris patent addressing wireless device locator technology provides detailed examples of mathematical equations used in power-distance measurements for conducting ranging techniques.[558] A wireless device locator having a power-distance detector will measure the difference between the signal receive power and the signal transmit power in order to determine the distance between the wireless device locator and the target wireless device that transmitted the signal.[559] If the wireless device locator knows the transmit power of the signal,[560] it can subtract that value from the signal receive power to obtain the loss power value.[561]

Because the intensity of radio wave propagation in free space is inversely proportional to the square of the distance traveled,[562] knowledge of the loss power value constrains the location of the target wireless device to any point around the circumference of a circle in a 2D coordinate system, or to any point on the surface of a sphere in a 3D coordinate system—

---

556. Miami, FL, USA – Legislative Files, Harris AmberJack Product Datasheet, p. 6-7; see also EXHIBIT 011 of 2nd Consolidated Exhibits (Dkt. #821-1) (datasheet attached).

557. Miami, FL, USA – Legislative Files, Harris KingFish Product Datasheet, p. 2; see also EXHIBIT 007 of 2nd Consolidated Exhibits (Dkt. #821-1) (datasheet attached).

558. See McPherson and Lanza, Harris, Wireless Transmitter Location Determining System And Related Methods, U.S. Patent No. 7,592,956, p. 9 et seq. (“Received Signal Strength Indication Based Approach”).


560. “[F]or signal-strength-based [geolocation measurement] systems it is necessary that the transmit power of the MSs be known and controlled with reasonable accuracy.” Caffery and Stüber, Overview of Radiolocation in CDMA Cellular Systems, IEEE Communications Magazine, 0163-6804/98/, p. 39. As previously explained, for 1xEV-DO Rel. 0 cellular data networks, the Access Network (e.g., StingRay or KingFish) controls the transmit power of the Access Terminal (i.e., target wireless device) by sending it commands called Reverse Power Control (RPC) Bits. See Technical Explanations, Section II(B)(3)(e)(ii), supra. Therefore, the StingRay and KingFish while operating in cell site emulator mode have the ability to know and control the transmit power of a target wireless device.


562. See id.
with each scenario having the wireless device locator at the center.\[563]\] The process for resolving 2D and 3D location ambiguity for a target wireless device while using power-distance measurements is identical to what is used in TOF involving the intersection of multiple circles or spheres.\[564]\] In U.S. Patent No. 7,592,956, McPherson et al. of Harris provides a diagram showing three power-distance circles (only two are drawn) plotted on a 2D map intersecting where the target wireless device is located.\[565]\] However, as indicated by the mathematical equations taught by McPherson et al., the power-distance geolocation measurement technique is typically used to locate wireless devices in a 3D coordinate system, \textit{i.e.}, the inclusion of altitude.\[566]\]

\textbf{iii. Signal angle-of-arrival (AOA) measurements to calculate direction (via a phased array antenna).}

Measurements of signal angle-of-arrival (AOA) are used to obtain a 3D directional fix (azimuth angle and elevation angle) on a target wireless device having an unknown location relative to the wireless device locator.\[567]\] The azimuth angle points in the direction of the wireless device along the horizontal plane and the elevation angle points in the direction of the wireless device along the vertical plane.\[568]\] “There are a myriad of methods for determining the angle of arrival of a signal at a receiving site, such as by: the use of a rotating antenna which is rotated to obtain the strongest signal from the target unit; a phase array of antenna elements which may be variably electrically steered to obtain the strongest


\[564\] See \textit{Technical Explanations}, Section II(G)(a)(i), \textit{supra} (explaining TOF geolocation measurements used by the StingRay and KingFish to locate wireless devices).

\[565\] See McPherson and Lanza, Harris, \textit{Wireless Transmitter Location Determining System And Related Methods}, U.S. Patent No. 7,592,956, Figure No. 10.

\[566\] See \textit{id.}, p. 9, ln. 38-67; p. 10, ln. 1-67.


signal; plural antennas at which the receiving unit may compare the instantaneous phase of the arriving signal at each of the plural antennas to determine the direction of a signal...; or other conventional methods. “[569] The most advanced direction finding antenna is the phased array beam-forming antenna. “[570] “An array antenna is a special arrangement of basic antenna components.” “[571] “In an array propagating a given amount of energy, more radiation takes place in certain directions than in others. The elements in the array can be altered in such a way that they change the pattern and distribute it more uniformly in all directions.... On the other hand, the elements could be arranged so that the radiation would be focused in a single direction.” “[572] Changing the directivity of a phased array antenna involves altering the phase of the antenna elements so that the various propagated radio waves either reinforce or cancel one another in controlled directions. “[573] The controlled directivity of a phased array antenna is the same for receiving signals as for transmitting signals. “[574][575]


570. “The signals induced on different elements of an array in space are combined to form a single output (beam) of the array. This process of combining the signals from different elements is known as beam forming. The direction at which the array has maximum response (array has maximum gain) is said to be the beam pointing direction or look direction.” Akhter, Mohammad S., Signal Processing for MC-CDMA, Master of Engineering (by Research) Dissertation, The University of South Australia (Mar. 1998), p. 70.


572. Id., p.4.32 (PDF, p. 198).

573. “Various reflected and refracted components of the propagated wave create effects of reinforcement and cancellation. At certain distant points from the transmitter, some of the wave components meet in space. Reception at these points is either impaired or improved. If the different components arrive at a given point in the same phase, they add, making a stronger signal available. If they arrive out of phase, they cancel, reducing the signal strength.” Id., p. 4.30, (PDF, p. 196).

574. See id., p. 4.11 (PDF, p. 177) (“When a transmitting antenna with a certain gain is used as a receiving antenna, it will also have the same gain for receiving.”).

575. When determining a line bearing via received signals, “[t]he angle of arrival of the response signal may be determined by evaluating the phase of the response signal simultaneously at each of the antennas. The simultaneous phase relationships at the antennas, the geometric relationship of the antennas and the frequency of the response signal can be used to estimate the angle of arrival of the response signal with respect to the
Harris wireless device locators are used with the AmberJack phased array antenna with beam-forming technology. “AmberJack is a phased array direction-finding (DF) antenna system capable of tracking and locating mobile phone users and base stations.”

“AmberJack combines Harris' expertise in phased array antenna technology and tracking and locating systems to offer a state-of-the-art direction finding system. Beam forming technology offers a universal DF antenna for existing as well as future cellular standards.”

The AmberJack is specifically designed to operate with the StingRay and allows it to determine “direction of arrival and received signal strength of a targeted mobile phone's transmissions.” “Harris' unique adaptive array processing techniques provide for automatic signal optimizing, interference suppression, and custom beam shaping.”

For adaptive antenna arrays, “the gain and phase of individual antennas are changed before combining to adjust the overall gain of the array in a dynamic fashion as required by the system [(i.e., electronically changing the direction of the beam in real-time)].” Harris' phased array antennas are backed by 20+ years of experience with capabilities that “combine two separate processes, classical antenna array design and antenna array signal processing, to antennas.”


577. Id.


579. Miami, FL, USA – Legislative Files, Harris AmberJack Product Datasheet, p. 6-7; see also EXHIBIT 011 of 2nd Consolidated Exhibits (Dkt. #821-1) (AmberJack datasheet attached).


significantly improve signal-to-noise, geolocation accuracy and Angle of Arrival estimates.”[582]

iv. Weighting collected geolocation data and using statistical functions (e.g., average, mean, median, mode, etc.).

In order to more precisely determine the location of a target wireless device, the wireless device locator will use received signal measurements to weight received signals corresponding to any given measurement family (e.g., TOF, power-distance, AOA, etc.). Received signal measurements may consist of bit-error rate measurements, received signal strength measurements, receiver metrics, and signal-to-noise ratio measurements.[583] When the received signal measurements indicate a high quality received signal, such as when the signal-to-noise ratio value is larger, the wireless device locator interprets the other associated signal measurements (used to determine the location of the target wireless device) to be of higher quality and weights those measurements more heavily while producing the location estimate.[584] The wireless device locator may also use statistical functions (e.g., mean, median, mode, etc.) on a group of geolocation measurements within a set of measurements corresponding to any given measurement family in order to more precisely determine the location of a target wireless device.[585] Both weighting and averaging depend on a multitude of geolocation measurements, preferably taken from different locations in order to increase the variety of the relevant signals.[586]

v. Data fusion of calculated geolocation measurements.

In order to more precisely determine the location of a target wireless device, the

582. Harris, Government Communications Systems Division, Phased Array Antennas Brochure; see also EXHIBIT 012 of 2nd Consolidated Exhibits (Dkt. #821-1) (Phased Array Antennas Brochure attached).


584. See id., p. 5, ln. 64-67; p. 6, ln. 1-7.


wireless device locator will use data fusion by combining and simultaneously using the various collected geolocation measurements spanning multiple measurement families (e.g., TOF, power-distance, AOA, etc.). By using data fusion, different families of measurements, and even measurements within families, can be combined in a weighted sense to arrive at an optimized target wireless device location estimate. Using data fusion across multiple measurement families increases the precision of locating a wireless device considering suspected measurement errors within any given measurement family can be given less weight or even eliminated completely. For example, the propagation delay used to determine distance in a TOF measurement may be imprecise due to measurements taken on multipath signals having a longer propagation delay when compared to direct path signals. The noted measurement errors may be eliminated by fusing power-distance geolocation data with TOF geolocation data. Data fusion may also be used to fill measurement voids that may be present within any given measurement family. For example, the TOF geolocation measurement technique requires at least three separate measurements in order to confine the location of a target wireless device to a single point in a 2D coordinate system. This limitation may be eliminated by fusing AOA measurements with an inadequate number of TOF measurements in order to achieve the same precision that would otherwise be achieved using an adequate number of TOF measurements. Just like weighting and averaging within signal measurement families, data fusion depends on a multitude of geolocation measurements preferably taken from different locations in order to increase the variety of the relevant signals.

587. See id., p. 13, ln. 50-59.
589. See id.
591. See Technical Explanations, Section II(G)(1)(a)(i), supra (explaining TOF geolocation measurements used by the StingRay and KingFish to locate wireless devices).
593. See McPherson and Lanza, Harris, Wireless Transmitter Location Determining System
b. Radio signal and data collection methods used by the StingRay and KingFish while triangulating the location of a wireless device.

i. Base station surveys.

Among other surveillance capabilities, the StingRay “performs network base station surveys...”[594] in any given network coverage area. Similarly, the KingFish “[i]dentifies active CDMA channels and catalogs base station parameters[.]”[595] Harris wireless device locators are used with the AmberJack phased array antenna, which “[d]etermines... received signal strength of a targeted base station's transmission[.]”[596] The Allums court opinion, published as United States v. Allums, No. 2:08-CR-30 TS, 2009 WL 806748 (D.Utah 2009), paraphrases sworn testimony given by FBI Agent William Shute on the StingRay's base station survey capabilities:

Shute testified that he identified the originating cell tower for each of the calls in question. Shute testified that he purchased a cell phone from the same service provider as the Defendant and placed the phone into 'engineering mode,' where the phone display showed the cell tower to which it was currently connected. Using that phone and another device called a Stingray, which also tracked which cell tower was the strongest at any geographical position, Shute drove for some time around the neighborhoods surrounding the cell towers in question and determined an approximate range for each cell tower. Specifically, Shute testified that he was able to determine the approximate distance from the originating cell tower where the cell phone and Stingray switched from the originating cell tower to another cell tower. Shute testified that this method allows him to determine, with a reasonable degree of certainty, a fairly narrow geographical location where an individual is located while a cell call is being placed.

Id. at 1.

ii. Cell site emulation and forced connection handoff.

The datasheet for the StingRay states that it “emulates base station to collect MINs...”
Lee Lapin, former government surveillance advisor, also indicated in his book that various Harris wireless device locators emulate base stations and force wireless devices to connect to the government's emulated cellular networks. Lapin explained cell site emulation as “[emulat[ing] Base Station Control Channel to 'capture' mobile phones in close proximity[.].” Documents from the Executive Office for United States Attorneys indicate that a cell site emulator “is a mobile device that can electronically force a cell phone to register its telephone number (MIN), electronic serial number (ESN), and information about its location, when the phone is turned on. This can be done without the user knowing about it, and without involving the cell phone provider.” While operating in cell site emulator mode, the wireless device locator will appear to all compatible wireless devices within signal range as an actual and legitimate cell site indistinguishable from cell sites operated by the wireless carrier. If configured for cdma2000 technologies, the wireless device locator will broadcast a high powered pilot signal, which will force the target wireless device to disconnect from its legitimate serving cell site and connect to the emulated cell site. Once forced to connect to the emulated cell site, the wireless device locator seizes control of the wireless device allowing for interrogation, downloading of stored data, denial-of-service attacks, and other supported operations.

The Harris RayFish line of wireless device locators can emulate cell sites...
across a wide range of mobile network protocols. As previously explained, the RayFish line is compatible with cdma2000, GSM, UMTS, and iDEN protocols with a maximum of three mobile network software packages loaded at any given time. In order to emulate a cell site under any given protocol, the StingRay and KingFish must follow the procedures set forth in the relevant communications standards set by international standards setting bodies.

iii. Downloading data from wireless device internal storage.

The StingRay “supports targeting and real-time searching of mobile identification numbers (MIN), dialed numbers, and electronic serial numbers (ESN)[.]” Similarly, the KingFish “provides investigators with a tool that extracts the telephone number (MIN) and Electronic Serial Number (ESN) from a CDMA mobile telephone.” Harris trademark documents for “StingRay” and “KingFish” also indicate that the devices are used for “gathering information from cellular telephones...” The process of searching for and extracting data from a target wireless device, as supported by the StingRay and KingFish, begins after the wireless device is forced to connect to the emulated cellular network being broadcast. For example, if operating as a 1xEV-DO Rel. 0 cell site, the wireless device locator will establish a session with the target wireless device in order to transmit signals...
containing a HardwareIDRequest message allowing the wireless device locator to download the ESN stored within the target wireless device.\[609\] By downloading identifying information from each wireless device that connects to the cell site emulator, the wireless device locator determines which wireless device is the target wireless device sought to be located and which wireless devices are to be ignore.

iv. Transmitting interrogation signals in order to force reply signals.

The StingRay datasheet contains a heading reading “Transmit Capabilities” with “For Interrogation and Active Tracking and Location” under the heading.\[610\] Similarly, the KingFish datasheet is titled “Portable CDMA Interrogation... System[.]”\[611\] The term “interrogation” in the geolocation context is adapted from radar terminology.\[612\] “The process by which a radar transmits a signal suitable for triggering the beacon is known as interrogation; the corresponding beacon transmission is termed the reply. Radar beacons which reply to interrogations are called transponders and the radar set used to interrogate a beacon is called an interrogator.”\[613\] A Harris patent addressing wireless device locator technology explains that interrogation in the geolocation context involves “prompt[ing] the target wireless communications device to send reply signals using the location finding signals, rather than passively waiting until the target device begins transmitting. This allows for quicker and more efficient device location.”\[614\] Another relevant Harris patent explains
that a location finding signal “may comprise a signal that would routinely prompt a
transmission reply from the wireless transmitter under the applicable communications
standard. Once the wireless transmitter receives the signal from the location determining
system, the wireless transmitter transmits a reply signal that is received by the platform.”[615]
In order to force a target wireless device to generate an abundance of response signals during
interrogation, the wireless device locator will exploit elements of the applicable mobile
communications protocol being used by the target wireless device.[616] For example, if
emulating a 1xEV-DO Rel. 0 cellular data network, the wireless device locator may force the
target wireless device to transmit an abundance of ACK signals that would go unnoticed by
the wireless device user.


The StingRay utilizes “active approach” in order to triangulate the location of a target
wireless device.[617] A relevant Harris patent explains that a wireless device locator engaged
in “approach” is fixed to a portable/transportable platform (e.g., airplane, automobile,
person, etc.) so that it may collect geolocation measurements during movement relative to
the wireless device being located,[618] i.e., while it “approaches” the wireless device. “As
the platform moves relative to the wireless transmitter, the accuracy of the location estimate
improves if the trajectory of the platform: breaks symmetry with regards to the wireless

The Harris patent also references U.S. Patent No. 5,706,010 (bridging the technology
reference gap between radar and geolocation for wireless devices).

615. See McPherson and Lanza, Harris, Wireless Transmitter Location Determining System

616. See Billhartz, et al., Harris, Wireless Communications System Including A Wireless
Device Locator And Related Methods, U.S. Patent No. 7,321,777, p. 6, ln. 29-36 (“By way
of example, the location finding signal may include the UID of the target device in a header
packet and a valid but empty data packet. This will force the target device to generate a
reply signal acknowledging receipt of the location finding signal (i.e., an ACK signal). Of
course, various other location finding signals could be used to cause the target terminal to
generate the ACK signal, as will be appreciated by those skilled in the art.”) (claim note
omitted).

617. See Miami, FL, USA – Legislative Files, Harris StingRay Product Datasheet, p. 1; see also
EXHIBIT 003 of 2nd Consolidated Exhibits (Dkt. #821-1) (datasheet attached).

618. See McPherson and Lanza, Harris, Wireless Transmitter Location Determining System
transmitter, reduces ambiguity resolution, and minimizes geometric dilution of precision
(GDOP).” The Harris patent further explains that “it may be preferable to encircle the
approximate location of the wireless transmitter to provide more accurate results, i.e.,
breaking the symmetry.” In referencing this method, the USDOJ Electronic Surveillance
Manual states that “[l]aw enforcement possesses electronic devices that allow agents to
determine the location of certain cellular phones[, and b]y shifting the location of the device,
the operator can determine the phone’s location more precisely using triangulation.” The
approach method is the primary benefit of using a portable/transportable wireless device
locator, as apposed to a stationary wireless device locator (e.g., a cell site with location
finding hardware and software), because it allows for many geolocation measurements to be
taken from different locations within a short time period. For example, if being transported
in an automobile while in cell site emulator mode, a wireless device locator may take a
geolocation measurement from a different location once every three seconds. Therefore,
if the wireless device locator is transported within the area of the target wireless device over
the course of 30 minutes, it would be the equivalent of having 600 wireless carrier cell sites
working together to triangulate the location of the target wireless device.

vi. Forced transmission power increase.

Increasing the signal transmission power of a target wireless device is standard
functionality for all wireless device locators. The Wiki for the OsmocomBB based “IMSI
Catcher Catcher” software—designed to detect and defeat wireless device locators such as

619. *Id.*, p. 6 In. 13-17 (claim note omitted).
620. *Id.*, p. 6 In. 50-53 (claim note omitted). In providing further explanation, McPherson
*et al.* also makes reference to Figure No. 8, attached to the cited patent, showing a wireless
device locator aboard an airplane taking three different range bearing measurements from
three different positions in order to triangulate the location of a cellular phone. *See also
EXHIBIT 52 of 1st Consolidated Exhibits* (Dkt. #587-1) (Figure No. 8, attached).
621. U.S. Dep’t of Justice, *Electronic Surveillance Manual*, p. 45 (emphasis added). *See also
EXHIBIT 052 of 2nd Consolidated Exhibits* (Dkt. #821-3) (section on cell site emulators,
*etc.*, p. 40-41 and 44-45).
622. *See Billhartz, et al., Harris, Wireless Communications System Including A Wireless
Device Locator And Related Methods*, U.S. Patent No. 7,321,777, p. 8, In. 63-64
(“Preferably, the location finding signals are transmitted over a relatively short interval (a
few seconds or less)...”).
the StingRay and KingFish—lists “[y]our phone sends at the highest possible power” as one of the StingRay/KingFish detection mechanisms. The process of instructing a target wireless device to transmit at the highest possible power, as supported by the StingRay and KingFish, is done after the wireless device is forced to connect to an emulated cellular network. Once the target wireless device is connected to the emulated cellular network, the wireless device locator employs closed-loop power control while transmitting signals instructing the target wireless device to transmit at the highest possible power. For example, if locating a 1xEV-DO Rel. 0 wireless device, the wireless device locator will transmit Reverse Power Control (RPC) bits, with a value of “1,” to the target wireless device until it is transmitting at the highest possible power. By increasing the transmit power of the target wireless device, the wireless device locator is able to collect higher quality signals sent in response to the location finding interrogation signals. By collecting higher quality response signals, geolocation measurements become more accurate and the precision of the location estimate increases.

H. The FBI Digital Collection Program.

The FBI Digital Collection Program provides agents “with the means to collect evidence and intelligence through the acquisition, deployment, and support of communications interception techniques and systems which facilitate and support national security, domestic counterterrorism, and criminal investigative efforts.” In more detail:


624. See Technical Explanations, Section II(G)(1)(b)(ii), supra.

625. “[I]n CDMA cellular systems the MSs are power controlled to combat the near-far effect. Time-division multiple access (TDMA) cellular systems use power control to conserve battery power in the Mss.” See Caffery and Stüber, Overview of Radiolocation in CDMA Cellular Systems, IEEE Communications Magazine, 0163-6804/98/, p. 39.

626. See Technical Explanations, Section II(B)(3)(e)(ii), supra (explaining 1xEV-DO Rel. 0 closed-loop power control on the Reverse Traffic Channel).

627. See Technical Explanations, Section II(B)(3)(e)(ii).

628. See id., Section II(G)(1)(b)(iv), supra (explaining interrogation used by the StingRay and KingFish to locate wireless devices).

629. See FBI Dec. 17, 2007, Response to EFF FOIA Request Nos. 1056287-000 &...
practical terms, the FBI Digital Collection Program provides agents of the FBI a means to:

1. collect communications content, 2. collect signaling information (i.e., Pen/Trap data)

[630] relating to transmitted communications, and 3. geolocate wireless devices such as cell phones and aircards. The Digital Collection Program is comprised of numerous elements including: (1) computer hardware and software, (2) surveillance equipment, (3) a specialized network used for intercepting data directly from telecommunications providers, (4) technical standards, (5) data collection and delivery points, (6) designated personnel responsible for administering and operating the program, and (7) FBI policy dictating operations of the program. The proceeding subsections provide a brief explanation of various elements making up the FBI Digital Collection Program, as explained in FBI documents.


In order to receive data collected through the Digital Collection Program, agents use specialized computers, referred to as Digital Collection Systems, comprised primarily of commercial-off-the-shelf hardware and software with limited proprietary application software.[631] The FBI began development of Digital Collection Systems in late 1996.[632] These systems intercept multi-source digital (and analog) communications information for intelligence gathering applicable to foreign counterintelligence activities and for investigative purposes for providing evidence at criminal trials.[633] The electronic


630. The term “Pen/Trap data” is shorthand for any data that may be obtained via a pen register and/or trap and trace device as defined in 18 U.S.C. §§ 3127(3) (pen registers) and 3127(4) (trap and trace devices).

631. See id.


633. See FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 33 of 150; see also EXHIBIT 046 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of
information collected includes Pen/Trap data (i.e., call-identifying information), analog and digital call content, facsimile transmissions, modem transmissions, microphone audio,\footnote{634} real-time cell site location information,\footnote{635} and other real-time geolocation information. Digital Collection Systems process and evaluate the collected electronic information “for migration to a separate information technology system where the collected data is analyzed, managed and archived as case related information. Processing of information collected through digital collection systems involves monitoring information, recording it onto digital media, and playback/transcription into a readable document.”\footnote{636} “Digital Collection Systems are used primarily by FBI field offices and Resident Agencies in support of active foreign intelligence and criminal cases. Support is also provided to other federal, state, local and tribal agencies, as required.”\footnote{637}

2. DCSNET.

The Digital Collection Systems Network (DCSNET)\footnote{638} is the communications medium used by the FBI Digital Collection Systems.\footnote{639} DCSNET is a peerless and private

\footnote{634} See id.

\footnote{635} See EXHIBIT 06 of 1st Consolidated Exhibits (Dkt. #587-1) (LAESP messages containing real-time cell site sector location information).


\footnote{637} See FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 33 of 150; see also EXHIBIT 046 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

\footnote{638} See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 56 of 125; see also EXHIBIT 039 of 2nd Consolidated Exhibits (Dkt. #821-5) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

\footnote{639} See FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 33 of 150; see also EXHIBIT 046 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).
encrypted IP network layered over the FBI Trilogy network backbone—an enterprise wide area digital communications network deployed to link all FBI field offices and resident agencies. DCSNET supports the transport and delivery of CALEA based call-identifying information and call content from Telecommunications Service Providers to Digital Collection Systems located at Central Monitoring Plants within FBI offices. The FBI is in a continual relationship with all major Telecommunications Service Providers to allow them limited access to DCSNET for the purpose of providing the FBI with call-identifying information and call content.


See FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 33 of 150; see also EXHIBIT 046 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 3 of 6], p. 32-33 of 90; see also EXHIBIT 042 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 20071022_dcs03.pdf attached with page numbers added).

See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 105 of 129; see also EXHIBIT 048 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).


See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 56 of 125; see also EXHIBIT 039 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

See FBI Jul. 2, 2007, Response to EFF FOIA Request [EFF PDF Set 8 of 8], p. 90; see also EXHIBIT 037 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 070207_dcs08.pdf attached with page numbers added).


See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 38 of 125; see also EXHIBIT 039 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).
associated with the communications of intercept targets. Telecommunications Service Providers deliver this information via Call Data Channels (CDCs) and Call Content Channels (CCCs) logically linked to FBI DCSNET gateways from Intercept Access Points (IAPs) located within telecommunications network infrastructure. Once CDC and CCC information is received at a DCSNET gateway, equipment maintained by FBI staff at the Engineering Research Facility (ERF) Operational Technology Division (OTD) Telecommunications Intercept and Collection Technology Unit (TICTU) Switch-Based Intercept Team (SBIT) distributes the data in real-time to network switches located at Central Monitoring Plants at the appropriate FBI field offices where the data is collected per court orders and/or warrants.

649. See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 105 of 129; see also EXHIBIT 048 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

650. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 60-62 of 74; see also EXHIBIT 041 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).


652. See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 105 of 129; see also EXHIBIT 048 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

653. An Intercept Access Point is “a point within a telecommunication system where some of the communications or call-identifying information of an intercept subject's equipment, facilities and services are accessed.” TIA/EIA/J-STD-025A, Lawfully Authorized Electronic Surveillance, § 3, p. 9. An Intercept Access Point typically consists of a telecommunications network switch. See id., “Annex A,” § A.1, p. 82. The switch is connected to a Packet Assembler-Disassembler (PAD) which is in turn connected to a modem with a direct link to a DCSNET gateway. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 58-59 of 74; see also EXHIBIT 041 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

654. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 3 of 6], p. 33 of 90 (“The DCSNET is monitored and maintained by staff from the Operational Technology Division's (OTD) Telecommunications Intercept and Collection Technology Unit (TICTU)...”); see also EXHIBIT 042 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 20071022_dcs03.pdf attached with page numbers added).

655. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 51 of 74 (“The TICTU's Switch-Based Intercept Team is responsible for distributing this data to the appropriate field offices where it is collected per court orders... [T]his data is delivered real-time...”); see also EXHIBIT 041 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

656. See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 38

Certain hardware and software elements of the FBI’s Digital Collection Program follow the technical specifications outlined in the Telecommunications Industry Association technical standard: TIA/EIA/J-STD-025A, Lawfully Authorized Electronic Surveillance.\[657\] J-STD-025A, which “defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance.”\[658\] According to J-STD-025A, in order to facilitate the collection and delivery of communications content and Pen/Trap data, the FBI and TSPs must implement an Access Function, a Delivery Function, and a Collection Function.\[659\]

The Access Function “consist[s] of one or more Intercept Access Points (IAPs)...”\[660\] and includes the ability to access intercept subjects' call-identifying information and call content unobtrusively, and make the information available to the Delivery Function.\[661\] “The Delivery Function is responsible for delivering intercepted communications [(over DCSNET)] to one or more Collection Functions. The Delivery Function delivers information over two distinct types of channels: Call Content Channels (CCCs) and Call Data Channels (CDCs).”\[662\] “The Collection Function is responsible for collecting and

---

\[657\] See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 123 of 129; see also EXHIBIT 039 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).


\[659\] See id., § 5.3, p. 34 (Network Reference Model).

\[660\] Id., § 4.2.2, p. 16.

\[661\] See id., § 5.3.1.1, p. 35.

\[662\] Id., § 4.2.2, p. 17 (“The CCCs are generally used to transport call content, such as voice or data communications. The CDCs are generally used to transport messages which report call-identifying information, such as the calling party identities and called party identities.”). However, in the case of packet-mode content information, CDCs are used by the Delivery Function to delivery communications content to the Collection Function. See id., § 5.3.1.2, p. 35.
analyzing intercepted communications and call-identifying information [(i.e., Pen/Trap data)] [663] sent to it by the Delivery Function. The Collection Function is solely the responsibility of the law enforcement agency. [664] For example, the FBI's primary Collection Function is at its Engineering Research Facility where the collected communications content and Pen/Trap data is forwarded to destination Central Monitoring Plants at the various FBI offices. [665]

Under J-STD-025A, delivery of Pen/Trap data from a wireless carrier Delivery Function is made over a DCSNET Call Data Channel using the Lawfully Authorized Electronic Surveillance Protocol (LAESP)—an Open System Interconnection (OSI) Layer 7 (Application Layer) Protocol. [666] LAESP messages are binary encoded and compatible with the X.208 Abstract Syntax Notation One (ASN.1) and the X.209 Basic Encoding Rules (BER). [667][668] LAESP messages received by an FBI Central Monitoring Plant are considered the raw and unaltered Pen/Trap data as collected and encoded by an Intercept Access Point belonging to a Telecommunications Service Provider. [669][670] LAESP messages are delivered over Call Data Channels to Central Monitoring Plants using a variety of OSI Layer 2-4 communications protocols including, but not limited to, Transmission Control/Internet Protocol (TCP/IP), Point-to-Point protocol (PPP), Serial Link Internet 663. Id.

664. See id.

665. See Technical Explanations, Section II(H)(2), supra (explaining DCSNET).


667. See id., § 6.3.2, p. 62.

668. See EXHIBIT 06 of 1st Consolidated Exhibits (Dkt. #587-1) (example of decoded LAESP messages).

669. See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 112 of 129; see also EXHIBIT 048 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

Protocol (SLIP), Link Access Protocol—Balanced (LAPB), and Link Access Protocol—D-Channel (LAPD).[671] Regardless of the protocol stack, Pen/Trap data sent to the FBI via LAESP messages must be sent in real-time, i.e., within eight seconds of the Intercept Access Point receiving Pen/Trap data from the telecommunications network.[672][673] As indicated by a data retention chart created by the Department of Justice, LAESP message data is not listed as being recorded/stored by Telecommunications Service Providers.[674]


The Digital Collection System 3000 (DCS-3000), deployed to Central Monitoring Plants in all FBI field offices and resident agencies,[675] is the FBI's primary Pen/Trap and communications content collection system.[676][677] For Pen/Trap data, the DCS-3000 is used by the FBI as its primary Pen/Trap and communications content collection system. For Pen/Trap data, the DCS-3000 is deployed to Central Monitoring Plants in all FBI field offices and resident agencies. For Pen/Trap data, the DCS-3000 is the FBI's primary Pen/Trap and communications content collection system.


672. See TIA/EIA/J-STD-025A, Lawfully Authorized Electronic Surveillance, § 4.7, p. 31 (“A call-identifying message must be sent from the TSP's IAP to the LEA Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the call event time-stamped to an accuracy of at least 200 milliseconds.”).

673. Depending on the type of circuit used to connect the functions, there is a possibility of the Delivery Function receiving call-identifying information before the Access Function utilizes that information for the purpose of providing aircard service. For example, a looped circuit would result in the prospective Pen/Trap data being switched out of the Access Function as a circuit, looped into the Delivery Function, and then back into the Access Function. See id., Annex A, p. 89 (showing diagram of CALEA network Looped Access); see also EXHIBIT 056 of 2nd Consolidated Exhibits (Dkt. #821-3) (diagram attached). In such a case, law enforcement may receive Pen/Trap data before the wireless carrier even utilizes the data to provide service to the intercept subject.


675. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 3 of 6], p. 32 of 90; see also EXHIBIT 042 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 20071022_dcs03.pdf attached with page numbers added).


677. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 22 of
responsible for processing LAESP messages\[^{678}\]\((containing call-identifying information)\) sent by Telecommunications Service Provider IAPs as they arrive at FBI Central Monitoring Plants over DCSNET. All major Telecommunications Service Providers have network switches configured to be IAPs capable of generating and sending LAESP messages that are ultimately routed to DCS-3000 servers by SBIT.\[^{679}\][\(^{680}\)] The DCS-3000 is a Microsoft Windows based\[^{681}\][\(^{682}\)] server platform comprised of commercial-off-the-shelf hardware\[^{683}\]\ and loaded with a custom application suite developed by Booz Allen & Hamilton (BAH)\[^{684}\][\(^{685}\)] under the direction of TICTU.\[^{686}\] The DCS-3000 server software...
suite consists of the following applications: (1) Server application (used to collect CDC
information pursuant to CALEA);[687] (2) Viking application (used to decode audio
communications);[688] (4) Enhanced Codec Decoder application (used to decode audio
communications);[689] (5) Multivanguard application (used to (a) route FISA CDC and CCC
information to the DCS-5000 (FISA platform),[690][691][692] (b) route Title III (wiretap) CCC
information to the DCS-6000 (criminal platform),[693][694] and (c) route CALEA CDC
information to the DCS-3000 Multiserver application); (6) Multiserver application (used to
send collected CALEA CDC information to DCS-3000 client computer workstations located
in the same Central Monitoring Plant as the DCS-3000 server);[695][696] (7) Tracker
application (used to geographically display cell site position based off of CALEA CDC
information associated with the communications of an intercept subject);[697] and (8)
Backtrack application (used to geographically display cell site position based off of historical

---

687. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 60-
62 of 74; see also EXHIBIT 041 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages
of 20071022_dcs02.pdf attached with page numbers added).

688. See id.

689. See id.

690. See id.

691. See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 105
of 129; see also EXHIBIT 048 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages
of 20080114_dcs04.pdf attached with page numbers added).

692. See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 115
of 125; see also EXHIBIT 039 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages
of 082707_dcs05.pdf attached with page numbers added).

693. See id.

694. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 60-
62 of 74; see also EXHIBIT 041 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages
of 20071022_dcs02.pdf attached with page numbers added).

695. See id.

696. See FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 17 of
150; see also EXHIBIT 046 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages
of 20071217_dcs05.pdf attached with page numbers added).

697. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 60-
62 of 74; see also EXHIBIT 041 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages
of 20071022_dcs02.pdf attached with page numbers added).
cell site location information associated with the communications of an intercept subject).

In order to access data collected by a DCS-3000 server, agents use a client software suite consisting of various component applications residing on one or more Microsoft Windows based client computer workstations within the Central Monitoring Plant.

5. DCS-3000 CDNRS Files.

Once the raw and unaltered LAESP messages are received at an FBI Central Monitoring Plant, they are processed and altered by the DCS-3000 into “human readable” text formatted archive files using the “CDNRS” file format.

While processing the raw and unaltered LAESP messages, the DCS-3000 attempts to extract and format relevant Pen/Trap data before saving it into archive files having .cdnrs file extensions. This post-processed (altered) Pen/Trap data is processed by the DCS-3000 a second time if agent instructs the DCS-3000 to save the data into the CDNRS upload file.

See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 85-87 of 100; see also EXHIBIT 043 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 17 of 74; see also EXHIBIT 041 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

See FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 149 of 150; see also EXHIBIT 046 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 63 of 74; see also EXHIBIT 041 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 112 of 129; see also EXHIBIT 048 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

See FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 100 of 143; see also EXHIBIT 044 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

See FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 105 of 150; see also EXHIBIT 046 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 46 of 100; see also EXHIBIT 043 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 46 of 100; see also EXHIBIT 043 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).
format.[707] In response to an agent requesting such a save, the DCS-3000 reformats the Pen/Trap data contained in the .cdnrs files and saves the reformatted data in “summary” and “log” files[709] having .sum and .log file extensions.[710] The DCS-3000 then automatically places the .sum and .log files into folders named “sum” and “log” respectively and places those folders into a second folder named “Cdnrs” nested in a parent folder taking the name of the target phone number[711] (e.g., H:\5551234567\Cdnrs\Log\000000.000.log). The CDNRS .sum and .log files are typically used to upload the post-processed Pen/Trap data to the Telephone Applications (TA) database[712] at FBI Headquarters.[713]

6. Telephone Applications System.

The Telephone Applications System, maintained by the FBI's Information Technology Operations Division (ITOD),[714] consists of a database of Pen/Trap data and various

---

707. See FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 105 of 150; see also EXHIBIT 046 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

708. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 75 of 100; see also EXHIBIT 043 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).


710. See EXHIBIT 10 of 1st Consolidated Exhibits (Dkt. #587-1) (example of .sum CDNRS file); EXHIBIT 09 of 1st Consolidated Exhibits (Dkt. #587-1) (example of .log CDNRS file).


712. See FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 75 of 100; see also EXHIBIT 043 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

713. See FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 100 of 143; see also EXHIBIT 044 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

714. See FBI Feb. 11, 2008, Response to EFF FOIA Request [EFF PDF Set 1 of 3], p. 15 of 154; see also EXHIBIT 049 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080211_dcs01.pdf attached with page numbers added).
software applications remotely used by FBI field offices to search and analyze the data contained in the database.\[715\] Most FBI field offices use the DCS-3000 as a front-end collection system for Pen/Trap data.\[717\] Once the Pen/Trap data is collected, it is converted into the CDNRS upload file format\[718\] and then uploaded to the Telephone Applications database located at FBI Headquarters.\[719\] The task of uploading the CDNRS files to the Telephone Applications database may be done either manually by an agent or automatically by the DCS-3000.\[720\] The Telephone Applications database maintains a record of all Pen/Trap data collected by the FBI since the time the database was created. The Telephone Applications software allow investigators to conduct cross reference and datamining investigations using the database in order to generate leads and display Pen/Trap data in a user friendly form. Agents may use either Trilogy desktop computers or DCS-3000 client computers to access the Telephone Applications database via search and analysis application software.

7. FBI Cell Site Database.

The FBI TICTU/SBIT maintains a large central database containing cell site position

---

715. See FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 100 of 143; see also EXHIBIT 044 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

716. See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 111 and 121 of 129; see also EXHIBIT 048 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

717. See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 121 of 129; see also EXHIBIT 048 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

718. See Technical Explanations, Section II(H)(5), supra.

719. See FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 100 of 143; see also EXHIBIT 044 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

720. See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 112 of 129; see also EXHIBIT 048 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

721. See FBI Feb. 11, 2008, Response to EFF FOIA Request [EFF PDF Set 1 of 3], p. 15-20 of 154; see also EXHIBIT 049 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080211_dcs01.pdf attached with page numbers added).
information for all major wireless carriers. The cell site database may be queried by agents to provide the geographic location of a particular target's location based off of either real time Pen/Trap data contained in LAESP messages or historical data obtained directly from wireless carrier personnel. The cell site database contains up to date records of the longitude and latitude coordinates for each wireless carrier cell site and the general cell site sector positioning convention used by each respective wireless carrier, i.e., beamrange and a standard default beamwidth for each sector. For some wireless carriers, the cell site database also contains up to date records on the precise antenna azimuth and beamwidth of each cell site sector covering the wireless network. There are numerous ways that agents may access the cell site database for the purpose of locating wireless devices. Among other means of access, the DCS-3000 has a “software hook” that can be used to automatically send cell site position records from the cell site database to various locally installed mapping programs such as Wintrack by Integrated Systems Research (ISR).
and Microsoft Streets and Trips. The “software hook” also allows for sending cell site position records from the cell site database to other DCS server platforms such as the DCS-1020 used in the FBI “WITT Van” integration project.

8. FBI Wireless Intercept and Tracking Team (WITT).

Once cell site location information (either historical or real time) is used to locate a target wireless device to an area covered by a single cell site sector, local FBI Wireless Intercept and Tracking Team (WITT) agents will attempt to pinpoint the location of the

---

731. See FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 93 of 143; see also EXHIBIT 044 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).


733. See FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 95 of 143 (“We developed this feature to integrate with our [REDACTED] van-based systems. The idea is to have the DCS 3000 feed lat/long information via cellular modem to a [REDACTED] van.”); see also EXHIBIT 044 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).


735. See FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 118 of 129; see also EXHIBIT 048 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

736. See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 45-47 of 67; see also EXHIBIT 038 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).
device by deploying a “WITT Van” equipped with a transportable wireless device locator, i.e., the Harris StingRay. The WITT agents will attempt to pinpoint the location of the target wireless device by using the StingRay and related surveillance equipment while driving the WITT Van around the area covered by the previously identified serving cell site sector. If agents are collecting call-identifying information on the intercept subject, the local Central Monitoring Plant will send the target's cell site sector location/position information to the WITT van in real-time. The local Central Monitoring Plant completes this task through the following chain of events: (1) the DCS-3000 server receives cell site location information for a target via LAESP messages.

737. See id., p. 41 of 67; see also EXHIBIT 038 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

738. See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 54 of 125; see also EXHIBIT 039 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

739. See id., p. 36 of 125 (“...DCS-1020 gateway server for the real-time delivery of cell site location information to Wireless Tracking Team (WITT) vans.”); see also EXHIBIT 039 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

740. See FBI Sept. 24, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 3], p. 52-58 of 113 (sections DCS-1020 Software Installation and Users Manual); see also EXHIBIT 040 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 092407_dcs01.pdf attached with page numbers added).

741. See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 41 of 67; see also EXHIBIT 038 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

742. See Technical Explanations, Section II(G)(1), supra (explaining the StingRay).

743. See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 16 and 26 of 67; see also EXHIBIT 038 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

744. See FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 100 of 143; see also EXHIBIT 044 of 2nd Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

745. See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 36 of 125 (“...DCS-1020 gateway server for the real-time delivery of cell site location information to Wireless Tracking Team (WITT) vans.”); see also EXHIBIT 039 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

746. See Technical Explanations, Section II(H)(4), supra (explaining the DCS-3000 server).

747. See id., Section II(H)(3), supra (explaining LAESP messages).
sent from a wireless carrier Intercept Access Point,\(^{[748]}\) (2) the DCS-3000 server processes and alters the LAESP messages into the CDNRS file format,\(^{[749]}\) (3) the DCS-3000 server queries the cell site database at the FBI ERF over DCSNET for longitude, latitude, azimuth, beamwidth, and beamrange\(^{[750]}\)\(^{[751]}\) of the serving cell site/sector listed in the CDNRS files, (4) once receiving the requested cell site position information, the DCS-3000 server sends the data to a DCS-1020 gateway server\(^{[752]}\) located at the same Central Monitoring Plant as the DCS-3000, and (5) the DCS-1020 server sends the cell site/sector location/position information over the Internet\(^{[753]}\)\(^{[754]}\) via a Virtual Private Network (VPN),\(^{[755]}\) to a wireless cellular modem (i.e., an FBI aircard)\(^{[756]}\)\(^{[757]}\) paired with a laptop computer\(^{[758]}\)\(^{[759]}\) located...
inside the WITT Van. Once the WITT van receives the real-time cell site location
information, WITT agents drive the van around the target area while using the StingRay to
obtain a general, but more precise, location estimate. Once the StingRay obtains the general
location, WITT agents will deploy handheld equipment (i.e., the Harris KingFish) to pinpoint
the exact location of the target wireless device—even as precise as within a hotel, office
building, or similar structure.[760]

III. PROCEDURAL HISTORY

The defendant is directly challenging ten different documents upon which the
government relied while conducting its numerous independent Fourth Amendment searches
and seizures.[761] In support of the Fourth Amendment arguments raised in the Argument
section of this memorandum (Section V, *infra*), the subsections immediately below
summarize the documents relied upon by the government to locate the aircard and search the
defendant's home. The noted documents are explained purely from a procedural viewpoint
and are later brought into context through the General Facts (Section IV, *infra*). The
Procedural History is separated from the General Facts to maintain modularity and to
facilitate an easy comprehension of the relevant issues.

A. D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615
relating to identification of the aircard and destination IP addresses.

On June 6, 2008, the government served Verizon Wireless with D.Ariz. Grand Jury
subpoena No. 07-03-609 seeking subscriber transactional records for the account assigned
the Verizon Wireless network IP addresses 75.209.101.132, 75.208.105.186, and
75.209.41.104. *See Submission Of Documents Related To District Of Arizona Grand Jury
Subpoenas 07-03-609 And 07-03-615 Obtained To Facilitate Locating The Aircard* (Dkt.
760. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 41
of 67; *see also* EXHIBIT 038 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of
082707_dcs01.pdf attached with page numbers added).

761. The defendant is challenging (1) D.Ariz. Grand Jury subpoena No. 07-03-609, (2)
D.Ariz. Grand Jury subpoena No. 07-03-615, (3) D.Ariz. 08-3286MB-LOA order, (4)
D.Ariz. 08-3298MB-LOA order, (5) D.Ariz. 08-7273MB-LOA order, (6) N.D.Cal. 08-
90330MISC-RS order, (7) N.D.Cal. 08-90331MISC-RS order, (8) N.D.Cal. 08-70460-HRL
search warrant *(original)*, (9) N.D.Cal. 08-70460-HRL search warrant *(amended)*, and (10)

- 123 -
On June 16, 2008, the government served Verizon Wireless with D.Ariz. Grand Jury subpoena No. 07-03-615 seeking the same information sought by the first subpoena but only making reference to IP address 75.209.41.104. See id. (Dkt. #565-2, p. 10). The two Grand Jury subpoenas were obtained pursuant to 18 U.S.C. § 2703(c)(2).

Among other information, the Grand Jury subpoenas requested that Verizon Wireless provide connection time, date, source IP address, source port and destination port, data transfer volume, and method of connection to system (telnet, ftp, http) for all IP addresses accessed by the defendant between March 1, 2008 and June 16, 2008. See, e.g., id. (Dkt. #565-1, p. 4).

On June 13, 2008, Verizon Wireless complied with D.Ariz. Grand Jury subpoena No. 07-03-609 by providing a response to AUSA Frederick A. Battista. See id. (Dkt. #565-1).

On June 18, 2008, Verizon Wireless complied with D.Ariz. Grand Jury subpoena No. 07-03-615 by providing a response to FBI Agent Richard J. Murray. See id. (Dkt. #565-2). The Verizon Wireless responses reported that the three source IP addresses were linked to a 1xEV-DO “BroadbandAccess Connect Service” account having wireless account number 270691733 (hereafter “aircard account”) opened under the name of Travis Rupard.

The Verizon Wireless responses further reported that the three source IP addresses were specifically linked to a “UTStarcom PC5740” wireless device (i.e., the “aircard”) with mobile directory number 415-264-9596 and ESN 005-00717190 (i.e., 050AF186). See, e.g., id. (Dkt. #565-1, p. 14). In addition to containing identifying information for the aircard and aircard account, the Verizon Wireless responses also consisted of logs containing 411,368 destination IP addresses pertaining to websites.

The aircard account also has “per message charges” text message service. See id. (Dkt. #565-1, p. 11).

The government was not able to locate the aircard with information obtained solely by the subpoenas.

005-00717190 is the standard 11-digit decimal number representation of hexadecimal 050AF186 (i.e., the aircard's 32 bit ESN). Because 0x05=5, the first 8 bits of the ESN is displayed as “005-”. Because 0xA000=655360, 0xF000=61440, 0x1000=256, 0x80=128, and 0x06=6 (655360+61440+256+128+6=717190), the last 24 bits of the ESN is displayed as “00717190.”

and other Internet resources accessed by the aircard during the date range of May 11, 2008 through June 12, 2008. See, e.g., id. (Dkt. #565-2, p. 7-9). Further information regarding the destination IP addresses is provided in the General Facts, Section IV(B)(1), infra.

B. D.Ariz. order No. 08-3286MB-LOA, i.e., the destination IP address retroactive order.

On July 9, 2008, AUSA Battista signed and submitted an order application[766] in the District of Arizona having docket No. 08-3286MB-LOA. See Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard (Dkt. #576-1). In the order application, AUSA Battista stated the following:

[D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615] were authorized by the prosecutor assigned to this case after reading Section [18 U.S.C. §] 2703 and inadvertently concluding that [[destination IP addresses] may be requested via a Grand Jury subpoena under Section [18 U.S.C. §] 2703(c). Verizon Wireless subsequently responded to the subpoenas; in one case providing a number of destination IP addresses... and in the second case providing a large number of destination IP addresses. The information was subsequently examined by members of the investigation team... [O]n July 7, 2008, the prosecutor was advised by an attorney with the Department of Justice's Office of Enforcement Operations that Section 2703(c) has been interpreted to only permit the collection of a subscriber's “source” IP addresses via a Grand Jury subpoena and not a subscriber's “destination” IP addresses. Upon receipt of this notice, the prosecutor informed his supervisor of these events and has since required that all of the information received by Verizon Wireless concerning destination IP addresses and information relating to the volume of the data transferred be sealed and not used in any manner in furtherance of the investigation.

Id. (application, p. 14-15) (Dkt. #576-1, p. 15-16).

Based on the above, AUSA Battista requested that the court “enter an order, effective June 6, 2008, relating to the subject destination IP addresses and any related materials retroactively in this case.” Id. (application, p. 15) (Dkt. #576-1, p. 16). In his order application, AUSA Battista failed to indicate that the government had used the illegally obtained destination IP addresses accessed by the aircard from May 11, 2008 through June 5, 2008 and the D.Ariz. Grand Jury subpoena No. 07-03-615 contained approximately 111 aircard destination IP addresses accessed by the aircard from May 19, 2008 through June 12, 2008. See Submission Of Documents Related To District Of Arizona Grand Jury Subpoenas 07-03-609 And 07-03-615 Obtained To Facilitate Locating The Aircard (Dkt. #565).

766. AUSA Battista's order application cited 18 U.S.C. § 2703(d) as authority authorizing his request.
addresses to significantly advance its investigation against the defendant over the prior 26 days.\[767]\n
On July 9, 2008, United States Magistrate Judge Lawrence O. Anderson signed a “retroactive order” approving the D.Ariz. 08-3286MB-LOA order application. See id. (order) (Dkt. #576-2). The D.Ariz. 08-3286MB-LOA order was made effective June 6, 2008 and required Verizon Wireless to provide the government with the same aircard destination IP addresses that were already illegally obtained under D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615. In the order, the magistrate found that AUSA Battista “offered 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. (order, p. 1) (Dkt. #576-2, p. 2); see also 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d).\[768]\n
Among other information, the D.Ariz. 08-3286MB-LOA order requested that Verizon Wireless provide connection source IP address, connection time and date, disconnect time and date, data transfer volume, connection IP destination, and method of connection to system (telnet, ftp, http) for all IP addresses accessed by the defendant between March 1, 2008 and July 9, 2008. See id. (order, p. 1) (Dkt. #576-2, p. 2).

The government served Verizon Wireless with the D.Ariz. 08-3286MB-LOA order on an unknown date. On July 16, 2008, Verizon Wireless complied with the order by providing FBI Agent Murray a response containing various information. See EXHIBIT 01 of 1st Consolidated Exhibits (Dkt. #587-1). The Verizon Wireless response consisted of logs containing (1) the 411,368 destination IP addresses accessed by the aircard from May 11, 2008 through June 5, 2008 that were already obtained via D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615, and (2) 1,424,772 additional destination IP addresses pertaining to websites and other Internet resources accessed by the aircard from June 5, 2008 through July 9, 2008. Further information regarding the destination IP addresses is provided in the

\[767\] See General Facts, Section IV(B)(1), infra (discussing factual aspects of the illegally obtained destination IP addresses).

\[768\] However, nowhere in the order does the magistrate make a finding of probable cause in support of any type of search and/or seizure.
General Facts, Section IV(B)(1), infra.

C. D.Ariz. order No. 08-3298MB-LOA, i.e., historical cell site information order.

On July 10, 2008, AUSA Battista signed and submitted an order application[769] in the District of Arizona having docket No. 08-3298MB-LOA. See Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard (Dkt. #576-3). Through the order application, AUSA Battista sought an order requiring Verizon Wireless to provide the government with historical cell site information for the last 30 days so that the government may “determine the cellular/data network's registration” of the aircard. Id. (application, p. 2-3) (Dkt. #576-3, p. 3-4). AUSA Battista further indicated that the sought after information is intended to “help government investigators to identify the individual(s) who are responsible” for the alleged scheme. Id. (application, p. 13) (Dkt. #576-3, p. 14). AUSA Battista did not indicate that he sought cell site location information, aircard location information, or other information that would assist the government in physically locating the aircard or aircard user.

On July 10, 2008, magistrate Judge Anderson signed an order approving the D.Ariz. 08-3298MB-LOA order application. Id. (order, p. 13) (Dkt. #576-4). The D.Ariz. 08-3298MB-LOA order required Verizon Wireless to provide the government with the following historical cell site information:

Cell site information and sector/distance information to determine the cellular/data network's registration of the assigned broadband access card(s) [(i.e., aircard)] associated with data transmissions or connections for 30 days prior to the date of this Order.

Id. (order, ATTACHMENT A) (Dkt. #576-4, p. 4).

In the order, the magistrate found that AUSA Battista “offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information

769. AUSA Battista's order application cited 18 U.S.C. § 2703(d) as authority authorizing his request.
sought are relevant and material to an ongoing criminal investigation.” Id. (order, p. 1) (Dkt. #576-4, p. 2); see also 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d). However, the magistrate did not make a finding of probable cause in support of any type of search and/or seizure.

The government served Verizon Wireless with the D.Ariz. 08-3298MB-LOA order on an unknown date. On July 12, 2008, Marko Denton, Verizon Wireless law enforcement liaison, complied with the order by providing FBI Agent Murray and Robert Byrne, Law Enforcement Online (LEO), a response containing historical cell site information for the aircard generated during the date range of June 10, 2008 through July 11, 2008. See EXHIBIT 02 of 1st Consolidated Exhibits (Dkt. #587-1). On August 1, 2008, John Profaca, Verizon Wireless law enforcement liaison, provided FBI Agent Murray with a second response containing additional aircard historical cell site information generated during the same date range of June 10, 2008 through July 11, 2008. See EXHIBIT 03 of 1st Consolidated Exhibits (Dkt. #587-1). John Profaca provided the second set of cell site information in response to a direct request made by FBI Agent Murray under the authority of the D.Ariz. 08-3298MB-LOA order.[770] FBI Agent Murray sought additional cell site location information from Verizon Wireless despite the fact that Marko Denton had already complied with the D.Ariz. 08-3298MB-LOA order on July 12, 2008—twenty days prior.

Among other information contained in the two responses, Verizon Wireless provided the government with historical cell site location information, i.e., the latitude and longitude coordinates for cell sites accessed by the aircard during the relevant time frame. Further information regarding the historical cell site location information is provided in the General Facts, Section IV(B)(2), infra.

D. D.Ariz. order No. 08-7273MB-ECV, i.e., historical cell site information order.

On July 16, 2008, AUSA Battista signed and submitted an order application[771] in the

---

[770] See EXHIBIT 04 of 1st Consolidated Exhibits (Dkt. #587-1) (August 1, 2008 emails from FBI Agent Murray to Verizon Wireless: requesting additional aircard historical cell site location information).

[771] AUSA Battista's order application cited 18 U.S.C. § 2703(d) as authority authorizing his request.
District of Arizona having docket No. 08-7273MB-ECV. See Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard (Dkt. #576-5). Through the order application, AUSA Battista sought an order requiring Verizon Wireless to provide the government with the most current historical cell site information so that it may “determine the cellular/data network's registration” of the aircard. Id. (application, p. 2-3) (Dkt. #576-5, p. 3-4). AUSA Battista further indicated that the sought after information is intended to “help government investigators to identify the individual(s) who are responsible” for the alleged scheme. Id. (application, p. 13) (Dkt. #576-5, p. 14). AUSA Battista did not indicate that he sought cell site location information, aircard location information, or other information that would assist the government in physically locating the aircard or aircard user.

On July 16, 2008, United States Magistrate Judge Edward C. Voss signed an order approving the D.Ariz. 08-7273MB-ECV order application. Id. (order, p. 13) (Dkt. #576-6, p. 14). The D.Ariz. 08-7273MB-ECV order required Verizon Wireless to provide the government with the following historical cell site information:

Cell site information and sector/distance information to determine the cellular/data network's registration of the assigned broadband access card(s) [(i.e., aircard)] associated with data transmissions or connections from July 11, 2008, to the date of this Order.

Id. (order, ATTACHMENT A) (Dkt. #576-6, p. 4).

In the order, the magistrate found that AUSA Battista “offered 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. (order, p. 10 (Dkt. #576-6, p. 2); see also 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d). However, the magistrate did not make a finding of probable cause in support of any type of search and/or seizure.

The government served Verizon Wireless with the D.Ariz. 08-7273MB-ECV order on an unknown date. On July 31, 2008, Verizon Wireless complied with the order by providing Robert Byrne, LEO, a response containing aircard historical cell site information generated
during the date range of June 11, 2008 through July 17, 2008. See EXHIBIT 05 of 1st Consolidated Exhibits (Dkt. #587-1). Among other information contained in the response, Verizon Wireless provided the government with historical cell site location information, i.e., the latitude and longitude coordinates for cell sites accessed by the aircard during the relevant time frame. Further information regarding the historical cell site location information is provided in the General Facts, Section IV(B)(2), infra.

E. N.D.Cal. order No. 08-90330MISC-RS, i.e., use and monitor a mobile tracking device order.

On July 11, 2008, AUSA Shawna Yen signed and submitted an order application [772] in the Northern District of California having docket No. 08-90330MISC-RS. See Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (Dkt. #470-1). [773] Through the order application, AUSA Yen sought an order directing Verizon Wireless to (1) assist the government in the use and monitoring of a mobile tracking device for the aircard while the aircard is located inside private residences and other locations not open to public or visual surveillance, and (2) provide the government immediately on request with all information needed to ascertain the physical location of the aircard. [774] Id. (application, p. 2-3) (Dkt. #470-1). AUSA Yen also sought specific authority allowing the government to (1) ignore Fed. R. Crim. P. 41(f), (2) not serve a copy of the order on any owner of the aircard, (3) not make an inventory of any resulting information, and (4) destroy all data obtained by the order at the conclusion of the


773. AUSA Yen's order application included an affidavit by FBI Agent William T. Ng wherein he outlined the government's investigation and stated his belief that “there is probable cause to believe that the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone will lead to evidence of violations of the statutes listed above; as well as to the identification of individuals who are engaged in the commission of these offenses.” Id. (application, p. 18) (Dkt. #470-1).

774. AUSA Yen also requested that the order application and order be sealed and that Verizon Wireless be directed not to reveal the existence of the order or investigation to anyone. See id. (application, p. 4) (Dkt. #470-1).
aircard locating mission. *Id.* (application, p. 3) (Dkt. #470-1). Nowhere in the order application does AUSA Yen define “mobile tracking device” or describe the various independent searches and seizures the FBI intended to conduct separate from Verizon Wireless.

On July 11, 2008, United States Magistrate Judge Richard Seeborg signed an order containing two separate findings and approving some of AUSA Yen's requests made through the N.D.Cal. 08-90330MISC-RS order application. See *id.* (order) (Dkt. #470-1). The first finding is as follows:

The Court FINDS that there is probable cause to believe that the use and monitoring of a mobile tracking device for the aircard[, will lead to evidence of violations of [the alleged offenses], as well as to identification of the individuals who are engaged in the commission of these offenses. *Id.* (order, p. 2) (Dkt. #470-1).

Although the magistrate found that there was probable cause to use and monitor a mobile tracking device, he did not find that there was probable cause to install a mobile tracking device nor did he define the term “mobile tracking device.” Additionally, after the above quoted finding, the magistrate did not expressly state in the operative section of the order that he authorized the government to install, use, or monitor a mobile tracking device. The magistrate also did not grant AUSA Yen's request to order Verizon Wireless to “assist the agents in the use and monitoring of a mobile tracking device.” *Id.* (application, p. 3) (Dkt. #470-1). Regardless of whether installation and use of an undefined “mobile tracking device” was authorized, nowhere in the order does the magistrate make a finding of probable cause in support of any type of search and/or seizure. Likewise, the magistrate did not authorize any search and/or seizure in the operative section of the order.

The magistrate's second finding addresses the government obtaining information relating to the location of the aircard directly from Verizon Wireless. The second finding is

---

775. Sections of the order that authorize sealing the relevant documents and nondisclosure by Verizon Wireless are not summarized here.

776. The N.D.Cal. 08-90330MISC-RS order did not authorize the government to conduct any sort of activity to locate the aircard—the order was entirely directed at Verizon Wireless.
as follows:

   The Court further FINDS that specific and articulable facts establish that there are reasonable grounds to believe that the requested information pertaining to the location of the [aircard] is relevant and material to an ongoing criminal investigation.”

   Id. (order, p. 2 (emphasis added)) (Dkt. #470-1); see also 18 U.S.C. §§ 2703(c) (1)(B) and 2703(d).

After stating the above, the magistrate paired his “specific and articulable facts” finding to an operative requiring that Verizon Wireless provide the FBI with the requested information pertaining to the location of the aircard:

   The Court therefore ORDERS, pursuant to Federal Rules of Criminal Procedure 41(b); Title 18, United States Code, Section 2703 and 3117; and Title 28, United States Code, Section 1651, that Verizon Wireless, within ten (10) days of the signing of this Order and for a period not to exceed 30 days, unless extended by the Court, shall provide to agents of the FBI data and information obtained from the monitoring of transmissions related to the location of the [aircard], and shall monitor such transmissions, to extend to any time of the day or night as required, including the monitoring of the [aircard] while the agents are stationed in a public location and the [aircard] is (a) inside private residences, garages and/or other locations not open to the public or visual surveillance; and (b) anywhere else the [aircard] may be present within the United States []; said ORDER being expressly limited to [monitoring] transmissions needed to ascertain the physical location of the [aircard], and expressly excludes any voice communications and data content transmitted by Verizon Wireless to or from the [aircard];

   Id. (order, p. 2-3 (emphasis added)) (Dkt. #470-1).

In regards to Verizon Wireless being required to provide the government with the above described aircard location information, the magistrate did not make a finding of probable cause that the information obtained would be evidence of a crime or that there was probable cause to seize aircard location information from Verizon Wireless. In addition to the above quoted operative, the magistrate also ordered that Verizon Wireless provide the FBI with all facilities and technical assistance needed to locate the aircard and that Verizon Wireless be compensated for its assistance:

   It is further ORDERED, pursuant to Federal Rule of Criminal Procedure 41(b); Title 18, United States Code, Sections 2703 and 3117; and Title 28, United States Code, Section 1651, that Verizon Wireless shall provide said agents immediately on request with all information, facilities, and technical assistance needed to ascertain the physical location of the [aircard] and the FBI shall compensate Verizon Wireless for reasonable expenses incurred in complying with any such request.
Regarding AUSA Yen's request to destroy evidence and ignore what would otherwise have been standard warrant requirements, the magistrate granted the request in full:

WHEREAS the return and inventory requirements of Federal Rule of Criminal Procedure 41(f) do not apply to the information sought to be obtained by the instant application, Special Agents of FBI are therefore not required to serve a copy of this Order on any owner of the aircard, nor to make an inventory of any resulting information to be served on any such owner, except upon further Order of the Court. However, at the conclusion of the tracking mission, the investigating agency shall expunge all of the data obtained by this Court Order;

Id. (order, p. 3) (Dkt. #470-1).

The magistrate also gave the government unrestrained and unchecked authority to edit out sections of the order prior to serving copies on the relevant parties:

The Court further ORDERS that the government's Application, the attached Affidavit, and the Court's Order be filed under seal, except that copies of the Court's Order in full or redacted form may be served on Special Agents and other investigative and law enforcement officers of the FBI, federally-deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, and the service providers as necessary to effectuate the Court's Order.

Id. (order, p. 3) (emphasis added) (Dkt. #470-1).

Verizon Wireless and various FBI technical agents were served with the N.D.Cal. 09-90330MISC-RS order on an unknown date. Details relating to service of the order, either in redacted form or in full, remain a mystery due to the government refusing to produce as witnesses the FBI technical agents who executed the order. During and after execution of the order, the government also failed to comply with Fed. R. Crim. P. 41(f)(1)(B); (f)(1)(D); (f)(2)(B); (e)(2)(B) and (iii); (e)(2)(A) and (iii); (f)(2)(C); and (f)(1)(C)—in the effect that the notation of time, receipt, service, and return requirements for both conventional and tracking device warrants were not followed. Additionally, by virtue of violating Rule 777.

See January 4, 2012 Court Order (Dkt. #723, p. 12) (Noting and agreeing with the government's position that “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.”).

778. All Rule 41 references contained in this memorandum correspond to the 2008 version.
41(f), the government prevented the issuing magistrate from complying with Rule 41(i).[779]

In response to the defendant's request for all data and information obtained from Verizon Wireless via the N.D.Cal 08-90330MISC-RS order, the government stated that “[t]he data has been expunged in accordance with the order...”[780][781] The government also destroyed the aircard location evidence obtained as a result of the FBI technical agents operating the StingRay and related equipment.[782]

F. N.D.Cal. order No. 08-90331MISC-RS, i.e., pen register and trap and trace order.

On July 10, 2008, AUSA Yen signed and submitted an order application[783] in the Northern District of California having docket No. 08-90331MISC-RS. See Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (Dkt. #470-2).[784] Through the order application, AUSA Yen sought an order directing Verizon Wireless to provide the government with real-time cell site location information pertaining to the aircard. AUSA Yen stated in the 08-90331MISC-RS order of the rule.

779. Rule 41(i) reads, “[t]he magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, of the inventory, and of all other related papers and must deliver them to the clerk in the district where the property was seized.” Id.

780. EXHIBIT 070 of 2nd Consolidated Exhibits (Dkt. #821-4) (June 18, 2010 letter from AUSA Battista to the defendant, p. 3).

781. See also January 4, 2012 Court Order (Dkt. #723, p. 14) (Noting the government's concession that “[a]ll 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.”).

782. See id.

783. AUSA Yen's order application cited 18 U.S.C. §§ 2703(c) and (d), and 18 U.S.C. §§ 3122 and 3123 as authority authorizing his request.

784. AUSA Yen's order application included an affidavit by FBI Agent Ng wherein he outlined the government's investigation and stated his belief that “there is probable cause to believe that the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone will lead to evidence of violations of the statutes listed above; as well as to the identification of individuals who are engaged in the commission of these offenses.” Id. (application/affidavit, p. 18) (Dkt. #470-1). However, FBI Agent Ng's affidavit is completely irrelevant to the N.D.Cal 08-90331MISC-RS order because the issuing magistrate made no finding of probable cause in the issued order.

- 134 -
application that “the general geographical location of the [aircard] derived from [real-time] cell site information... can [be] compare[d] [to] observations of the user of the [aircard]... in order to verify the identification and approximate location of the user of the [aircard].” *Id.* (application, p. 8) (Dkt. #470-2).

On July 11, 2008, Judge Seeborg signed an order approving the N.D.Cal. 08-90331MISC-RS order application. *See id.* (order) (Dkt. #470-2). The N.D.Cal. 08-90331MISC-RS order required Verizon Wireless to provide the government with the following real-time cell site location information:

For the Target Device [(i.e., aircard)], after receipt and storage, records or other information pertaining to subscriber(s) or customer(s), including... cellsite information, provided to the United States for (a) the origination of a call from the Target Device or the answer of a call to the Target Device and (b) the termination of the call (but not including the contents of communications.) *Id.* (order, p. 4) (Dkt. #470-2).

The magistrate defined “cell site information,” as used in the order, to mean “the physical location and/or address of the cellular tower and identification of the particular sector of the tower receiving the signal[]” but also made clear his understanding that cell site information “does not provide the specific or precise geographical coordinates of the [aircard].” *Id.* (order, p. 2 fn. 1) (Dkt. #470-2). Furthermore, the magistrate specifically forbade the government from obtaining “(1) any cell site information that might be available when the [aircard] is turned 'on' but a call is not in progress; [and] (2) information that would allow [the government] to triangulate multiple antenna tower locations and thereby attempt to determine the precise location of the user of the [aircard].” *Id.* (order, p. 3) (Dkt. #470-2).

The N.D.Cal. 08-90331MISC-RS order required Verizon Wireless to provide the government with cell site location information “after receipt and storage” during the date range of July 11, 2008 through September 8, 2008 and “as soon as practicable, twenty four (24) hours a day for the duration of the Order,” *i.e.*, in real-time. *Id.* (order, p. 5-6) (Dkt. #470-2). The magistrate explained the “after receipt and storage” provision of the order to mean that the cell site location information must “first [be] captured and recorded by the provider before being sent to the Investigative Agency.” *Id.* (order, p. 4 fn. 6) (Dkt. #470-2).
The magistrate found that AUSA Yen “certified that the information likely to be obtained... is relevant to an ongoing criminal investigation” and that there are “specific and articulable facts showing that there are reasonable grounds to believe that... cell site information regarding the [aircard is]... relevant and material to an ongoing criminal investigation.” *Id.* (order, p. 1-2) (Dkt. #470-2); *see also* 18 U.S.C. § 3123, and 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d). However, the magistrate did not make a finding of probable cause in support of any type of search and/or seizure.

Verizon Wireless was served with the N.D.Cal. 08-90331MISC-RS order on an unknown date. On July 16, 2008, the FBI configured its SF-Martinez DCS-3000 server (pen register and trap and trace device) to receive real-time LAESP messages from Verizon Wireless Intercept Access Points (IAPs). The FBI used the SF-Martinez DCS-3000 server to receive LAESP messages (containing real-time cell site sector location information) generated in response to the FBI surreptitiously placing voice calls to the aircard on July 16, 2008. *See EXHIBIT 06 of 1st Consolidated Exhibits* (Dkt. #587-1). The LAESP messages received by the FBI related to the aircard accessing the Verizon Wireless cellular voice network. The government later converted the LAESP messages to CDNRS formatted files for ease of use. *See EXHIBIT 07, EXHIBIT 08, EXHIBIT 09, and EXHIBIT 10 of 1st Consolidated Exhibits* (Dkt. #587-1). Further information regarding the real-time cell site location information obtained via the SF-Martinez DCS-3000 server is provided in the *General Facts, Section IV(B)(6), infra.*

**G. D.Ariz. Grand Jury subpoena No. 07-03-709 relating to Domicilio electronic gate key access records.**

On July 23, 2008, the government served Quality Alarm Service, 3523 Haven Ave, Menlo Park, CA 94025, with D.Ariz. Grand Jury subpoena No. 07-03-709 seeking Domicilio electronic gate key access records for the occupant of apartment No. 1122. *See Submission Of Documents Related To District Of Arizona Grand Jury Subpoena 07-03-709 Obtained To Facilitate Locating The Aircard* (Dkt. #805-1). The Grand Jury subpoena sought the following information:
All secure gate records, including but not limited to, access date, access time and gate accessed, pertaining to Domicilio Resident: Steven Brawner, Address: 431 El Camino Real, Apartment 1122, Santa Clara, California, 95050, Assigned “fob” Number: 58261, for the time period January 1, 2008 to July 23, 2008.

Id. (Dkt. #805-1, p. 3).


Further information regarding the historical electronic gate key access information is provided in the General Facts, Section IV(B)(12), infra.

H. N.D.Cal. warrant No. 08-70460-HRL (the original unexecuted and amended versions).

On July 22, 2008, IRS-CI Agent Michael P. Fleischmann and AUSA Yen submitted a search warrant application and affidavit in the Northern District of California having docket No. 08-70460-HRL. See Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122 (Dkt. #566-1). Through the N.D.Cal. 08-70460-HRL warrant application, IRS-CI Agent Fleischmann and AUSA Yen sought a search warrant to physically search for and seize items out of apartment No. 1122. See id. Paragraph No. 102 of IRS-CI Agent Fleischmann's affidavit in support of the N.D.Cal. 08-70460-HRL warrant application provides the only information linking the aircard location to apartment No. 1122:

102. Historical cell tower information and other investigative techniques have led the investigation team to the location of the Travis Rupard Broadband Access Card within the “domicilio” apartment complex; 431 El Camino Real; Apartment 1122; Santa Clara, California, 95050.

Id., p. 31 (Dkt. #566-1, p. 33).

In his affidavit, IRS-CI Agent Fleischmann also provided information on the rental application for apartment No. 1122:

103. On July 17, 2008, a Grand jury subpoena was issued to domicilio...
for the file information related to 431 El Camino Real, Apartment 1122, Santa
Clara, California, 95050. The subpoena revealed the apartment is currently
being rented by an individual claiming to be Steven Travis Brawner. The
rental application indicates Brawner is a software engineer.

104. Brawner provided a California driver's license, license number
D6870214. Further investigation revealed the California driver's license
number is assigned to a female with a Chino Hills, California address.

105. In order to rent the apartment, Brawner was required by the rental
company to provide a copy of the first page of what he claimed to be this [sic]
2006 tax return. The return purports to show an adjusted gross income (AGI)
of $110,314. The social security number on the return is [REDACTED]4167.
Internal records for the Internal Revenue Service were researched and revealed
no tax return for 2006 was filed for Steven Brawner. Additionally, Social
Security Administration records for social security number [REDACTED]4167
indicated that Steven Brawner died in 1997.

conducted a handwriting analysis of the original application documents for the
Sacramento Post Office Box. After conducting the analysis of the documents,
Mr. Flynn has advised that forensic evidence indicates common authorship
among the documents.

Id. (Dkt. #566-1, p. 33).

On July 22, 2008 at 3:40pm, United States Magistrate Judge Howard R. Lloyd signed
a “No-Knock” search warrant approving the N.D.Cal. 08-70460-HRL warrant application.
See id. (Dkt. #566-2). The N.D.Cal. 08-70460-HRL warrant required the government to
search on or before July 31, 2008, and not to exceed ten (10) days, in the daytime from
6:00am to 10:00pm. See id. (Dkt. #566-2, p. 2). In addition to physical effects, the warrant
also authorized seizure of “[a]ll data stored within any and all computer systems, including
any related electronic storage media... [f]or the purpose of searching for items 2-19 below:”
Id. (Dkt. #566-2, p. 6). The search warrant then lists in paragraphs 2-19 the specific subjects
upon which a file must relate in order for the government to seize the file under the warrant.
The search warrant also contains a “Computer Search Protocol For The Northern District Of
California,” wherein the government was required to “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....” and, within
60 days following the search, destroy “copies of any data that are outside the scope of the
warrant but that were copied or accessed during the search process...” Id. (Dkt. #566-2, p.
15-17); see also Argument, Section V(C)(10), infra (analyzing the computer search protocol in detail).

On July 30, 2008, the N.D.Cal. 08-70460-HRL warrant was returned unexecuted to United States Magistrate Judge Patricia V. Trumbull. On July 30, 2008, IRS-CI Agent Fleischmann and AUSA Yen resubmitted amended versions of the original N.D.Cal. 08-70460-HRL search warrant application and affidavit in the Northern District of California. See Submission Of Materials Related To Search Warrant No. 08-70460, Authorized By Magistrate Judge Patricia V. Trumbull, Northern District Of California, On July 30, 2008 (Dkt. #464-2). IRS-CI Agent Fleischmann and AUSA Yen resubmitted the amended documents under the same docket number but this time to Magistrate Judge Trumbull. See id. (Dkt. #464-2). In paragraph 2b of his amended affidavit, IRS-CI Agent Fleischmann stated the following regarding the amended nature of the search warrant application and affidavit:

b. Your affiant previously submitted an affidavit in support of a prior search warrant for the above address (431 El Camino Real; Apartment 1122; Santa Clara, California, 95050). Magistrate Judge Howard R. Lloyd authorized that warrant (# 08-70460 HRL) on July 22, 2008. That warrant has been returned unexecuted due to the ongoing nature of the investigation. This affidavit is substantially the same as the prior affidavit, with the exception of the information added in paragraphs 2b, 2c, 34a and 126, and the additions of items 21 (gold) and 22 (the person of Steven Travis Brawner) in Attachment B.

Id., p. 1-2 (Dkt. #464-2, p. 3-4).

With respect to the additional information added in paragraphs 2c, 34a and 126: (1) paragraph 2c indicates that an indictment and arrest warrant issued on an unspecified date for “Steven Travis Brawner, a.k.a. Travis Rupard, a.k.a Patrick Stout” in case No. CR08-814-PHX-DGC. Id., p. 2 (Dkt. #464-2, p. 3); (2) paragraph 34a provides information regarding a purchase of gold made on May 20, 2008 using a debit card “linked to fraudulent tax refunds.” Id., p. 8-9 (Dkt. #464-2, p. 10-11); (3) paragraph 126 provides information in support of a night-time execution of the warrant and includes: (a) electronic gate key access records indicate that “the individual purporting to be Steven Travis Brawner accessed the domicilio apartment complex sixteen times between June 4, 2008 and July 23, 2008[,]” (b)
“[d]uring the month of July 2008, daytime surveillance and spot check surveillance have not
been able to observe any residents at the location[.]” and (c) “[o]n July 22, 2008, at
approximately 7:20 pm, an FBI Special Agent acting in an undercover capacity knocked on
the door using the ruse of a fast food delivery[,] [n]o one answered the door.” Id., p. 40-41
(Dkt. #464-2, p. 42-43). The remainder of the amended affidavit is the same as the original.

On July 30, 2008 at 2:30pm, Magistrate Judge Trumbull signed a “No-Knock and
night-time” amended search warrant approving the N.D.Cal. 08-70460-HRL amended search
warrant application. See id. (warrant) (Dkt. #464-1, p. 2). The N.D.Cal. 08-70460-HRL
amended warrant required the government to search on or before August 11, 2008, and not to
exceed ten (10) days, at any time of the day or night. See id. (Dkt. #464-1, p. 2). On August
3, 2008 at 5:20pm, the N.D.Cal. 08-70460-HRL amended warrant was executed to physically
search apartment No. 1122 and then later returned to Magistrate Judge Trumbull on August
5, 2008. See id. (return) (Dkt. #464-1, p. 19-24). Other than for authority to conduct a
“night-time” search, the only difference between the amended and original versions of the
warrant is that the reissued version adds (1) “Gold, in any amount[,]” and (2) “The person of
Steven Travis Brawner, a.k.a. Travis Rupard, a.k.a. Patrick Stout[ ]” as items to be seized.[785]
Additionally, both versions of the warrant have identical computer search protocols. See
Argument, Section V(C)(10), infra (analyzing the computer search protocol in detail).

IV. GENERAL FACTS

The proceeding subsections, in conjunction with the defendant's declarations
accompanying this memorandum, set forth general facts in support of the Fourth Amendment
arguments raised in the Argument section of this memorandum (Section V, infra). The
defendant's declarations include (1) declaration RE: Daniel Rigmaiden's residence was at
431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, (2) declaration RE:
Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet
connection, (3) declaration RE: Internet activity reflected by the 1,836,140 aircard

785. See Submission Of Materials Related To Search Warrant No. 08-70460, Authorized
By Magistrate Judge Patricia V. Trumbull, Northern District Of California, On July 30,
2008 (warrant) (Dkt. #464-1, p. 14).
destination IP addresses seized by the government, and (4) declaration RE: Data extracted from hard drive images corresponding to seized hard drives connected to Daniel Rigmaiden's home computer. The noted declarations should be referenced for information on apartment No. 1122, the aircard, and the host laptop computer prior to continuing further with this section. In support of the factual claims outlined in the subsections immediately below, the defendant cites to his declarations, case discovery, and public sources of information—most of which is provided through a series of 168 separate exhibits.[786] The Procedural History (Section III, supra) and the Technical Explanations (Section II, infra) are also directly referenced in support of the General Facts. An overall factual introduction is contained in the Introduction section of this memorandum (Section I, supra).

A. Prerequisite background information.

1. General background information on the aircard, host laptop computer, aircard account, and aircard service.

   1. The aircard[787] is a “UTStarcom PC5740 Broadband Connection Card For Verizon Wireless”[788] purchased by the defendant from a Verizon Wireless store using his own physical cash.[789] The aircard was used by the defendant to access his monthly billed Verizon Wireless 1xEV-DO “BroadbandAccess Connect Service” account opened in person.

---

786. In support of this memorandum and accompanying motion, the defendant has submitted (1) First Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues (hereafter “1st Consolidated Exhibits”) (Dkt. #587), and (2) Second Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues (hereafter “2nd Consolidated Exhibits”) (Dkt. #821). Both 1st Consolidated Exhibits and 2nd Consolidated Exhibits, including all attachments, are hereby incorporated into this motion by reference pursuant LRCiv 7.1(d)(2) when referenced through LRCrim 12.1.

787. The government's filings relating to the D.Ariz. 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV applications and court orders, and the N.D.Cal. 08-90330MISC-RS and 08-90331MISC-RS applications and court orders, interchangeably refer to the aircard as the “Target Device,” “target broadband access card,” “Target Broadband Access Card/Cellular Telephone,” “telephone,” and other similar terms.

788. See Procedural History, Section III(A), supra, (D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615 produced identifying information on the aircard); EXHIBIT 11 of 1st Consolidated Exhibits (Dkt. #587-1) (government web research on aircard).

789. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 2, p. 1-2.
by the defendant under his alias of Travis Rupard. The aircard account allowed for accessing the Internet through the Verizon Wireless cellular data network, which is based on the cdma2000 1xEV-DO Rel. 0 technical standards, and also had an SMS text message service based on the cdma2000 1xRTT technical standards. The associated aircard account did not have cellular telephone service.

2. The aircard is a cellular device that transmits and receives Internet data and text messages (i.e., electronic communications) through a radio transceiver and antenna contained in the device. Specifically, the aircard is a High Rate Packet Data (HRPD) 1xEV-DO Rel. 0 Access Terminal with hybrid 1xRTT text message service and low rate data service capabilities. The aircard hardware is incapable of ringing or alerting to an incoming call and it does not allow for placing or receiving telephone calls (i.e., wire communications).

Unlike cellular telephones that have built into their hardware “a compact speaker, a microphone, a keyboard, [and] a display screen...,” the aircard is a cellular device that transmits and receives Internet data and text messages through a radio transceiver and antenna contained in the device. Specifically, the aircard is a High Rate Packet Data (HRPD) 1xEV-DO Rel. 0 Access Terminal with hybrid 1xRTT text message service and low rate data service capabilities. The aircard hardware is incapable of ringing or alerting to an incoming call and it does not allow for placing or receiving telephone calls (i.e., wire communications).
personal computer hardware “add-on card” that can only function when plugged into the
PCMCIA slot of a host laptop computer.\footnote{799}

3. The host laptop computer used by the defendant with his aircard was an IBM
ThinkPad (S/N #LV-C4398) laptop computer (hereafter “host laptop computer” or “home
computer”) with mouse, docking station, external LCD monitor, external keyboard, and
external hard drives.\footnote{800}\footnote{801} In order to function, the aircard drew power from the host
laptop computer, stored data on the hard drive of the host laptop computer, and its functions
and operations were accessed through software installed on the host laptop computer.\footnote{802}

4. Whenever the aircard was plugged into the host laptop computer, the defendant
would immediately initiate a connection with Verizon Wireless and take measures to ensure
that his connection would reconnect upon a disconnect.\footnote{803} In order to connect to Verizon
Wireless and access the Internet, the defendant would use either his operating system
software compatible with the aircard or the VZAccess Manager software bundled with the
aircard.\footnote{804} While accessing the Internet, radio waves were transmitted to/from the aircard
and the cell sites that were part of the Verizon Wireless 1xEV-DO Rel. 0 data network.\footnote{805}
The radio waves sent between the aircard and the Verizon Wireless 1xEV-DO Rel. 0 data
network carried the signals that communicated data between the host laptop computer and

\footnote{799}{See EXHIBIT 11 of 1st Consolidated Exhibits (Dkt. #587-1) (government web
research on aircard).}

\footnote{800}{See Submission Of Materials Related To Search Warrant No. 08-70460, Authorized
By Magistrate Judge Patricia V. Trumbull, Northern District Of California, On July 30,
2008 (return) (Dkt. #464-1).}

\footnote{801}{See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden
owns the aircard and used the aircard service as a home Internet connection, ¶ 4, p. 2-3.}

\footnote{802}{See EXHIBIT 11 of 1st Consolidated Exhibits (Dkt. #587-1) (government web
research on aircard indicating that the aircard is bundled with VZAccess Manager software);
see also defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden
owns the aircard and used the aircard service as a home Internet connection, ¶ 17, p. 6-7.}

\footnote{803}{See id., ¶ 17-20, p. 6-7.}

\footnote{804}{See id., ¶ 17, p. 6-7.}

\footnote{805}{See Technical Explanations, Section II(B) et seq., supra (explaining aspects of a
1xEV-DO Rel. 0 cellular data network).}
2. Basis for concluding that the government used the Harris StingRay, KingFish, and related equipment to locate the aircard and the defendant.

   a. The government admitted that FBI technical agents used the Harris StingRay to locate the aircard.

      5. The government refuses to disclose detailed discovery to the defense relating to the portable/transportable wireless device locators used to locate the aircard. Likewise, the Court refuses to order the government to produce the evidence sought by the defendant. [807]

      However, the government has already identified one piece of equipment used to locate the aircard: the StingRay manufactured by Harris. [808][809] In a report of investigation disclosed to the defense, USPIS Inspector James L. Wilson stated that FBI technical agents were “using a 'Stingray' to pinpoint the location of the aircard.” [810] Furthermore, in rough notes disclosed to the defense, IRS-CI Agent Denise L. Medrano created a “to-do list” containing the “StingRay” term in Case-CoRrEcT fashion. [811][812]

806. See id.

807. See January 4, 2012 Court Order (Dkt. #723, p. 13) (Denying the defendant's motion for disclosure (Dkt. #592) and noting that “[d]isclosing 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.”).

808. See Technical Explanations, Section II(G) et seq., supra (explaining technical details of the Harris StingRay).

809. Even if the government used portable/transportable wireless device locators that were not the Harris products, the operations of the actual devices used will be similar to the operations of the Harris products. For example, any portable/transportable wireless device locator seeking to locate a 1xEV-DO Rel. 0 wireless device in cell site emulator mode must follow all of the procedures outlined in the Technical Explanations, Sections II(B) et seq., supra (addressing the 1xEV-DO Rel. 0 communications protocol). Additionally, geolocation of radio frequency signals discussed in the Technical Explanations is a well defined science.

810. EXHIBIT 26 of 1st Consolidated Exhibits (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson) (emphasis added).

811. See EXHIBIT 109 of 2nd Consolidated Exhibits (Dkt. #821-6) (July 15, 2008 rough notes by IRS-CI Agent Medrano).

812. Harris spells “StingRay” with a capital “S” and a capital “R” in the same way IRS-CI Agent Medrano used the term on her list. IRS-CI Agent Medrano did not use such capital spelling style for any other listed phrase.
6. After realizing that use of the Harris StingRay was revealed to the defendant, AUSA Battista sought to cover up this government mistake by claiming, without any evidence whatsoever, that the term “StingRay” is a generic term used by law enforcement to refer to any type of surveillance equipment capable of locating wireless devices.[813][814] AUSA Battista specifically claimed that USPIS Inspector Wilson and IRS-CI Agent Medrano used the term “StingRay” generically and supported his claim with a false statement[815] that the primary case agents neither saw nor learned of the equipment used to locate the aircard.

813. The government made this claim via AUSA Battista during the September 22, 2011 court hearing:

    MR. BATTISTA: I've sought to explain to Mr. Rigmaiden, and the example I use, and I talked about this case so many times, is Kleenex and tissue. Kleenex is a brand name but it's a tissue. People regularly refer to tissue as Kleenex. “I need to blow my nose. Will you give me a Kleenex?” Everyone knows what they're talking about.

    In the law enforcement world, there's a StingRay and then there's the generic term “StingRay” meaning all types of devices. The five case agents were using the term “StingRay” as the term “Kleenex.” They did not operate the equipment. They did not know what the equipment is. They didn't receive any training on the equipment.


814. Contrary to AUSA Batista's claim, a government document produced via a FOIA request does not list “StingRay” as one of the many generic terms used to refer to portable/transportable wireless device locators (i.e., cell site emulators). See USDOJ [M.D.La.] Aug. 12, 2008, Response to ACLU FOIA Request No. 07-4130, p. 18 of 42 (listing “digital analyzer, cell site locator, triggerfish, ESN reader, or swamp box” as generic terms used to refer to cell site simulators); see also EXHIBIT 021 of 2nd Consolidated Exhibits (Dkt. #821-1) (relevant pages of cellfoia_release_074130_20080812.pdf attached with page numbers added).

815. In this context, the term “false statement” means that the information provided by AUSA Battista was/is false but it does not necessarily imply that AUSA Battista knew the information was false. Nevertheless, the government as a single entity knew the information was false.

816. The false statement made by AUSA Battista during the September 22, 2011 court hearing is as follows:

    So they were -- in the course of the investigation, the term “StingRay” was used as a generic term. I've explained this to the defendant numerous times. None of the five investigators know the make, model, manufacturer of the exact equipment. There were tech agents out there. They're the ones who possessed the equipment, operated the equipment.
7. Contrary to AUSA Battista's false statement, FBI Agent Murray (a primary case agent) stated in two “case write ups” that he conducted a test with the IRS involving the geolocation of a similar aircard prior to FBI technical agents locating the actual aircard:

I worked with the AUSA and the FBI SF to obtain a pen register and tracking court order to locate the aircard with TTA [(i.e., FBI Technically Trained Agent)] assistance. I ran a field test with IRS of a similar aircard and communicated with OTD to ensure that the tracking would not be detected by the subject.

See EXHIBIT 065 of 2nd Consolidated Exhibits (Dkt. #821-3) (Feb. 28, 2009 “case write up” by FBI Agent Murray).

The above quoted “case write up” is corroborated by a text message sent by FBI Agent Murray to FBI Agent Kevin F. Killigrew on July 16, 2008 at 1:46am.[817] Because the primary case agents were aware of the precise make and model of the equipment used, the references in the discovery to the StingRay refer to the Harris StingRay.

b. Heuristics and process of elimination confirms that FBI technical agents used the Harris StingRay, KingFish and AmberJack to locate the aircard.

8. FBI Supervisory Agent Bradley S. Morrison confirmed that the “equipment used to locate the defendant's aircard did not capture, collect, decode, view, or otherwise obtain any content transmitted from the aircard, and therefore was unable to pass any of this information from the aircard to Verizon Wireless [(i.e., no communication interception)].”[818][819] The prosecution thereafter stated that the equipment used to locate

So, yes, the word “StingRay” is in the discovery. When they're using the term “StingRay,” and I've explained this to the defendant, it's Kleenex. It's tissue. They don't know. It could be a StingRay. It could not be. It could be something else. They didn't know what it was. They didn't see it. They didn't operate it.


[817] See EXHIBIT 063 of 2nd Consolidated Exhibits (Dkt. #821-3) (July 16, 2008, 1:46am, text message sent from FBI Agent Murray to FBI Agent Killigrew: “We verified the ability to pull the card over through testing on an irs verizon card. Atech agent from [REDACTED: TTA First Name], is here helping out and he has top game.”).


[819] The defendant does not agree with any other claims made by FBI Agent Morrison. The remainder of FBI Agent Morrison's claims are technically incorrect as indicated by the
the aircard was simply **incapable** of intercepting and forwarding aircard communications content.\[820\] Through process of elimination, the surveillance equipment used to locate the aircard must be limited to solely having geolocation capabilities. While there are numerous air interface surveillance devices available from various manufacturers, only Altron, NeoSoft, MMI, and Harris manufacture devices specifically designed to not have the ability to intercept communications and conduct man-in-the-middle attacks.\[821\]

9. Through further process of elimination, the only possible manufacturer of the equipment used to locate the aircard is Harris. It is undisputed that in order to “track the signals from the aircard, the FBI used [][equipment] that functions as a cell site simulator. The equipment mimicked a Verizon Wireless cell tower and sent and received signals directly to and from the aircard.”\[822\] It is also undisputed that the aircard is a cdma2000 based wireless device, *i.e.*, compatible with the 1xEV-DO Rel. 0 and 1xRTT air interface standards.\[823\] Out of all cell site emulator capable air interface surveillance equipment sold by Altron, NeoSoft, MMI, Harris, Ability, Meganet, Shoghi Communications Ltd., Verint, and View Systems—only the Harris StingRay and KingFish support cdma2000 based air interface standards (*e.g.*, 1xEV-DO Rel. 0 and 1xRTT as used by the aircard).\[824\] Through process of elimination, the only portable/transportable wireless device locators that are technologically capable of locating the aircard are the Harris StingRay and KingFish.

defendant's *Technical Explanations*, Section II *et seq.*, *supra.*

820. *See EXHIBIT 071* of 2nd *Consolidated Exhibits* (Dkt. #821-4) (December 2, 2011 letter from AUSA Battista to the defendant, p. 2: “[T]he FBI equipment used in your case could not be used to conduct a 'man in the middle' attack.”).

821. *See Technical Explanations*, Section II(G), *supra* (explaining how technical data on air interface surveillance equipment manufactured by Ability, Meganet, Shoghi Communications Ltd., Verint, and View Systems indicate an ability to conduct man-in-the-middle attacks while technical data on certain models of air interface surveillance equipment manufactured by Altron, NeoSoft, MMI, and Harris indicate no such capabilities).

822. *Government's Response To Motion For Discovery* (Dkt. #602, p. 3).

823. *See General Facts*, Section IV(A)(1), *supra* (explaining how the aircard communicates with the Verizon Wireless 1xEV-DO Rel. 0 and 1xRTT cellular networks).

824. *See Technical Explanations*, Section II(G), *supra* (other than for Harris equipment, all off-the-shelf cell site emulator capable air interface surveillance devices only support surveillance of UMTS and/or GSM based wireless devices).
10. The government also effectively conceded that the FBI used two separate wireless device locators to locate the aircard. The government stated that “[t]he FBI used the [locating] equipment in multiple locations... [but] it never used more than a single piece of equipment at any given time.”[^825^] It logically follows that the government’s concession means that the FBI used more than one device but not at the same time. Additionally, the government conceded that “[d]uring a portion of the tracking operation, the FBI used handheld equipment from within the Domicilio apartment complex.”[^826^] Although the FBI initially used the StingRay, it is designed to be transportable via a land or air vehicle;[^827^] therefore, the FBI needed to use a second, handheld wireless device locator while on foot within the Domicilio apartment complex. The Harris KingFish is the only handheld man-portable wireless device locator that operates in cooperation with the Harris StingRay.[^828^] It logically follows that the FBI would use the KingFish along with the StingRay, as opposed to using a handheld device not designed for cooperative operation with the StingRay.

11. The standard antenna used with the StingRay is the AmberJack phased array beam-forming antenna.[^829^] The datasheet for the StingRay indicates that it operates with the AmberJack[^830^] and the datasheet for the AmberJack indicates that it operates with the StingRay.[^831^] Because the AmberJack is the standard antenna used with the StingRay, and because the FBI technical agents used the StingRay to locate the aircard, they also used the AmberJack to locate the aircard.

[^825^]: Government’s Response To Motion For Discovery (Dkt. #602, p. 3).
[^826^]: Id.
[^827^]: See Technical Explanations, Section II(G)(1), supra (explaining how the StingRay is vehicle-transportable as apposed to man-portable).
[^828^]: See id., Section II(G), supra.
[^829^]: See id., Section II(G)(1)(a)(iii), supra (explaining the AmberJack phased array beam-forming antenna used with the StingRay).
[^830^]: See Miami, FL, USA – Legislative Files, Harris StingRay Product Datasheet, p. 1; see also EXHIBIT 003 of 2nd Consolidated Exhibits (Dkt. #821-1) (datasheet attached).
[^831^]: See Miami, FL, USA – Legislative Files, Harris AmberJack Product Datasheet, p. 6-7; see also EXHIBIT 011 of 2nd Consolidated Exhibits (Dkt. #821-1) (AmberJack datasheet attached).
B. The government's mission to locate the aircard and the defendant within his private home residence.

1. The government identified the aircard and seized destination IP addresses relating to the defendant's Internet activity.

12. Based on an unrelated aspect of the investigation, the government identified Verizon Wireless network IP addresses 75.209.101.132, 75.208.105.186, and 75.209.41.104 as being possible end-source IP addresses responsible for submitting three of the allegedly fraudulent e-filed tax returns. In June of 2008, the government served Verizon Wireless with D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615 requesting identifying information on the customer account and wireless device assigned the three source IP addresses noted above.

13. On June 13, 2008, Verizon Wireless responded to the government's request and provided identifying information on the defendant's aircard and aircard account. In the subpoena response, Verizon Wireless also provided the government with approximately 411,257 destination IP addresses pertaining to websites and other Internet resources accessed by the defendant via the aircard. A sample of the destination IP addresses resolved to their respective website URLs is attached to the defendant's declaration accompanying this memorandum RE: Internet activity reflected by the 1,836,140 aircard destination IP addresses seized by the government.

14. By June 25, 2008, the government had matched up a list of IP addresses associated with various e-filed tax returns to some of the defendant's destination IP addresses.

---

832. See EXHIBIT 065 of 2nd Consolidated Exhibits (Dkt. #821-3) (“[T]hrough separate investigative means, [FBI Agent Murray] and other agents analyzed ISP IP records and identified the Internet aircard used by the subject...”).


834. See id.

835. Although agents obtained identifying information for the aircard and aircard account, they were unable to determine the defendant's true identity and home address based off of the account records alone—hence the need for the aircard locating mission.

836. See id.

837. On June 18, 2008, the government obtained an additional 111 aircard destination IP addresses accessed by the defendant using the aircard. See id.
listed in the Verizon Wireless subpoena responses. Based on the match up, the
government was convinced that the aircard was responsible for perpetuating the alleged
scheme. On July 1, 2008, the government began to prepare and execute plans to use
historical cell site location information, real-time cell site location information, and Harris
brand portable/transportable wireless device locators to “ping and triangulate on a cellular
broadband card we are 99% sure is him.”

15. After investigators had relied upon the destination IP addresses to investigate
the defendant for a period of 26 days, AUSA Battista learned that it was illegal for the
government to use Grand Jury subpoenas to compel disclosure of the defendant's destination
IP addresses and that subpoenas only allow for disclosure of source IP addresses. On
July 8, 2008, AUSA Battista instructed the investigation team to place all aircard destination
IP addresses into sealed envelopes and then subsequently applied for a “retroactive

838. See EXHIBIT 078 of 2nd Consolidated Exhibits (Dkt. #821-4) (June 25, 2008 email
from IRS-CI Agent Daun to FBI Agent Murray et al.: “based on the pattern following along
for just all of the Ips that I found to match - I really think this is the person filing the
returns...”). See also EXHIBIT 14 of 1st Consolidated Exhibits (Dkt. #587-1) (July 1, 2008
e-mail from IRS-CI Agent Daun to Nathan A. Watt: “We have correlated returns being filed
from specific Proxy Ips, that this guy was also connected to at the same time.”); EXHIBIT
15 of 1st Consolidated Exhibits (Dkt. #587-1) (July 7, 2008 email from IRS-CI Agent
Medrano to Constance M. Davis: “We strongly believe we have identified the []
suspect...”).

839. See Submission Of Documents Related To Original Northern District Of California
08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122, Application,
p. 17-25 (Dkt. #566-1, p. 19-27) (explaining government's use of the aircard destination IP
addresses to link aircard to e-filed tax returns).

840. EXHIBIT 14 of 1st Consolidated Exhibits (Dkt. #587-1) (July 1, 2008 email from IRS-
CI Agent Daun to Nathan A. Watt); see also EXHIBIT 16 of 1st Consolidated Exhibits (Dkt.
#587-1) (July 7, 2008 email from IRS-CI Agent Daun to IRS-CI Agent Willert: the FBI plans
to “triangulate down on the [][suspect's] broadband access card with Verizon in San Jose.”).

841. The government was unable to identify or locate the defendant based on the aircard
account records alone—hence the need for the aircard locating mission.

842. See 18 U.S.C. § 2703(c)(2) et seq. (allowing the government to obtain “records of
session times and durations” and “any temporarily assigned network address” but not
destination IP addresses).

843. See EXHIBIT 17 of 1st Consolidated Exhibits (Dkt. #587-1) (on July 7, 2008, USDOJ
Office of Enforcement Operations notified AUSA Battista of an “issue” with the aircard
destination IP addresses); see also Procedural History, Section III(B), supra, (discussing
procedural aspects of D.Ariz. 08-3286MB-LOA court order).

844. See EXHIBIT 18 of 1st Consolidated Exhibits (Dkt. #587-2) (July 8, 2008 email from
AUSA Battista to all primary case agents: “Please place[] in a sealed envelope all copies of
order” to unseal the envelopes. On July 9, 2008, the “retroactive order” was granted and the government then continued with its plan to use various geolocation techniques to obtain the precise location of the aircard and the defendant.

2. The government seized aircard historical cell site location information and conducted historical triangulation / location signature techniques.

16. In July of 2008, the government served Verizon Wireless with the D.Ariz. 08-3298MB-LOA order requesting historical cell site information relating to connections made by the aircard to Verizon Wireless cell sites. On July 12, 2008, Verizon Wireless responded to the D.Ariz. 08-3298MB-LOA order by emailing Robert Byrne, LEO, and FBI Agent Murray historical cell site information pertaining to the aircard and generated during the date range of June 10, 2008 through July 11, 2008.

17. Although the order only authorized obtaining historical cell site information to determine the network's registration of the aircard, the government obtained historical cell site location information showing the network's geographical location of the aircard, i.e., locations of cell sites where the aircard established sessions with the 1xEV-DO Rel. 0 cellular data network. The information provided by Verizon Wireless indicated that the aircard had been historically located within signal range of the following cell sites:

   (1) Cell site # 5; Latitude: 37.369733; Longitude: -121.923442; Street address: 2001...
Gateway Place, San Jose, CA 95110;

(2) Cell site # 139; Latitude: 37.34955; Longitude: -121.943435; Street address: 900 Lafayette St, Santa Clara, CA 95050;

(3) Cell site # 153; Latitude: 37.418053; Longitude: -121.85978; Street address: 10000 Old Piedmont Rd., San Jose, CA 95132;

(4) Cell site # 268; Latitude: 37.346481; Longitude: -121.923164; Street address: 1070 Elm St, San Jose, CA 95126;

(5) Cell site # 279; Latitude: 37.3416; Longitude: -121.947941; Street Address: 490 Lincoln St., Santa Clara, CA 95050;

The historical cell site location information allowed the government to determine that the aircard was previously located within signal range of five cell sites covering parts of San Jose and Santa Clara, CA.[851][852]

18. As explained in the Technical Explanations, Section II(B)(3)(c)(vi), supra,[853] 1xEV-DO Rel. 0 wireless devices such as the aircard do not “register” with cell sites (i.e., Access Networks)—instead, they establish “sessions”[854] and conduct “route updates”[855] with both operations being associated with the IPv6 address identifying the cell site sector. 1xEV-DO Rel. 0 registration occurs separate from cell sites, over the A11 Interface, and does not involve location information as may be relevant to “registration” in the context of GSM

851. See EXHIBIT 20 of 1st Consolidated Exhibits (Dkt. #587-2) (July 14, 2008 email from AUSA Battista to AUSA Yen: the government is looking for the aircard in the area of San Jose International Airport and Santa Clara University).

852. On July 31, 2008, Verizon Wireless responded to the D.Ariz. 08-7273MB-LOA order by providing similar aircard historical cell site location information generated during the date range of June 11, 2008 through July 17, 2008. See EXHIBIT 05 of 1st Consolidated Exhibits (Dkt. #587-1); see also Procedural History, Section III(D), supra (discussing procedural aspects of D.Ariz. 08-7273MB-LOA historical cell site information order). Additionally, On August 1, 2008, John Profaca provided a second set of cell site information in response to a direct request made by FBI Agent Murray under the authority of the D.Ariz. 08-3298MB-LOA order. See Procedural History, Section III(C), supra (discussing procedural aspects of D.Ariz. 08-3298MB-LOA historical cell site information order). The defendant is seeking suppression of all historical cell site location information—regardless of when or how it was obtained.

853. See also fn. No. 343, supra.

854. See Technical Explanations, Section II(B)(3)(c)(iii), supra.

855. See id., Section II(B)(3)(d) et seq., supra.
and other non IP based mobile networks.\[856\]

19. As an initial matter, the historical cell site location information provided by Verizon Wireless allowed the government to determine that the aircard was in a stationary location from June 10, 2008 to July 11, 2008.\[857\]

20. On the morning of July 14, 2008,\[858\] FBI Agent Killigrew created a cell tower range chart/map consisting of a street map, plotted Verizon Wireless cell site sectors belonging to cell site Nos. 268, 139, and 279, and a triangulated aircard location signature estimate represented by a shaded area.\[859\] On the chart/map, the total land area collectively covered by cell site Nos. 268, 139, and 279 is approximately 105,789,264 \(\text{ft}^2\).\[860\] FBI Agent Killigrew used triangulation techniques and location signature techniques to eliminate 93.9% of that 105,789,264 \(\text{ft}^2\) area resulting in the location estimate being reduced to 6,412,224 \(\text{ft}^2\) represented by the shaded area. The shaded area on the cell tower range chart covers the location of apartment No. 1122 at the Domicilio apartment complex.\[861\]

21. FBI Agent Killigrew's triangulation techniques and location signature

---

\[856\] See id., Section II(B)(3)(c)(vi) and fn. No. 343, supra.

\[857\] See EXHIBIT 35 of 1st Consolidated Exhibits (Dkt. #587-3) (IRS-CI Agent Medrano rough notes stating that the aircard was accessing the “same tower in San Jose 90% [of the time]” and it “appears not moving[,]”); EXHIBIT 20 of 1st Consolidated Exhibits (Dkt. #587-2) (July 14, 2008 email from AUSA Battista to AUSA Yen: “the initial Cell Site data” has the government “looking at the area around San Jose International Airport and Santa Clara University.”).

\[858\] See EXHIBIT 068 of 2nd Consolidated Exhibits (Dkt. #821-3) (May 2, 2011 letter from AUSA Battista to the defendant, p. 5: “[P]lease be advised that it appears that the cell tower range chart was created the morning of July 14, 2008, and then shared with the investigation team after 1:00 p.m. that same date.”).

\[859\] See EXHIBIT 21 of 1st Consolidated Exhibits (Dkt. #587-2) (cell tower range chart/map showing a 6,412,224 \(\text{ft}^2\) triangulated location signature estimate (marked with black pen lines) covering the location of apartment No. 1122); EXHIBIT 22 of 1st Consolidated Exhibits (Dkt. #587-2) (cell tower range chart/map with government's 6,412,224 \(\text{ft}^2\) triangulated location signature estimate marked in red and apartment No. 1122 marked with a yellow star).

\[860\] See 1st Consolidated Exhibits (Dkt. #587-2) (mathematical equation information for calculating the square footage of overlapping signal coverage areas of multiple cell sites and cell site sectors).

\[861\] See EXHIBIT 22 of 1st Consolidated Exhibits (Dkt. #587-2) (cell tower range chart/map with government's 6,412,224 \(\text{ft}^2\) triangulated location signature estimate marked in red and apartment No. 1122 marked with a yellow star).
techniques consisted of the following steps: (1) obtaining aircard historical cell site location information for June 10, 2008 through July 11, 2008, (2) using the latitude and longitude coordinates of three of the five cell sites (cell site Nos. 268, 139, and 279) contained in the historical cell site location information to plot the cell site locations on a digital/computerized street map, (3) using prior knowledge of Verizon Wireless cell site signal ranges (i.e., antenna radiation patterns) to draw signal range circles around each of the three cell site locations plotted on the digital/computerized street map, (4) using prior knowledge of typical Verizon Wireless cell site sector orientations (i.e., sector azimuths at 0°, 120°, and 240° with sector radiation patterns covering 300°-60°, 60°-180°, and 180°-300°) to draw lines separating each of the noted signal range circles into three sectors each, (5) using the historical cell site location information to calculate which two cell sites were being accessed by the aircard most often (i.e., cell site Nos. 268 and 139) and then weighting the respective signal range circle of the remaining cell site (i.e., cell site No. 279) with a

---

1. See EXHIBIT 25 of 1st Consolidated Exhibits (Dkt. #587-2) (January 7, 2011 email from FBI Agent Killigrew to FBI Agent Murray: FBI Agent Killigrew indicating that he “took the historical cell site data that the cellular provider provided to [[FBI Agent Murray]] in order to create the cell tower range chart/map.”).

2. See id. (January 7, 2011 email from FBI Agent Killigrew to FBI Agent Murray: “The historical data provided several cell towers with their latitude and longitude. I plotted these on the map by lat/lon.”).

3. See EXHIBIT 068 of 2nd Consolidated Exhibits (Dkt. #821-3) (May 2, 2011 letter from AUSA Battista to the defendant, p. 5: AUSA Battista indicating that FBI Agent Killigrew informed FBI Agent Murray on March 31, 2011 that, “For this particular case I used my knowledge of Verizon wireless cell tower layouts from working previous cases and previous training.”).

4. See id. (May 2, 2011 letter from AUSA Battista to the defendant, p. 5: AUSA Battista indicating that FBI Agent Killigrew informed FBI Agent Murray on March 31, 2011 that, “Generally speaking, in urban areas Verizon Azimuths are 0, 120, and 240 degrees. The sectors then encompass 300-60, 60-180, and 180-300.”).

5. See EXHIBIT 25 of 1st Consolidated Exhibits (Dkt. #587-2) (January 7, 2011 email from FBI Agent Killigrew to FBI Agent Murray: “After the towers were plotted, using my past experience and training in dealing with cellular networks, I drew circles around the towers that provided for overlapping areas of cellular coverage.”).

6. See EXHIBIT 02 of 1st Consolidated Exhibits (Dkt. #587-1) (historical cell site location information showing that the aircard was accessing cell site Nos. 268 and 139 most often); EXHIBIT 25 of 1st Consolidated Exhibits (Dkt. #587-2) (January 7, 2011 email from FBI Agent Killigrew to FBI Agent Murray: “The tower data provided by the wireless company showed that three towers were hit most often, with one of the three hit significantly more often than the other two.”).
confidence value of -1 (i.e., the aircard is absolutely NOT in the estimated area),\[868\] (6)
using the digital/computerized street map to calculate an overlapping signal range area for
the two cell sites used by the aircard most often (i.e., cell site Nos. 268 and 139),\[869\] (7)
using the digital/computerized street map to calculate the three overlapping sector regions
within the overlapping signal range area described in No. 6 above,\[870\] (8) weighting two of
the noted three overlapping sector regions covering non residential areas (i.e., the airport as
shown on the noted cell tower range chart/map) with a confidence value of -1 (i.e.,
absolutely NOT containing the location of the aircard),\[871\] and (9) weighting the remaining
overlapping sector region (i.e., the shaded area on the cell tower range chart/map) with a
confidence value of 1 (i.e., the aircard is absolutely within the corresponding estimated area).
\[872\] The shaded area on the cell tower range chart/map represents a government
triangulated aircard location signature based off of the above explained geolocation
techniques.

22. FBI Agent Killigrew's geolocation techniques fit the definition of cell site
triangulation as explained by Judge Kaplan.\[873\] For the triangulation calculation

---

868. See EXHIBIT 22 of 1\textsuperscript{st} Consolidated Exhibits (Dkt. #587-2) (labeled cell tower range chart/map showing nearly no shade lines over sector signal coverage area belonging to cell site No. 279).

869. See id. (labeled cell tower range chart/map showing cell site Nos. 268 and 139 having signal coverage areas overlapping).

870. See id. (labeled cell tower range chart/map showing overlapping sectors from cell site Nos. 268 and 139 creating three separate overlapping sector regions).

871. See id. (labeled cell tower range chart/map showing no shade lines over sectors from cell site Nos. 268 and 139 that cover the airport); see also EXHIBIT 070 of 2\textsuperscript{nd} Consolidated Exhibits (Dkt. #821-4) (June 18, 2010 letter from AUSA Battista to the defendant, p. 4-5: “The three circles represent estimates of the range of the noted cell towers taking into consideration multiple factors, primarily the distance between the towers and the terrain.” (emphasis added)).

872. See EXHIBIT 21 of 1\textsuperscript{st} Consolidated Exhibits (Dkt. #587-2) (cell tower range chart/map showing a 6,412,224 ft\textsuperscript{2} triangulated location signature estimate (marked with black pen lines) covering the location of apartment No. 1122); EXHIBIT 22 of 1\textsuperscript{st} Consolidated Exhibits (Dkt. #587-2) (cell tower range chart/map with government's 6,412,224 ft\textsuperscript{2} triangulated location signature estimate marked in red and apartment No. 1122 marked with a yellow star).

873. See Technical Explanations, Section II(D)(3), supra (“In the context of cell site information, the two known points are the antenna towers, the third point is the cellular telephone, and the direction from each tower to the phone is discerned from the information..."
represented by the shaded area on the cell tower range chart/map, the two known points are cell sites No. 139 and 268, the third unknown point is the aircard, and the south-east sector of cell site No. 139 and the south-west sector of cell site No. 268 are the angles used to complete the equation. [874]

23. FBI Agent Killigrew's geolocation techniques also fit the definition of a location signature calculation using a statistical database containing historical cell site location information and heuristics similar to what is explained by inventors of location signature technology. [875] The statistical database used by FBI Agent Killigrew was the aircard's historical cell site location information (seized from Verizon Wireless) covering the date range of June 10, 2008 through July 11, 2008. FBI Agent Killigrew's location signature techniques allowed for determining (1) the precise cell site sectors accessed by the aircard for use in the triangulation calculation, [876] (2) the specific regions within those sectors accessed by the aircard (e.g., elimination of the terrain covering the airport), [877] and (3) confirmation that the aircard remained in a stationary position over time.

3. The primary case agents flew from Arizona to California to triangulate the precise location of the aircard and the defendant.

24. On July 15, 2008, one day after receiving FBI Agent Killigrew's triangulated aircard location signature estimate, [878] FBI Agent Murray, IRS-CI Agent Medrano, IRS-CI about which face of each tower is facing the phone.” (quoting district Judge Kaplan)).

874. See EXHIBIT 22 of 1st Consolidated Exhibits (Dkt. #587-2) (labeled cell tower range chart/map).

875. See Technical Explanations, Section II(D)(3), supra (explaining location signature techniques that take into consideration the terrain, historical cell site location information, weighting of data for confidence values, etc. to separate cell site sectors into regions for location signatures).

876. Verizon Wireless only provided the cell sites accessed by the aircard and not the cell site sectors. Through location signature techniques, FBI Agent Killigrew was able to determine the precise sectors accessed by the aircard so that a triangulation calculation could be conducted.

877. See EXHIBIT 22 of 1st Consolidated Exhibits (Dkt. #587-2) (labeled cell tower range chart/map showing no shade lines over sectors from cell site Nos. 268 and 139 that cover the airport).

878. See EXHIBIT 068 of 2nd Consolidated Exhibits (Dkt. #821-3) (May 2, 2011 letter from AUSA Battista to the defendant, p. 5: “[P]lease be advised that it appears that the cell
Agent Fleischmann, IRS-CI Agent Tracy L. Daun, and USPIS Inspector Wilson (previously and hereafter collectively the “primary case agents”) “flew to Santa Clara/San Jose to start triangulating the suspect's position.”

Upon their arrival, the primary case agents met with FBI Agent Ng at the Campbell FBI field office and later “met with several FBI agents with their Technical Service Division to help [them] track the suspect's aircard.”

25. While in California, the primary case agents employed the help of three FBI technical agents from San Francisco to conduct the real-time portion of the aircard locating mission. The FBI technical agents were members of a Wireless Intercept and Tracking Team (WITT), which uses aspects of the FBI Digital Collection Program to locate wireless devices. The prosecution has not provided the defense with the identities of three FBI technical agents.

4. The FBI technical agents began the real-time portion of the aircard locating mission by conducting base station surveys of all cell sites located in the area covered by the cell tower range chart.

26. Prior to the real-time portion of the aircard locating mission, the FBI technical tower range chart was created the morning of July 14, 2008, and then shared with the investigation team after 1:00 p.m. that same date.”

879. EXHIBIT 26 of 1st Consolidated Exhibits (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson).

880. Id.

881. See EXHIBIT 073 of 2nd Consolidated Exhibits (Dkt. #821-4) (December 16, 2011 letter from AUSA Battista to the defendant, p. 1: AUSA Battista making reference to “two of the three tech agents…”).

882. See EXHIBIT 065 of 2nd Consolidated Exhibits (Dkt. #821-3) (Feb. 28, 2009 “case write up” by FBI Agent Murray indicating that he “worked with the AUSA and the FBI SF to obtain a pen register and tracking court order to locate the aircard with TTA assistance.” (emphasis added); EXHIBIT 066 of 2nd Consolidated Exhibits (Dkt. #821-3) (FBI technical agent memorandum stating that “Phoenix Division requested assistance from San Francisco in locating a target wireless aircard.”).


884. See Technical Explanations, Section II(H)(8), supra (explaining FBI WITT).

885. See January 4, 2012 Court Order (Dkt. #723, p. 12) (The Court denied the defendant's motion for disclosure (Dkt. #592) and concluded that “[d]isclosures 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.”).
agents loaded CDMA communications protocol firmware onto their StingRay and KingFish (if not loaded previously).[886][887] The firmware is provided by Harris[888] and was loaded onto the FBI's devices so that they would be able to send and receive signals to/from the aircard using the CDMA based 1xEV-DO Rel. 0 communications protocol.[889] Once the firmware was loaded onto the FBI's devices, the technical agents were ready to conduct the real-time portion of the aircard locating mission.

27. In preparation of using the Harris StingRay and KingFish to locate the aircard on July 16-17, 2008, the FBI technical agents collected data on all cell sites located in the area identified by FBI Agent Killigrew. In order to complete this task, the FBI used its StingRay in “base station survey” mode[890] while traveling around the area covered by the cell tower range chart/map.[891]

28. While conducting base station surveys, the data collected by the FBI technical agents included signal range estimates for every cell site in the area and radio frequencies used by each cell site sector. The signal range estimates, in combination with other data, were intended to assist the FBI technical agents “in obtaining a start location for the search.”[892] The radio frequency information was needed so that the FBI technical agents


887. See Technical Explanations, Section II(G)(1), supra (explaining how the Harris StingRay and KingFish support CDMA, GSM, iDEN, and UMTS wireless technologies but only a maximum of three simultaneously).


889. See Technical Explanations, Section II(B), supra (explaining how all cell sites (including cell site emulators) wishing to communicate with 1xEV-DO Rel. 0 wireless devices must follow the instructions contained in the relevant technical standards).

890. See Technical Explanations, Section II(G)(1)(b)(i), supra (explaining base station surveys conducted by the Harris StingRay).

891. See EXHIBIT 21 of 1st Consolidated Exhibits (Dkt. #587-2) (cell tower range chart/map).

892. See EXHIBIT 066 of 2nd Consolidated Exhibits (Dkt. #821-3) (FBI technical agent memorandum).
could properly configure their StingRay and KingFish for use in cell site emulator mode. By
referencing a list of all the radio frequencies already in use, the FBI was able to choose an
unused frequency for use by its emulated cellular network that would not interfere with the
various FCC licensed cellular networks already operating in the noted area.\footnote{893}

5. The FBI technical agents had Verizon Wireless reprogram and
write data to the aircard so that it would be compatible with the
Harris StingRay and KingFish.

Service Provisioning (OTASP), also known as Over-The-Air Parameter Administration
(OTAPA)\footnote{894} to surreptitiously write data to the aircard's internal storage device, \textit{i.e.,} the
Number Assignment Module (NAM)\footnote{895}. The purpose of initiating OTAPA was to facilitate
compatibility between the aircard, the Verizon Wireless network, and the government's
Harris StingRay, KingFish, and related equipment. Verizon Wireless “had a set-up problem
with the 'Provisions'”\footnote{896} and the government was therefore “not able to get a signal”\footnote{897} on
July 15\textsuperscript{th}. The following day, all OTAPA issues were resolved and the required data had been
written to the aircard's hardware.

30. During the OTAPA session on July 16, 2008, Verizon Wireless wrote data to
the aircard consisting of (1) identifying information for the FBI's emulated cell sites\footnote{898} (2)
configuration changes that would cause the aircard to recognize the FBI's emulated cell sites
as authorized for providing service, and (3) configuration changes that would cause the
aircard to attempt connections with the FBI's emulated cell sites prior to attempting

\footnote{893}{See Technical Explanations, Section II(B)(3)(g)(i), \textit{supra} (explaining how the FCC requires cellular networks to be carefully planned so as to avoid various types of radio signal interference such as interference with ambulance radios).
\footnote{894}{See Technical Explanations, Section II(B)(3)(a), \textit{supra} (explaining OTASP and OTAPA).
\footnote{895}{See Technical Explanations, Section II(B)(2)(a), \textit{supra} (explaining the Access Terminal NAM).
\footnote{896}{EXHIBIT 26 of \textit{1st Consolidated Exhibits} (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson).
\footnote{897}{Id.}
\footnote{898}{Cell site emulation was a feature of the Harris StingRay and KingFish used by the FBI technical agents to locate the aircard. See General Facts, Section IV(B)(9)(a), \textit{supra}.}
connections with actual Verizon Wireless cell sites. The FBI technical agents needed Verizon Wireless to write data to the aircard in this manner because the aircard's properly configured Preferred Roaming List prevented it from accessing rogue, unauthorized cell sites such as cell site emulators used by the FBI.

31. In order to write data to the aircard as described in paragraph No. 30 above, Verizon Wireless: (1) surreptitiously initiated Over-the-Air Parameter Administration (OTAPA) with the aircard over the air interface; (2) disabled the SPL for the aircard's internal NAM by using the aircard's SPC; (3) used the SSD known only to the aircard.

899. See Technical Explanations, Section II(B)(3)(b)(i), supra (explaining how an Access Terminal will only scan radio frequencies listed in its Preferred Roaming List Acquisition Table); id., Section II(B)(3)(c)(i), supra (explaining how an Access Terminal will only establish a session with an Access Network that has a subnet listed as authorized in the Access Terminal Preferred Roaming List System Table).

900. The only other option for causing the aircard to recognize an emulated cell site as being authorized for service is for the FBI to (1) hijack identifying information for an actual Verizon Wireless cell site by recording Overhead Messages off the air interface, (2) load the Overhead Messages parameters into its cell site emulator, and (3) proceed to spoof an actual Verizon Wireless cell site by broadcasting copies of the hijacked Overhead Messages while within signal range of the aircard. Because the aircard would already have the hijacked identifying information stored on its Preferred Roaming List, the FBI would not need Verizon Wireless to update the list via OTAPA. However, such a spoofing operation would run the risk of intermarket and intramarket radio signal interference causing disruption to numerous users of not only Verizon Wireless' network but also of other cellular and Public Safety Radio Service networks operating in the area. See id., Section II(B)(3)(g)(i), supra (explaining interference). In order to avoid spectrum interference, it is a logical assumption that Verizon Wireless updated the aircard's Preferred Roaming List with separate frequencies, etc. as apposed to the FBI hijacking Overhead Messages from a random Verizon Wireless cell site for use in a cell site spoofing operation.

Additionally, such a spoofing operation would be a criminal offense. Since October of 1994, it has been a crime for whoever “knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver,” 18 U.S.C. § 1029(a)(8), meaning “a device or apparatus that can be used to... intercept an... identifier of any telecommunications service, equipment, or instrument,” 18 U.S.C. § 1029(e)(8), which would include, e.g., using the StingRay to record the SUBNET_COMMON_LENGTH, SUBNET_COMMON, and other identifying data fields contained in the SectorParameters and QuickConfig messages broadcast by Verizon Wireless cell sites. In the context of 18 U.S.C. § 1029(a)(8), the “intent to defraud” element is satisfied by the FBI defrauding the defendant out of his aircard service via the second denial of service attack. See General Facts, Section IV(B)(9)(i), infra (explaining DOS attack using Harris products). It is a reasonable assumption that the FBI technical agents did not commit a criminal offense and instead had Verizon Wireless update the aircard's Preferred Roaming List.

901. See Technical Explanations, Section II(B)(3)(a), supra (explaining how OTAPA is initiated by the wireless carrier surreptitiously).

902. See id. (explaining how NAM parameters are protected by the SPC/SPL).
and Verizon Wireless to validate the aircard's SPASM;\[903\] (4) transmitted a Configuration Request Message to the aircard instructing it to transmit back all of its stored NAM parameters;\[904\] (5) received the aircard's transmitted Configuration Response Message containing all of its stored NAM parameters;\[905\] (6) transmitted a Download Request Message\[906\] to the aircard containing an updated Preferred Roaming List consisting of (a) an Acquisition Table containing the band-class and channel number corresponding to the radio frequencies used by FBI's cell site emulators,\[907\][908] and (b) a System Table with the highest priority entry\[909\] containing the sector subnet and other identifying information for the FBI's cell site emulators,\[910\] and (7) transmitted a Commit Request Message to the aircard instructing it to write the new Preferred Roaming List to its permanent NAM memory.\[911\]

32. During the OTAPA session on July 16, 2008, additional data was written to the aircard by Verizon Wireless in order to reprogram the aircard's hardware. Verizon Wireless reprogrammed the aircard to respond in the following manner upon receiving a paging signal indicating an incoming 1xRTT voice call: (1) disconnect from its 1xEV-DO Rel. 0 data

---

903. See id. (explaining how NAM parameters are protected by the SPASM).

904. See id. (explaining how the Configuration Request Message is used by the Access Network to read data from the NAM).

905. See id. (explaining how the Configuration Response Message is used to return NAM data to the Access Network).

906. See id. (explaining how the Download Request Message is used by the Access Network to write data to the Access Terminal NAM).

907. See id., Section II(B)(3)(b)(i), supra (explaining how the Preferred Roaming List Acquisition Table is used to choose radio frequencies to scan for available Access Networks).

908. The frequencies used by the FBI's cell site emulators and loaded onto the aircard by Verizon Wireless were the frequencies chosen after the FBI conducted base station surveys to determine an appropriate unused frequency. See General Facts, Section IV(B)(4), supra.

909. See Technical Explanations, Section II(B)(3)(a), supra (explaining how Preferred Roaming List System Table entries are listed with the most preferred system first).

910. See id., Section II(B)(3)(c)(i), supra (explaining how the Preferred Roaming List System Table is used to identify Access Networks authorized for providing service).

911. See id., Section II(B)(3)(a), supra (explaining how the Commit Request Message is used by the Access Network to write the Download Request Message data to the Access Terminal permanent NAM memory).
connection being provided by an actual Verizon Wireless cell site, and (2) enter the Idle State. Additionally, the aircard was reprogrammed to respond to incoming 1xRTT voice calls by generating real-time cell site location information that could be forwarded to the FBI's SF-Martinez DCS-3000 server by Verizon Wireless. Because the aircard is not a telephone and does not normally respond to incoming 1xRTT voice calls, the FBI needed Verizon Wireless to use OTAPA to reprogram the aircard's hardware to respond to the FBI's planned surreptitious voice calls placed to the aircard from a landline telephone.

33. In order to write data to the aircard as described in paragraph No. 32 above, Verizon Wireless: (1) surreptitiously initiated Over-the-Air Parameter Administration (OTAPA) with the aircard over the air interface; (2) disabled the SPL for the aircard's internal NAM by using the aircard's SPC; (3) used the SSD known only to the aircard.

912. See id., Section II(B)(3)(c) et seq., supra (explaining the 1xEV-DO Idle State).
913. See General Facts, Section IV(B)(6), infra (explaining the FBI's forced generation of real-time cell site sector location information facilitated through surreptitious voice calls placed to the aircard).
914. See id., Section IV(A), supra (general background information on the aircard).
915. See Technical Explanations, Section II(B)(3)(g)(ii), supra (explaining how non-telephone 1xEV-DO Access Terminals ignore incoming 1xRTT voice calls).
916. See General Facts, Section IV(B)(8), infra (explaining the FBI's denial-of-service attack facilitated through surreptitious voice calls placed to the aircard).
917. In the alternative, if the aircard did not contain adequate manufacturer specific NAM parameters to reprogram the aircard as desired, the FBI had Verizon Wireless use IP Based Over-the-Air Device Management (IOTA-DM) using the Open Mobile Alliance Device Management (OMA DM) protocol to surreptitiously update the aircard's firmware over-the-air so that it would respond to the FBI's planned surreptitious voice calls placed to the aircard from a landline telephone. See Technical Explanations, Section II(B)(3)(a), fn. No. 121, supra (referencing technical standard explaining protocol used to update wireless device firmware surreptitiously using radio waves). See also USDOJ [M.D.La.] Aug. 12, 2008, Response to ACLU FOIA Request No. 07-4130, p. 18 of 42 (“It may also be possible to flash the firmware of a cell phone.... You don't even have to have possession of the phone to modify it; the 'firmware' is modified wirelessly.”) (emphasis added)); see also EXHIBIT 021 of 2nd Consolidated Exhibits (Dkt. #821-1) (relevant pages of cellfoia_release_074130_20080812.pdf attached with page numbers added).
918. See Technical Explanations, Section II(B)(3)(a), supra (explaining how OTAPA is initiated by the wireless carrier surreptitiously).
919. See id. (explaining how NAM parameters are protected by the SPC/SPL).
and Verizon Wireless to validate the aircard's SPASM;\(^\text{920}\) (4) transmitted a Configuration Request Message to the aircard instructing it to transmit back all of its stored NAM parameters;\(^\text{921}\) (5) received the aircard's transmitted Configuration Response Message containing all of its stored NAM parameters;\(^\text{922}\) (6) transmitted a Download Request Message\(^\text{923}\) to the aircard containing manufacturer-specific NAM parameters\(^\text{924}\) instructing the aircard to (a) generate real-time cell site location information upon receiving an incoming 1xRTT paging signal, and (b) disconnect from its Verizon Wireless 1xEV-DO Rel. 0 data connection upon receiving an incoming 1xRTT paging signal; and (7) transmitted a Commit Request Message to the aircard instructing it to write the new manufacturer-specific NAM parameters to permanent NAM memory.\(^\text{925}\)

6. The FBI used the SF-Martinez DCS-3000 Pen/Trap device to obtain real-time cell site sector location information to narrow the geographical area of where to use the StingRay, KingFish, and related equipment.

34. Prior to using the Harris StingRay, KingFish, and related equipment to pinpoint the precise location of the aircard and the defendant, the FBI needed to first narrow the geographical area of where to search for the aircard. In order to accomplish this task, the three FBI technical agents planned to use real-time cell site sector location information to determine the Verizon Wireless cell site sector providing service to the aircard.\(^\text{926}\) In order

920. See id. (explaining how NAM parameters are protected by the SPASM).
921. See id. (explaining how the Configuration Request Message is used by the Access Network to read data from the NAM).
922. See id. (explaining how the Configuration Response Message is used to return NAM data to the Access Network).
923. See id. (explaining how the Download Request Message is used by the Access Network to write data to the Access Terminal NAM).
924. See id. (explaining how an Access Terminal NAM contains manufacturer-specific NAM parameters).
925. See id. (explaining how the Commit Request Message is used by the Access Network to write the Download Request Message data to the Access Terminal permanent NAM memory).
926. See EXHIBIT 069 of 2nd Consolidated Exhibits (Dkt. #821-4) (June 7, 2011 letter from AUSA Battista to the defendant, p. 1: AUSA Battista indicating that the FBI technical agents “generate[d] activity on the device [(i.e., aircard)] in order to obtain the cell site serving the device pursuant to the [N.D.Cal 08-90331MISC-RS] Court Order...”).
to obtain the needed real-time cell site sector location information relating to the aircard, the
FBI relied upon the N.D.Cal. 08-90331MISC-RS order[927] to use a Pen/Trap device.

35. At the time of the aircard locating mission, Verizon Wireless had not yet
configured its network Intercept Access Points (IAPs)[928] to provide FBI DCS-3000
servers[929] (Pen/Trap devices) with real-time cell site location information relating to 1xEV-
DO Rel. 0 data connections for aircards.[930] As a workaround, the FBI decided to “ping the
number associated to the [air]card...”[931] in order to generate the needed data. By pinging
the aircard (i.e., placing surreptitious telephone calls to the aircard without having it ring or
answer),[932][933] the FBI would force the aircard to generate real-time cell site sector
location information associated with a 1xRTT voice call (as apposed to an 1xEV-DO Rel. 0
data connection) that could be forwarded to the FBI SF-Martinez DCS-3000 server from a
Verizon Wireless IAP.[934]

[927] See Procedural History, Section III(F), supra, (discussing procedural aspects of the
N.D.Cal. 08-90331MISC-RS order).

[928] See Technical Explanations, Section II(H)(2) and fn. No. 654, supra (explaining
Intercept Access Points).

[929] See Technical Explanations, Section II(H)(4), supra (explaining DCS-3000 servers,
i.e., Pen/Trap devices and the FBI Digital Collection Program).

[930] See, e.g., EXHIBIT 27 of 1st Consolidated Exhibits (Dkt. #587-2) (FBI Agent
Murray's rough notes indicating that no cell site data is available for an aircard when using a
Pen/Trap device); EXHIBIT 28 of 1st Consolidated Exhibits (Dkt. #587-2) (June 27, 2008
email from FBI Agent Murray to FBI Agent Leising: “Verizon Wireless can't separate tower
data from content for a broadband card.”).

[931] EXHIBIT 26 of 1st Consolidated Exhibits (Dkt. #587-2) (August 7, 2008 USPIS
Investigation Details Report entry by USPIS Inspector Wilson); see also EXHIBIT 27 of 1st
Consolidated Exhibits (Dkt. #587-2) (FBI Agent Murray's rough notes indicating that “you
have to call into the card.”).

[932] See General Facts, Section IV(A)(1), supra (explaining how the aircard is incapable
of ringing or answering calls).

[933] The only other option for the government was to obtain a Title III wiretap warrant to
receive real-time cell site location information along with the communications content of
which the location data could not be separated. See, e.g., EXHIBIT 26 of 1st Consolidated
Exhibits (Dkt. #587-2) (Based on the destination IP addresses obtained via subpoenas, the
government was “in the process of securing a Title 3” so that agents could “monitor the
content of the computer that the [air]card [was] being used [with]” in order to “possibly
triangulate the signal.”)

[934] See EXHIBIT 072 of 2nd Consolidated Exhibits (Dkt. #821-4) (December 9, 2011
letter from AUSA Battista to the defendant, p. 1: AUSA Battista indicating that “the
incoming phone calls made to your aircard were placed in order to stimulate your aircard to
36. Beginning at 11:02 am on July 16, 2008, the FBI began to place surreptitious telephone calls to the aircard using the public telephone network while Verizon Wireless, acting pursuant to the N.D.Cal. 08-90331MISC-RS order, forwarded the resulting LAESP messages (i.e., Pen/Trap data including the cell site and sector accessed by the aircard) to the FBI SF-Martinez DCS-3000 server in real-time. The FBI continued to surreptitiously call the aircard a total of 32 times until 5:03 pm on July 16, 2008. The LAESP messages sent over that six hour period informed the FBI that the aircard was located within the signal coverage area of sector No. 3, Verizon Wireless cell site No. 5, having a latitude of 37.369733 and longitude of -121.923442 with a cell site street address of 2001 Gateway Place, San Jose, CA 95110.

37. While the FBI called/pinged the aircard, the real-time cell site sector location information was fed into the SF-Martinez DCS-1020 gateway server and sent over the Internet via a Virtual Private Network (VPN) to a wireless cellular modem (i.e., the FBI's own aircard) paired with a laptop computer being accessed by the FBI technical agents provide the identity of the cell tower with which your aircard connected during these calls.”).

935. See EXHIBIT 06 of 1st Consolidated Exhibits (Dkt. #587-1) (LAESP messages sent to the SF-Martinez DCS-3000 server (Pen/Trap device) by Verizon Wireless IAPs); see also EXHIBIT 07, EXHIBIT 08, EXHIBIT 09, and EXHIBIT 10 of 1st Consolidated Exhibits (Dkt. #587-1) (The FBI's “human readable” CDNRS files created from the Verizon Wireless LAESP messages).

936. See EXHIBIT 069 of 2nd Consolidated Exhibits (Dkt. #821-4) (June 7, 2011 letter from AUSA Battista to the defendant, p. 1: “The operators called this number [belonging to the aircard] using the Public Switched Telephone Network to generate activity on the device in order to obtain the cell site serving the device...”).

937. See Technical Explanations, Section II(H)(3), supra (explaining LAESP messages).

938. See id. (neither LAESP messages, call-identifying information, nor Pen/Trap data are amongst the data recorded and retained by Verizon Wireless).

939. See EXHIBIT 07, EXHIBIT 08, EXHIBIT 09, and EXHIBIT 10 of 1st Consolidated Exhibits (Dkt. #587-1) (The FBI's “human readable” CDNRS files created from the Verizon Wireless LAESP messages).

940. See id. (showing a “location = 5-3” relating to the FBI's surreptitious phone calls); see also General Facts, Section IV(B)(2), supra (listing location information for Verizon Wireless cell site No. 5 in San Jose, CA).

941. See Technical Explanations, Section II(H)(8), supra (explaining DCS-1020 gateway servers).

942. See id.
while they were lurking the streets of Santa Clara, CA looking for the aircard. The FBI technical agents used the real-time cell site sector location information to narrow the geographical area of where to use the Harris StingRay, KingFish, and related surveillance equipment to search for the aircard.

38. Considering the aircard is not a telephone and does not have telephone service, the FBI's surreptitious phone calls did not cause the aircard to “ring” and otherwise did not cause the aircard to notify the defendant that the FBI was calling the aircard. As shown by the LAESP messages and as admitted by the prosecution, the FBI's surreptitious phone calls were not answered by the aircard in any fashion, i.e., no calls were ever established as “in progress” and the aircard was never “off the hook.”

39. As supported by credible sources cited in the Technical Explanations, Section II(H)(3), supra, and as admitted by the prosecution, Verizon Wireless only buffered the

943. Using a DCS-1020 gateway server, VPN, and aircard is the standard Digital Collection Program (DCS) operation conducted by FBI Wireless Intercept and Tacking Team (WITT) agents to locate wireless devices. See Technical Explanations, Section II(H) et seq., supra (explaining the FBI Digital Collection Program). The FBI's WITT was used to locate the defendant's aircard. See EXHIBIT 066 of 2nd Consolidated Exhibits (Dkt. #821-4) (FBI technical agent memorandum stating: “Personnel Performing Mission: TTA-WITT”).

944. See EXHIBIT 068 of 2nd Consolidated Exhibits (Dkt. #821-3) (May 2, 2011 letter from AUSA Battista to the defendant, p. 5: FBI Agent Killigrew advised FBI Agent Murray that “when a call comes into the monitoring device, it produces a shadow over the sector of the tower the phone is hitting.”).

945. See General Facts, Section IV(A)(1), supra (general background information on the aircard).

946. See EXHIBIT 06 of 1st Consolidated Exhibits (Dkt. #587-1) (LAESP messages showing that the FBI's surreptitious phone calls were forwarded to internal Verizon Wireless telephone numbers set up to handle unanswered calls).

947. See EXHIBIT 069 of 2nd Consolidated Exhibits (Dkt. #821-4) ( June 7, 2011 letter from AUSA Battista to the defendant, p. 1: “The forwarded numbers arose after the operators of the equipment used to locate the aircard called a telephone number associated with the aircard.... Because the aircard device was not a conventional telephone, incoming calls to the device could not be connected to it as a normal call. The incoming calls in question were forwarded by the Verizon Wireless network to the various numbers which belong to, and are used by, Verizon Wireless for processing incoming calls that cannot be connected/terminated to the original called number - i.e., the targeted number.”).

948. See EXHIBIT 067 of 2nd Consolidated Exhibits (Dkt. #821-3) (January 28, 2011 letter from AUSA Battista to the defendant, p. 4: “Any information transmitted to the FBI pursuant to any disclosed court Order was received by Verizon Wireless, buffered by Verizon Wireless and then transmitted to the FBI. The time period from receipt by Verizon Wireless, buffering and then transmission to the FBI is extremely short.”).
aircard's Pen/Trap data and neither recorded nor stored the data prior to forwarding it to the
FBI. Even if Verizon Wireless, through a separate mechanism, simultaneously recorded
some of the data sent in the real-time LAESP messages (for example, recording “call-detail
records” as historical data via separate network elements), it still did not record cell site
sector information before sending it to the FBI. The data retention chart showing Verizon
Wireless' practices for recording historical data lists “Cell towers used by phone” but not cell
site sectors.\footnote{949} Additionally, an analysis of the aircard's historical cell site information
recorded by Verizon Wireless\footnote{950} confirms that it only recorded and saved cell site locations
—not the more precise cell site sectors as was provided in real-time via the LAESP
messages sent to the FBI.

7. The FBI obtained additional real-time aircard data from
Verizon Wireless through means other than the SF-Martinez
DCS-3000 Pen/Trap device.

40. As explained above, the FBI relied upon the N.D.Cal. 08-90331MISC-RS
order and used the SF-Martinez DCS-3000 server (Pen/Trap device) to obtain real-time cell
site sector location information corresponding to the location of the aircard. In order to
further narrow the location of where to use the Harris StingRay, KingFish, and related
equipment, the FBI also sought further real-time aircard data from Verizon Wireless while
relying upon the N.D.Cal. 08-90330MISC-RS order.\footnote{951} Because the government destroyed
and/or failed to preserve all data seized from Verizon Wireless,\footnote{952} the precise and full
nature of the data and how it was obtained and/or generated is unknown. However, at the

\footnote{949} See Department of Justice, Retention Periods of Major Cellular Service Providers

\footnote{950} See aircard historical cell site information records provided to the FBI by Verizon Wireless: EXHIBIT 02 of 1st Consolidated Exhibits (Dkt. #587-1); EXHIBIT 03 of 1st Consolidated Exhibits (Dkt. #587-1); EXHIBIT 05 of 1st Consolidated Exhibits (Dkt. #587-1).

\footnote{951} See Procedural History, Section III(E), supra, (discussing procedural aspects of the
N.D.Cal. 08-90330MISC-RS order).

\footnote{952} See General Facts, Section IV(B)(15), infra (discussing the government's destruction of evidence).
very least, an FBI technical agent received from Verizon Wireless the aircard's distance from
a specific cell site sector.\[953\]

8. The FBI's surreptitious phone calls booted the aircard off the
Internet so that the FBI's StingRay and related equipment
could hijack the aircard's signal from Verizon Wireless.

41. Prior to conducting geolocation techniques using the Harris StingRay and
KingFish, the FBI first needed to force the aircard to establish a session\[954\] with the FBI's
emulated cellular network. Due to technical limitations of the 1xEV-DO Rel. 0
communications protocol, the Harris StingRay and KingFish were incapable of forcing the
aircard to handoff an open data connection established with a Verizon Wireless cell site to the
FBI's emulated cellular network.\[955\] The only possible inter-system handoffs in 1xEV-DO
Rel. 0 are Idle State Route Updates\[956\] and the Harris products are not immune to this
inherent protocol limitation.\[957\]

42. Because the defendant attempted to keep his aircard continuously in the
Connected State\[958\] (i.e., connected to the Internet) whenever powered on,\[959\] the FBI
technical agents first had to knock the aircard offline and into the Idle State\[960\] so that it

\[953\] See EXHIBIT 066 of 2nd Consolidated Exhibits (Dkt. #821-3) (FBI technical agent
memorandum stating that “Verizon gave a distance from the tower to the target.”)

\[954\] See Technical Explanations, Section II(B)(3)(c)(iii), supra (explaining 1xEV-DO Rel. 0
sessions).

\[955\] As explained in the Technical Explanations, Section II(B)(3)(d) et seq., supra, 1xEV-
DO Rel. 0 Access Networks (which include the FBI's cell site emulators) are incapable of
accepting a wireless device active connection “handoff” from another Access Network
without significant collaboration between the Access Terminal, the serving Access Network,
the new Access Network, and the underlying network. Because the FBI's emulated cell sites
are on their own network not connected to Verizon Wireless, the only type of aircard handoff
possible is an Idle State handoff, which is done autonomously by the aircard. See id.

\[956\] See Technical Explanations, Section II(B)(3)(d) et seq., supra (explaining the different
types of handoffs dictated by the Default Route Update Protocol).

\[957\] See Technical Explanations, Section II(B)(3), supra (explaining how all 1xEV-DO
Rel. 0 compatible Access Terminals and Access Networks must follow the instructions
contained in the relevant standards).

\[958\] See Technical Explanations, Section II(B)(3)(c)(vi), supra (explaining technical
procedures for opening a 1xEV-DO Rel. 0 connection).

\[959\] See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden
owns the aircard and used the aircard service as a home Internet connection, ¶ 17-20, p. 6-7.

\[960\] “It must be ensured, that the mobile phone of the observed person is in standby mode
would be in a position to conduct an Idle State Route Update (i.e., handoff)\(^{[961]}\) of its signal
to the FBI's emulated cellular network. With the aircard in the Idle State, the FBI's emulated
cellular network would have the opportunity to broadcast a very strong signal and present
itself to the aircard as an available and preferred network over all Verizon Wireless cell sites
in the area.\(^{[962]}\)

43. As explained by the FBI, in addition to generating real-time cell site sector
location information, the previously noted surreptitious phone calls\(^{[963]}\) also served the
purpose of knocking the aircard offline from its Verizon Wireless data connection so that it
would “connect to the best available cell phone tower that will provide it service.”\(^{[964]}\) Each
surreptitious voice call placed to the aircard by the FBI resulted in Verizon Wireless sending
a paging signal from sector No. 3, cell site No. 5, notifying the aircard of the incoming call.
\(^{[965]}\) Based on the aircard's new NAM parameter configuration facilitated via OTAPA,\(^{[966]}\)
the paging signals caused the aircard to disconnect from its Verizon Wireless 1xEV-DO Rel.
0 data connection and enter the Idle State.

44. While in the Idle State, the aircard had the opportunity to use the Default Route
Update Protocol to decide whether to conduct an Idle State Route Update (i.e., handoff) to a

\(^{[961]}\) See Technical Explanations, Section II(B)(3)(d)(i), \textit{supra} (explaining 1xEV-DO Rel. 0
Idle State Route Updates).

\(^{[962]}\) As explained in the General Facts, Section IV(B)(5), \textit{supra}, the FBI previously had
Verizon Wireless use OTAPA to update the aircard's Preferred Roaming List with identifying
information on the FBI's cell site emulators.

\(^{[963]}\) See General Facts, Section IV(B)(6), \textit{supra} (explaining details on the FBI's
surreptitious phone calls placed to the aircard).

\(^{[964]}\) \textbf{EXHIBIT 071} of 2\textsuperscript{nd} Consolidated Exhibits (Dkt. \#821-4) (December 2, 2011 letter
from AUSA Battista to the defendant, p. 1).

\(^{[965]}\) See \textbf{EXHIBIT 07}, \textbf{EXHIBIT 08}, \textbf{EXHIBIT 09}, and \textbf{EXHIBIT 10} of 1\textsuperscript{st} Consolidated
Exhibits (Dkt. \#587-1) (The FBI's “human readable” CDNRS files created from the Verizon
Wireless LAESP messages showing a “location = 5-3” relating to the FBI's surreptitious
phone calls).

\(^{[966]}\) See General Facts, Section IV(B)(5), \textit{supra} (explaining how the aircard was
reprogrammed using OTAPA).
cell site broadcasting a pilot signal with a higher signal strength than the current serving cell
site sector. After each surreptitious voice call placed to the aircard (over the previously
noted six (6) hour period), the FBI technical agents used their StingRay in the area of the cell
tower range chart/map to broadcast an emulated cellular network signal in hopes that the
aircard would detect the network and conduct an Idle State Route Update (i.e., handoff) to
the StingRay.

45. Because the defendant attempted to keep his aircard continuously connected to
the Internet, the FBI only had a very short window of time to force the aircard to handoff
its signal to the StingRay after each surreptitious voice call. Due to the auto-reconnect
software used by the defendant and/or his typical manual reconnect attempts, the
FBI needed to repeatedly call the aircard in order to repeatedly boot it offline over the six
hours of surreptitious phone calls. Each few minute window of time that followed each
denial-of-service attack (i.e., surreptitious phone call) was used by the FBI to move its
StingRay, while in cell site emulator mode, to various positions until it was close enough to
the aircard to force an Idle State Route Update (i.e., handoff).

9. The FBI technical agents used the Harris StingRay, KingFish, and related equipment to locate the aircard precisely inside
apartment No. 1122.

a. Cell site emulation and forced connection handoff.

46. During the final surreptitious phone call placed to the aircard at 5:03pm on
July 16, 2008, the FBI technical agents finally positioned their StingRay close enough to the
aircard and to force it to acquire the pilot signal of the FBI's emulated cellular network.
Because the StingRay was broadcasting a stronger pilot signal than the legitimate Verizon

967. See Technical Explanations, Section II(B)(3)(d)(i), supra (explaining 1xEV-DO Rel. 0
Idle State Route Updates).

968. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden
owns the aircard and used the aircard service as a home Internet connection, ¶17-20, p. 6-7.

969. See id.

970. See id.

971. See Technical Explanations, Section II(B)(3)(b)(ii), supra (explaining 1xEV-DO Rel. 0
Access Terminal Pilot Acquisition Substate).
Wireless cell sites in the area, the aircard began an Idle State Route Update (i.e., handoff) of its Verizon Wireless connection to the StingRay. Once the Idle State Route Update was in progress, the aircard was no longer communicating with Verizon Wireless and was now forced unwittingly to communicate directly with the government.

47. While the aircard was in direct communication with the government, the FBI technical agents engaged in a series of actions that further intruded upon the defendant's Fourth Amendment protected interests. The proceeding subsections detail the specific actions carried out by the FBI technical agents after the aircard acquired the StingRay's pilot signal. All of the government actions explained below were necessary in order for the FBI technical agents to locate the aircard.

b. The FBI repeatedly wrote data to the aircard using its StingRay.

48. Once the Idle State Route Update was complete, the aircard began monitoring the StingRay's broadcast Control Channel as dictated by 1xEV-DO Rel. 0 technical standards. Via its forward link Control Channel, the StingRay sent a Sync message to the aircard with the following data fields intended to be written to the aircard's internal storage: (1) MessageID, (2) MaximumRevision, (3) MinimumRevision, (4) PilotPN, and (5) SystemTime. Upon receiving the Sync message, the data contained in the message was written to the aircard's internal storage so that the aircard could further communicate with the StingRay.

49. Once the data contained in the Sync message had been written to the aircard's internal storage, the aircard began to monitor the StingRay's overhead messages broadcast.

---

972. Although an archaic technical term, Harris refers to this technique as “forced registration.” See id., Section II(G)(b)(iii), supra; see also id., Section II(B)(3)(c)(iii) and II(B)(3)(d), supra (explaining how in the context of 1xEV-DO Rel. 0 and other all IP based cellular networks, wireless devices establish “sessions” and conduct “route updates” with cell sites as opposed to “registering” with cell sites).

973. See Technical Explanations, Section II(B)(3)(b)(iii), supra.

974. See id.

975. See id.
over its Control Channel as dictated by 1xEV-DO Rel. 0 technical standards.\[976\] The aircard received the StingRay's overhead messages which included the QuickConfig message and SectorParameters message.\[977\] The QuickConfig message contained numerous data fields including MessageID, ColorCode, SectorID24, SectorSignature, AccessSignature, Redirect, RPCCount, ForwardTrafficValid, and a Reserved field.\[978\] The SectorParameters message contained numerous data fields including MessageID, CountryCode, SectorID, SubnetMask, SectorSignature, Latitude, Longitude, RouteUpdateRadius, LeapSeconds, LocalTimeOffset, ReverseLinkSilenceDuration, ReverseLinkSilencePeriod, ChannelCount, Channel, NeighborCount, NeighborPilotPN, NeighborChannelIncluded, NeighborChannel, NeighborSearchWindowSizeIncluded, NeighborSearchWindowSize, NeighborSearchWindowOffsetIncluded, NeighborSearchWindowOffset, and a Reserved field.\[979\] Upon receiving the overhead messages, the data contained in the messages was written to the aircard's internal storage so that the aircard could further communicate with the StingRay.\[980\]

50. Immediately after receiving the SectorParameters message, the aircard used the SectorID and SubnetMask data fields to determine the subnet of the system to which the StingRay belonged.\[981\] After deducing the StingRay's subnet, the aircard checked its locally stored Preferred Roaming List System Table to determine if the subnet was listed as corresponding to a group of Access Networks (i.e., a system) authorized for providing wireless service.\[982\] Because the government had Verizon Wireless update the aircard's Preferred Roaming List, the aircard found the StingRay's subnet listed as an authorized network and believed that it was accessing a legitimate Verizon Wireless cell site and not a

976. See \textit{id.}, Section II(B)(3)(c)(i), \textit{supra}.

977. See \textit{id.}.

978. See \textit{id.}.

979. See \textit{id.}.

980. See \textit{id.}.

981. See \textit{id.}.

982. See \textit{id.}. 
51. Prior to beginning the Access Probe process to establish a session with the FBI's StingRay, the aircard received the StingRay's AccessParameters message broadcast by the StingRay. The AccessParameters message contained numerous data fields including MessageID, AccessCycleDuration, AccessSignature, OpenLoopAdjust, ProbeInitialAdjust, ProbeNumStep, PowerStep, PreambleLength, CapsuleLengthMax, Apersistence, and a Reserved field. Upon receiving the AccessParameters message, the data contained in the message was written to the aircard's internal storage so that the aircard could further communicate with the StingRay via the Access Probe process.

c. The StingRay deactivated 1xEV-DO Rel. 0 security layer encryption during session establishment causing the aircard's signals to be transmitted in plaintext and exposed to third-parties.

52. While the aircard was establishing a session during the Access Probe process, the FBI's StingRay failed to initiate negotiation of the security layer protocols resulting in no session key being created for use in data integrity, authentication, and encryption in the MAC layer. The prosecution admitted that no encryption was in use while the FBI's surveillance equipment was communicating with the aircard. Because the FBI failed to implement standard security layer encryption over the air interface, the

---

983. See id., Section II(B)(3)(c)(ii), supra.
984. See id.
985. See id.
986. After the Access Probe process, there are numerous other occurrences of an Access Network (e.g., the StingRay) writing data to an Access Terminal (e.g., the aircard). For example, the UATIAssignment message. See Technical Explanations, Section II(B)(3)(c) (iii), supra. Not all occurrences of the StingRay writing data to the aircard are explained in this memorandum.
987. See Technical Explanations, Section II(B)(3)(c)(iii), supra (explaining 1xEV-DO Rel. 0 session establishment).
988. See id., Section II(B)(3)(c)(iv), supra (explaining how the Access Terminal is responsible for initiating security layer encryption in 1xEV-DO Rel. 0).
989. See EXHIBIT 072 of 2nd Consolidated Exhibits (Dkt. #821-4) (December 9, 2011 letter from AUSA Battista to the defendant, p. 1: AUSA Battista indicating that “while the specific techniques used to locate the aircard are Law Enforcement Sensitive, neither encryption nor encryption-defeating techniques were used in this location mission.”).
aircard's signals containing private information (e.g., the ESN via the HardwareIDRequest message) and geolocation information were exposed to third-parties over the air interface.

d. The FBI used its StingRay to download data stored on the aircard's internal storage device (i.e., the aircard's Electronic Serial Number (ESN)).

53. After the aircard and the FBI's StingRay had established a session, the StingRay was only aware that a 1xEV-DO Rel. 0 compatible wireless device had connected to its emulated cellular network while the identity of the device remained unknown.[990] Prior to conducting geolocation techniques, the FBI technical agents needed to determine if the wireless device connecting to its emulated cellular network was actually the aircard and not another device. In order to identify the aircard prior to collecting signals for triangulation purposes, the StingRay sent a HardwareIDRequest message[991][992] (via radio wave transmissions) to the receive antenna of what was then an unknown device. The aircard, being the unknown device, responded by transmitting back its ESN to the FBI's StingRay via a HardwareIDResponse message.[993] The FBI technical agents logged (i.e., seized) the ESN it received directly from the aircard and then compared it to the aircard ESN it previously received from Verizon Wireless via subpoena.[994] By matching the two separate ESNs, the FBI technical agents determined that its StingRay was communicating with the right wireless device.

990. See Technical Explanations, Section II(B)(3)(c)(v), supra (explaining how prior to sending the HardwareIDRequest message, the Access Network does not have the absolute identity of the Access Terminal).

991. See id.

992. See id., Section II(G)(1)(a)(iv), supra (explaining how the Harris StingRay downloads identifying data from wireless devices such as ESNs).

993. See id., Section II(B)(3)(c)(v), supra.

994. See Procedural History, Section III(A), supra (discussing D.Ariz. subpoenas used to obtain the aircard's ESN from Verizon Wireless).
The FBI used the StingRay to send location finding interrogation signals into the defendant's home and into the defendant's aircard in order to search out the location of the aircard and the defendant.

54. Once the FBI downloaded the aircard's stored ESN via the HardwareIDRequest message, the FBI technical agents knew that they had locked-on to the right wireless device and began “using [...] the 'Stingray' to pinpoint the location of the aircard.”\[995\] The StingRay conducts geolocation through the process of interrogation involving the transmission of specially crafted location finding interrogation signals sent to a target wireless device.\[996\] In response to the location finding interrogation signals, the target wireless device responds with location finding response signals.\[997\] The prosecution conceded that the FBI technical agents used interrogation to locate the aircard and the defendant within apartment No. 1122.\[998\] Because the aircard was located inside apartment No. 1122, the StingRay's location finding interrogation signals penetrated the exterior walls of the apartment and entered the confines of the defendant's home. Once inside the confines of the defendant's home, the StingRay's location finding interrogation signals searched out the aircard, entered the aircard's receive antenna, and forced the aircard to transmit location finding response signals telling of its location.\[999\]

55. While using the StingRay, the FBI technical agents used the AmberJack phased array beam-forming antenna to transmit a highly directional and concentrated beam of location finding interrogation signals into the defendant's home.\[1000\] The AmberJack

---

995. EXHIBIT 26 of 1st Consolidated Exhibits (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson).

996. See Technical Explanations, Section II(G)(1)(b)(iv), supra (explaining the interrogation techniques used by the Harris StingRay to locate wireless devices).

997. See id.

998. See Government's Response To Motion For Discovery (Dkt. #602, p. 3) (“The equipment mimicked a Verizon Wireless cell tower and sent and received signals directly to and from the aircard.”); January 4, 2012 Court Order (Dkt. #723, p. 14) (signals sent by the surveillance equipment used by the FBI technical agents were “signals that would not have been sent to the aircard in the normal course of Verizon’s operation of its cell towers.”).

999. See Technical Explanations, Section II(G)(1)(a)(v), supra (explaining the interrogation techniques used by the StingRay and KingFish to locate wireless devices).

1000. See id., Section II(G)(1)(a)(iii), supra (explaining the AmberJack phased array antenna used with the StingRay to locate wireless devices).
antenna is different from cell site antennas in the effect that it is capable of facilitating highly
precise angle-of-arrival measurements in order to obtain a line-bearing to a target wireless
device.\[1001\]

f. The FBI collected the aircard's signal transmissions sent in response to the location finding interrogation signals sent to the aircard by the FBI via the StingRay.

56. While the FBI technical agents were conducting interrogation, they used the StingRay to collect (i.e., seize) the aircard's location finding response signals.\[1002\] During the September 22, 2011 court hearing, the prosecution admitted that the aircard's signals were seized by the FBI with its concession that the “device sent signals to, and received signals from, the air card."\[1003\] The signals that were seized contained information (i.e., the UATI assigned to the aircard by the StingRay during session establishment)\[1004\] allowing the FBI to determine that the signals were being transmitted by the aircard. The signals in question were generated and transmitted by the aircard upon the StingRay's specific instruction (via the location finding interrogation signals) and would not have been transmitted during the aircard's communications with actual Verizon Wireless cell sites.

g. In order to determine the location of the aircard and the defendant, the FBI conducted triangulation techniques on the aircard's location finding response signals collected by the StingRay.

57. While conducting interrogation techniques, the FBI technical agents engaged in active approach to facilitate triangulation of the aircard's collected location finding response signals. The approach method involves using the StingRay to collect and measure location finding response signals while emulating a cell site at one location and then

1001. See id.
1002. See id.
1003. October 5, 2011 Court Order (Dkt. #644, p. 2) (emphasis added) (noting undisputed facts). Note: In the October 5, 2011 order and in other orders, the Court repeatedly refers to the FBI's surveillance equipment as a “mobile tracking device.” The devices used by the FBI technical agents to locate the aircard are not mobile tracking devices and the government agrees with the defendant on this undisputed fact. See Argument, Section V(F)(1)(c), infra.
1004. See Technical Explanations, Section II(B)(3)(c)(iii), supra (explaining how the Access Terminal UATI is assigned by the Access Network and used by the MAC layer protocol to label and identify transmissions during a session).
repeatedly moving the StingRay to new locations to repeat cell site emulation, signal
collection, and signal measurements.\textsuperscript{1005} By emulating a cell site at numerous locations,

enough geolocation measurements can be taken by the StingRay to triangulate the location of

a wireless device.\textsuperscript{1006} The prosecution admitted that the StingRay was used to triangulate

the location of the aircard in this manner when it conceded that the FBI technical agents

“would take a reading, move to a new location, take another reading, move to another

location, \textit{etc.}.”\textsuperscript{1007}

58. While conducting interrogation techniques during movement of the StingRay

in the geographical area surrounding the aircard (\textit{i.e.}, active approach), the FBI technical

agents conducted numerous geolocation measurements on collected aircard signals. The

geolocation measurement techniques included time-of-flight,\textsuperscript{1008} power-distance,\textsuperscript{1009}

angle-of-arrival,\textsuperscript{1010} statistical functions,\textsuperscript{1011} and data fusion.\textsuperscript{1012} The geolocation

measurement techniques used by the FBI technical agents meet the definition of triangulation

in the geolocation context.\textsuperscript{1013}

59. At some point prior to 4:45pm on July 16, 2008, the FBI technical agents were

able to triangulate the location of the aircard and the defendant as being somewhere within

the Domicilio apartment complex. In a report of investigation, USPIS Inspector Wilson

\textsuperscript{1005} See id., Section II(G)(1)(b)(v), supra (explaining the approach method used by the

StingRay and KingFish to locate wireless devices).

\textsuperscript{1006} See id.

\textsuperscript{1007} January 4, 2012 Court Order (Dkt. #723, p. 14) (noting government concession).

\textsuperscript{1008} See Technical Explanations, Section II(G)(1)(a)(i), supra (explaining TOF as used by

the StingRay and KingFish to locate wireless devices).

\textsuperscript{1009} See id., Section II(G)(1)(a)(ii), supra (explaining power-distance as used by the

StingRay and KingFish to locate wireless devices).

\textsuperscript{1010} See id., Section II(G)(1)(a)(iii), supra (explaining AOA as used by the StingRay and

KingFish to locate wireless devices).

\textsuperscript{1011} See id., Section II(G)(1)(a)(iv), supra (explaining statistical functions as used by the

StingRay and KingFish to locate wireless devices).

\textsuperscript{1012} See id., Section II(G)(1)(a)(v), supra (explaining data fusion as used by the StingRay

and KingFish to locate wireless devices).

\textsuperscript{1013} See id., Section II(C), supra (explaining triangulation in the context of geolocation of

radio frequency (RF) signals).
indicated that at some point after July 16, 2008 he was informed that the FBI technical agents “were able to get a positive signal at an apartment complex in Santa Clara[,]” i.e., the Domicilio apartment complex located at 431 El Camino Real, Santa Clara, CA 95050.\[1014\]

At approximately 4:45pm on July 16, 2008, government agents began visual surveillance of the Domicilio apartment complex.\[1015\] Therefore, it can be reasonably assumed that the FBI technical agents used their StingRay and related equipment to narrow down the location of the aircard and the defendant to the Domicilio apartment complex shortly before 4:45pm on July 16, 2008.

h. The FBI technical agents used the KingFish within the Domicilio apartment complex to pinpoint the exact location of the aircard and the defendant within apartment No. 1122.

60. In Section IV(A)(2) et seq., supra, the defendant explained how relevant evidence, heuristics, and process of elimination confirm that the handheld equipment used by the FBI technical agents included the Harris KingFish. The KingFish operates nearly identical to the StingRay with the only relevant difference being that it is a man-portable wireless device locator, as apposed to a vehicle-transportable wireless device locator, and is capable of locating wireless devices more accurately than the StingRay.\[1016\] Therefore, all of the operations explained in Sections IV(B)(9)(a) through (g), supra (paragraph Nos. 46-59 above), were repeated by the FBI technical agents while it used the handheld KingFish within the Domicilio apartment complex.

61. Once the FBI technical agents narrowed the location of the aircard and the defendant down to the Domicilio apartment complex, they began “to pin the exact number”\[1017\] where the aircard was located. In order to do so, “the FBI used handheld

\[1014\] EXHIBIT 26 of 1st Consolidated Exhibits (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson).

\[1015\] See EXHIBIT 097 of 2nd Consolidated Exhibits (Dkt. #821-6) (surveillance log indicating that visual surveillance of the Domicilio apartment complex began at 4:45pm on July 16, 2008).

\[1016\] See Technical Explanations, Section II(G)(1) et seq., supra.

\[1017\] See id.
At approximately 12:53 am on July 17, 2008, FBI Agent Murray sent a text message to FBI Agent Killigrew stating that “[w]e are down to an apt complex[]” At approximately 2:42 am on July 17, 2008, one of the FBI technical agents locating the aircard sent a text message to an unknown individual stating that they had “[f]ound the card[]” and “Sqd is working on a plan for arrest[].” Additionally, the prosecution agreed “to allow the Court to factually assume, that, at the conclusion of the July 16, 2008, aircard tracking operation, the FBI located the aircard within Unit 1122 of the Domocilio [sic] Apartments.”

i. Whenever the aircard was connected to either the StingRay or KingFish, the FBI denied the aircard access to the Internet (i.e., a denial-of-service attack).

62. Immediately after the aircard established a session with the FBI’s StingRay or KingFish, the defendant, believing he was connected to a Verizon Wireless cell site, attempted to connect his aircard and laptop computer to his aircard Internet access service. Because the StingRay and KingFish are not capable of forwarding communications content to Verizon Wireless, the defendant was not provided with any type of Internet access service. From approximately 5:03 pm on July 16, 2008 (time at which the last...
surreptitious phone call was placed to the aircard to approximately 2:42am on July 17, 2008 (time at which the KingFish pinpointed the aircard inside apartment No. 1122), the defendant was denied access to the Internet by the FBI. Using the StingRay and KingFish, the FBI technical agents conducted a denial-of-service attack on the defendant's aircard for almost a 10 hour period.

j. The FBI's StingRay and KingFish relied upon the electricity provided to the aircard by the defendant via his home.

63. In order for radio waves to be transmitted from a wireless device, they require a power source of which to draw electricity. Once transmitted, the radio waves carry the energy drawn from the power source to the receive antenna of the destination radio receiver. The receive antenna uses the transmitted energy to decode the radio waves into readable signals. Without the energy that originated at the transmit antenna, the receiver would be unable to receive, let alone decode, the transmitted signals.

64. Because the FBI technical agents were forcing the aircard to generate and transmit radio waves that were subsequently collected and decoded by their surveillance equipment, the FBI was relying upon the electricity the defendant was providing to his aircard. The aircard received its power from the defendant's laptop computer, which in turn received its power from a wall outlet within the defendant's home at apartment No. 1122. The electricity flowing from the wall outlet was purchased by the defendant.

#723, p. 14). The defendant does not agree with the government's concession. The defendant agrees, and the evidence shows, that the FBI technical agents caused an extensive disruption in service, i.e., first for a six (6) hour period using surreptitious phone calls (see General Facts, Section IV(B)(8), supra) followed by a ten (10) hour period using the StingRay and KingFish (see General Facts, Section IV(B)(9)(i), supra).

1025. See General Facts, Section IV(B)(9)(a), supra.

1026. See id., Section IV(B)(9)(h), supra.


1028. See id.

1029. See General Facts, Section IV(A)(1), supra (general background information on the aircard and host laptop computer).

1030. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 11-12, p. 3-4.

- 180 -
from Silicon Valley Power via the defendant's utility account. The FBI technical agents were effectively stealing (i.e., seizing) the defendant's electricity for use in their aircard locating mission.

**k. The FBI's StingRay and KingFish sent the aircard commands instructing it to increase its signal transmission power to facilitate more effective geolocation.**

65. The FBI technical agents were also forcing the aircard to transmit at the highest possible power thus increasing the amount of electricity seized from the defendant. One feature of the StingRay and KingFish while emulating 1xEV-DO Rel. 0 cell sites is the ability to transmit closed-loop Reverse Power Control (RPC) bits to a target wireless device. By transmitting enough RPC bits, the FBI's equipment can force a wireless device to transmit at the highest possible power so that the collected location finding response signals are easier to measure. In order to more precisely search for and locate the aircard while using its StingRay and KingFish, the FBI technical agents sent RPC bits to the aircard causing it to transmit at a higher power than it would have normally transmitted if it were accessing cellular service through an actual Verizon Wireless cell site covering apartment No. 1122.

**10. The government's plan to conceal the real-time portion of the aircard locating mission.**

66. Once the FBI technical agents pinpointed the precise location of the aircard, they “handed off” their knowledge of the aircard location to the primary case agents. The primary case agents then set out to “develop independent probable cause of the search warrant...” used to physically search apartment No. 1122. Similarly, AUSA Battista

1031. See id., ¶ 11, p. 3.
1032. See Technical Explanations, Section II(G)(1)(b)(vi), supra (explaining forced transmission power increase as used by the StingRay and KingFish to locate wireless devices).
1033. See id., Section II(B)(3)(e)(ii), supra (explaining 1xEV-DO Rel. 0 closed-loop power control on the Reverse Traffic Channel).
1034. See id., Section II(G)(1)(b)(vi), supra (explaining forced transmission power increase as used by the StingRay and KingFish to locate wireless devices).
1035. EXHIBIT 34 of 1st Consolidated Exhibits (Dkt. #587-2) (July 17, 2008 email by IRS-
had a plan to “tie the target to the case without emphasis on the [REDACTED] [(i.e., the StingRay and related equipment used to locate the aircard)].”[1036]

67. The investigative techniques stemming from the “hand off” evidence included, but were not limited to:[1037] (1) obtaining the names and addresses of individuals receiving mail at various apartments;[1038] (2) obtaining utility information for various apartments and occupant driver license information;[1039] (3) running occupant driver license numbers through the California Department of Motor Vehicles;[1040] (4) running an IRS database query for tax records belonging to occupants of various apartments;[1041] (5) running an Accurint query for occupants of various apartments;[1042] (6) obtaining rental application records for various apartments;[1043] (7) conducting handwriting comparisons using rental records; (8) taking pictures and video within and around the Domicilio apartment complex; (9) analyzing electricity use for apartment No. 1122; (10) obtaining electronic gate key access records for apartment no. 1122;[1044] (11) conducting motor vehicle license plate record checks for vehicles parked at the Domicilio apartment complex; (12) conducting a ruse Chinese food delivery at apartment No. 1122,[1045] and (13) “renting” an apartment next CI Agent Medrano sent to Albert A. Childress).

1036. EXHIBIT 38 of 1st Consolidated Exhibits (Dkt. #587-3) (emphasis added) (July 17, 2008 email by AUSA Battista sent to AUSA Yen).

1037. Despite the government's efforts, all evidence obtained after the aircard had been electronically located was in no way independent of the “hand off” evidence considering all subsequent evidence was derived from investigative techniques centered on the location of the aircard, i.e., apartment No. 1122.

1038. See EXHIBIT 44 of 1st Consolidated Exhibits (Dkt. #587-3) (IRS-CI – Notations of which law enforcement officials assisted with the government's attempt to establish independent probable cause to physically search apartment No. 1122).

1039. See id.

1040. See id.

1041. See id.

1042. See id.

1043. See id.

1044. See General Facts, Section IV(B)(12), infra (discussing government's efforts to obtain electronic gate key access records for occupant of apartment No. 1122).

1045. See EXHIBIT 45 of 1st Consolidated Exhibits (Dkt. #587-3) (July 22, 2008 email by FBI Agent Murray, sent to AUSA Battista: “Ruse tonight has been run. No one answered.”)
door to apartment No. 1122 so that agents could use it as a surveillance post to watch apartment No. 1122. [1046]

11. The government's failed attempts to visually observe the defendant or anyone entering or leaving apartment No. 1122.

68. On July 16, 2008, shortly after using the StingRay to narrow the location of the aircard as being within the Domicilio apartment complex, the government began visual surveillance of the complex. [1047] After using the KingFish to pinpoint the aircard precisely inside apartment No. 1122 on July 17, 2008, the government began visual surveillance of the exterior of the apartment and its assigned parking space. [1048] The government had four to five agents watching the complex and/or apartment No. 1122 and the surrounding area during any given surveillance operation. [1049]

69. During the surveillance operations, the government never visually observed anyone enter or leave apartment No. 1122. On July 22, 2008, FBI Agent Murray noted that the investigation revealed that the defendant's neighbors do not know him [1050] and on July 23, 2008 IRS-CI Agent Daun noted that the defendant still has not been seen. [1051] The government was unable to observe the defendant even while conducting an attempted ruse.

Neighbours don't know the resident.”); EXHIBIT 46 of 1st Consolidated Exhibits (Dkt. #587-3) (July 23, 2008 email by IRS-CI Agent Daun, sent to IRS-CI Agent Willert: “The subject did not answer his door when they attempted deliver food last night and he still hasn't been seen.”).

1046. See EXHIBIT 47 of 1st Consolidated Exhibits (Dkt. #587-3) (Rough notes by IRS-CI Agent Medrano and IRS-CI Agent Daun: “provided empty apt next door”); EXHIBIT 48 of 1st Consolidated Exhibits (Dkt. #587-3) (July 17, 2008 email by USPIS Inspector Wilson, sent to FBI Agent Murray: “man[age]ment knows it's [law enforcement] related, they voluntar[il]y let us have the room... for a couple days.”); EXHIBIT 49 of 1st Consolidated Exhibits (Dkt. #587-3) (FBI report of investigation conducted on August 4, 2008 by FBI Agent Murray RE: returning the keys to Manager Mona Chen for apartment No. 1124 at the Domicilo apartment complex).

1047. See EXHIBIT 097 of 2nd Consolidated Exhibits (Dkt. #821-6) (visual surveillance of the Domicilio apartment complex began at 4:45pm on July 16, 2008).

1048. See id. (visual surveillance of apartment No. 1122 began at 1:01pm on July 17, 2008).

1049. See id.

1050. See EXHIBIT 45 of 1st Consolidated Exhibits (Dkt. #587-3) (July 22, 2008 email by FBI Agent Murray, sent to AUSA Battista).

1051. EXHIBIT 46 of 1st Consolidated Exhibits (Dkt. #587-3) (July 23, 2008 email by IRS-CI Agent Daun, sent to IRS-CI Agent Willert).
Chinese food delivery and while conducting other visual surveillance efforts done from an apartment directly next door to apartment No. 1122. 

Likewise, the government was unable to observe anyone inside apartment No. 1122 by observing the exterior. As of July 21, 2011, USPIS Inspector Wilson indicated that the government “has no evidence that someone is living in that apartment...” and on July 30, 2008, IRS-CI Agent Fleischmann stated that “[d]uring the month of July 2008, daytime surveillance and spot check surveillance have not been able to observe any residents at the location.”

12. The government obtained and used the defendant's historical geolocation information via his Domicilio electronic gate key access records.

On July 22, 2008, FBI Agent Murray and other unknown agents interviewed Domicilio apartment complex manager, Mona Chen, regarding the electronic gate key access system at the complex. Manager Chen advised that “she only recently learned how to use the computer system which handles the gate access information[]” and demonstrated the process used for retrieving gate key access records. “The process observed [] by the interviewing agents was extremely time consuming.”

Giving up on obtaining the geolocation data from Domicilio management, FBI Agent Murray interviewed employees of Quality Alarm Service, the company contracted to

1052. See EXHIBIT 46 of 1st Consolidated Exhibits (Dkt. #587-3) (July 23, 2008 email from IRS-CI Agent Daun to IRS-CI Agent Willert: “The subject did not answer his door when they attempted deliver food last night and he still hasn't been seen.”).

1053. See fn. Nos. 1046 and 1053, supra (citing supporting evidence for claim of ruse Chinese food delivery and agents “renting” apartment No. 1124).

1054. See EXHIBIT 098 of 2nd Consolidated Exhibits (Dkt. #821-6) (July 21, 2008 email by USPIS Inspector Wilson, sent to IRS-CI Agent Medrano).

1055. Affidavit for the amended N.D.Cal. 08-70460-HRL warrant application by IRS-CI Agent Fleischmann, p. 41 (Dkt. #464-2).

1056. EXHIBIT 099 of 2nd Consolidated Exhibits (Dkt. #821-6) (FBI FD-302 report of investigation conducted on July 22, 2008 by FBI Agent Murray RE: electronic gate key access investigation conducted at Domicilio).

1057. Id.

1058. Id.
install and maintain the Domicilio electronic gate key access system. Quality Alarm Service informed FBI Agent Murray that “[D]omicilio Apartments have crashed the database which contains historical gate access information for residents.” FBI Agent Murray then served Quality Alarm Service with D.Ariz. Grand Jury Subpoena No. 07-03-709 requesting the historical electronic gate key access records for the occupant of apartment No. 1122, fob No. 58261.

73. On July 24, 2008, Quality Alarm Service responded to D.Ariz. Grand Jury Subpoena No. 07-03-709 by assisting the FBI in obtaining the requested geolocation information. On July 24, 2008, FBI Agent Murray and an employee from Quality Alarm Service went to the Domicilio apartment complex to physically retrieve the defendant’s historical electronic gate key access records from various gates. FBI Agent Murray reported the following regarding the retrieval of the geolocation data:

One caveat on the data: The alarm guy cancelled [sic] his day off and plans with family to pull this data asap for me. It took him all day to pull 12 of the 16 gates. At 4 o’clock, I took what he had and told him to go. It’s possible that there may be additional accesses.

Id.

74. Quality Alarm Service provided FBI Agent Murray with electronic gate key access records for “Building 1 Elevator Lobby at Stair Podium,” “Podium Level Gate Building 4 and 2,” and “Podium Level Gate by Leasing.” for listed dates/times between June 25, 2008 and July 24, 2008. The historical geolocation data provided by Quality Alarm Service at Domicilio.

1059. See EXHIBIT 100 of 2nd Consolidated Exhibits (Dkt. #821-6) (FBI FD-302 report of investigation conducted on July 23, 2008 by FBI Agent Murray RE: electronic gate key access investigation conducted at Quality Alarm Service).

1060. Id.

1061. See Procedural History, Section III(G), supra (discussing procedural aspect of D.Ariz. Grand Jury Subpoena No. 07-03-709).

1062. See EXHIBIT 101 of 2nd Consolidated Exhibits (Dkt. #821-6) (July 24, 2008 email by FBI Agent Murray, sent to AUSA Battista et al.: electronic gate key access records were not easily obtained.).

Service has an offset date/time scheme as follows: (1) actual access dates are one day previous to the dates listed, and (2) actual access times are approximately ten minutes previous to the times listed.\[1064\] The information provided by Quality Alarm Service indicated that the defendant had been historically located at the following Domicilio electronic gates on the dates specified:\[1065\]

1. June 4, 2008  2:26am
2. June 8, 2008  12:48am
3. June 7, 2008  2:16am
4. June 13, 2008  12:24am
5. June 20, 2008  7:31am
7. June 24, 2008  4:41am
8. June 24, 2008  4:43am
9. June 24, 2008  6:35am
10. June 25, 2008  7:39am
11. June 25, 2008  7:40am
12. July 1, 2008  12:35am
13. July 4, 2008  8:59pm
14. July 5, 2008  2:15pm
15. July 5, 2008  2:15pm
16. July 13, 2008  11:03pm
17. July 18, 2008  2:45am
18. July 18, 2008  2:45am
19. July 18, 2008  2:46am
20. July 18, 2008  2:46am
21. July 23, 2008  9:02pm

1064. \textit{See id.}

1065. The following list was created based off of the subpoena response with dates and times adjusted according to FBI Agent Murray's report of investigation.
75. Using the above historical geolocation information, AUSA Battista was able to conclude (1) the defendant made “14 Visits in 50 days [to apartment No. 1122] = 1 visit every 3.6 days,” (2) the estimated next entry to apartment No. 1122 by the defendant is “Saturday 7-26 or Sunday 7-27 between the Hours of 12:01 AM and 7:00 AM,” (3) “Frequency of days of week” for entries by the defendant was “Monday - None, Tuesday - 2, Wednesday - 3, Thursday - 0, Friday - 4, Saturday - 2, Sunday – 3,” and (4) “Frequency of times of day” for entries by the defendant was “12:00 AM to 6:00 AM - 7, 6:01 AM to 12:00 PM - 3, 12:01 PM to 6:00 PM - 1, 6:01 PM to 11:59 PM – 3.” Additionally, despite all government agents failing to visually observe anyone entering or leaving apartment No. 1122, AUSA Battista was still able to advance the ongoing investigation on July 25, 2008 by using the above listed geolocation records to infer that the defendant was located precisely inside apartment No. 1122 two days prior.

13. The FBI's August 3, 2008 sighting of the defendant within the Domicilio apartment complex and his subsequent arrest by Santa Clara, CA city police officers.

76. From August 1-3, 2008, agents continued visual surveillance of apartment No. 1122. Just like in the prior month, agents failed to observe anyone entering or exiting the apartment. Although surveillance of the specific apartment was unfruitful, at 4:15pm on August 3, 2008, FBI Agent Aleksandr Kobzanets “observed a white male fitting...”

1066. EXHIBIT 101 of 2nd Consolidated Exhibits (Dkt. #821-6) (July 24, 2008 email by AUSA Battista, sent to FBI Agent Murray et al.: analysis of historical electronic gate key access records.).

1067. Because the electronic gates at the Domicilio apartment complex can be pushed open from the inside without using an electronic gate access key, the geolocation records at issue do not contain information on when the defendant exited his home. Therefore, no inferences can be made about the length of time spent by the defendant within his home during the times between the logged entry dates.

1068. See EXHIBIT 103 of 2nd Consolidated Exhibits (Dkt. #821-6) (July 25, 2008 email by AUSA Battista, sent to AUSA Yen: “We have confirmed that the target is in the Santa Clara Area and visited the target apartment on 7/23.”).

1069. See EXHIBIT 104 of 2nd Consolidated Exhibits (Dkt. #821-6) (FBI FD-302 report of investigation conducted on August 2, 2008 by FBI Agent Robert L. Kay RE: August 2, 2008 visual surveillance of apartment No. 1122); EXHIBIT 105 of 2nd Consolidated Exhibits (Dkt. #821-6) (FBI FD-302 report of investigation conducted on August 2, 2008 by FBI Agent Wade Luders RE: August 3, 2008 visual surveillance of apartment No. 1122).

1070. See id.
the known description of [][the defendant] exiting the first floor hallway and walking to the
entry gate located near University of Santa Clara center field."[1071][1072] “Since the male
exited the apartment complex from the general direction of the subject's apartment and fit the
description of the subject, [][FBI Agent] Kobzanets decided to follow the male and attempt
to establish his identity."[1073]

77. While following the unknown male, FBI Agent Kobzanets “believed that the
male was able to see [][him] following at a distance.”[1074] After following the unknown
male for some time, he “got off the main road and continued in the same direction, walking
through the rear parking lots of the businesses along El Camino Real.”[1075] FBI Agent
Kobzanets eventually lost site of the unknown male “near the Starbucks coffee shop located
on the corner of El Camino Real and Railroad Avenue.”[1076] FBI Agent Kobzanets then
“flagged down a Santa Clara Police Department marked unit in the area and sought PD
assistance in locating the individual.”[1077] FBI Agent Kobzanets “requested assistance with
locating and identifying the possible subject from officers Dominic Sandoval and Thuy

1071. EXHIBIT 106 of 2nd Consolidated Exhibits (Dkt. #821-6) (FBI FD-302 report of
investigation conducted on August 3, 2008 by FBI Agent Aleksandr Kobzanets RE: August
3, 2008 arrest of unknown male seen within the Domicilio apartment complex).

1072. Although the defendant had never been seen by agents either within the Domicilio
apartment complex or anywhere, they had a very general description of him from grainy
store surveillance videos and similar. See, e.g., EXHIBIT 075 of 2nd Consolidated Exhibits
(Dkt. #821-4) (images of the defendant paying his aircard account bill extracted from June
12, 2008 video camera footage for Verizon Wireless store located at 768 Market St., San
Francisco, CA, 94102); EXHIBIT 074 of 2nd Consolidated Exhibits (Dkt. #821-4) (FBI FD-
302 report of investigation conducted on July 17, 2008 by FBI Agent Murray RE:
subpoenaed DVD of June 12, 2008 video camera footage for Verizon Wireless store located
at 768 Market St., San Francisco, CA, 94102 where aircard payment was made).

1073. EXHIBIT 106 of 2nd Consolidated Exhibits (Dkt. #821-6) (FBI FD-302 report of
investigation conducted on August 3, 2008 by FBI Agent Aleksandr Kobzanets RE: August
3, 2008 arrest of unknown male seen within the Domicilio apartment complex).

1074. Id.

1075. Id.

1076. Id.

1077. See EXHIBIT 107 of 2nd Consolidated Exhibits (Dkt. #821-6) (September 17, 2008
email from FBI Agent Murray to FBI Agent Ng: summary justification as to why the Santa
Clara, CA police officers should receive awards for arresting the unknown male).
Eventually, FBI Agent Kobzanets “observed the male running South through the parking lot towards El Camino Real.” A combination of federal agents on foot, Santa Clara police officers on foot, and two Santa Clara police cruisers began to chase the unknown male. “One of the police units then attempted to block his escape by getting on the curb in front of the subject.” At that point, Santa Clara police officers struck the unknown male with a police cruiser knocking him to the ground. Santa Clara police officers then apprehended the unknown male and placed him into handcuffs. A search of the unknown male produced keys and a small amount of cash.

The unknown male was taken to the Santa Clara Police Department and eventually booked into the Santa Clara county jail under the name “Steven Brawner”—the name given to Santa Clara law enforcement by USPIS Inspector Wilson. The United States Marshal Service (USMS) later fingerprinted the unknown male and determined his identity to be Daniel David Rigmaiden.


As previously noted, keys were found on the defendant at the time of his arrest. Shortly after the keys were seized from the defendant, FBI Agent Vinh Nguyen “transported the keys found on the subject to 431 El Camino Real, Apartment # 1122, Santa Clara, California, and was able to confirm that the key was for that apartment.” In other words, FBI Agent Nguyen conducted a keyhole search of apartment No. 1122 by inserting

1078/ EXHIBIT 106 of 2nd Consolidated Exhibits (Dkt. #821-6) (FBI FD-302 report of investigation conducted on August 3, 2008 by FBI Agent Aleksandr Kobzanets RE: August 3, 2008 arrest of unknown male seen within the Domicilio apartment complex).

1079. Id.

1080. See id.

1081. Id.

1082. See id. (“While still behind the subject by about 100 yards, SA Kobzanets observed the subject hitting the police vehicle and falling to the ground.”).

1083. See id.

1084. See id.

1085. Id.
the key and unlocking the door (but not entering).

15. The government's destruction of the seized/collection real-time aircard data.

81. Once the defendant was arrested and in custody, the government continued with its plan to conceal evidence by destroying the real-time aircard data obtained via portable/transportable wireless device locators and from Verizon Wireless.\footnote{1086}[1087] This data was “destroyed shortly after [the defendant's] arrest on August 3, 2008.”\footnote{1088} The government claims that “the FBI has a standard policy of destroying the real-time data at the end of a tracking operation.”\footnote{1089} The prosecution provided the defendant with a “copy and paste” excerpt of the FBI policy upon which the FBI technical agents purportedly relied while destroying the real-time aircard data obtained from Verizon Wireless and obtained directly by the FBI through use of the StingRay and related surveillance equipment:

Extracted from HQ-1068430 serial 342, an EC dated 8/24/2004:

Upon completion of a case all data related to that particular case must be removed from the cellular tracking equipment. Thus, prior to deploying equipment to effect a collection authorized pursuant to particular court order, TTAs should ensure that the equipment has been cleared of any prior case operational data.

EXHIBIT 071 of 2nd Consolidated Exhibits (Dkt. #821-4) (December 2, 2011 letter from AUSA Battista to the defendant, p. 1).

82. Separate from the FBI’s express policy, which is void of a directive

\footnote{1086. See January 4, 2012 Court Order (Dkt. #723, p. 14) (Noting the settled fact that “[a]ll data generated by the [[portable/transportable wireless device locators] and received from Verizon as part of the locating mission was destroyed by the government shortly after Defendant’s arrest on August 3, 2008.”).}

\footnote{1087. Although the government conceded to full destruction of evidence, the destroyed data did not include the LAESP messages (i.e., Pen/Trap data) obtained from Verizon Wireless pursuant to the N.D.Cal. 08-90331MISC-RS order or the historical cell site location information obtained from Verizon Wireless pursuant to the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders.}

\footnote{1088. See October 5, 2011 Court Order, p. 2 (Dkt. #644) (Establishing as undisputed that the real-time aircard geolocation data “was destroyed shortly after Defendant’s arrest on August 3, 2008[.]”); EXHIBIT 33 of 1st Consolidated Exhibits (Dkt. #587-2) (Letter by AUSA Battista, sent to the defendant).}

\footnote{1089. Government's Response To Defendant's Motion To Dismiss For Destruction Of Evidence – Docket No. 595 (Dkt. #633, p. 3).}
supporting absolute deletion of any data (whether obtained by the FBI directly or seized from a wireless carrier), the FBI made a public statement to The Wall Street Journal indicating that agents destroy evidence in an attempt to conceal the portable/transportable wireless device locators from those that they track/locate:

In September, a Federal Bureau of Investigation representative told the Journal the policy of deletion “is intended to protect law enforcement capabilities so that subjects of law enforcement investigations do not learn how to evade or defeat lawfully authorized investigative activity.”


On September 22, 2011, the same day The Wall Street Journal published its original article making reference to the above quoted FBI statement, the prosecution addressed the FBI's evidence destruction in court and stated that “[t]here's been statements now in the public record that that's also FBI policy.”

16. The government seized evidence from apartment No. 1122 by executing the previously returned N.D.Cal. 08-70460-HRL search warrant.

83. On July 22, 2008, IRS-CI Agent Fleischmann and AUSA Yen obtained the N.D.Cal. 08-70460-HRL search warrant, which required the government to search apartment No. 1122 by July 31, 2008. “Since the identity of the subject was unknown, agents did not proceed with a search warrant of the apartment in case the subject used [] the apartment"


1091. See Procedural History, Section III(H), supra (discussing procedural aspect of N.D.Cal. 08-70460-HRL search warrant).
only as an off-site to house his computer.”[1092] Instead of executing the warrant, agents
decided that “it may be necessary to do another controlled delivery of money from the CI to
the suspect...”[1093]

84. The original N.D.Cal. 08-70460-HRL warrant was “returned unexecuted
due to the ongoing nature of the investigation.”[1094] Once returned to Magistrate Judge
Trumbull on July 31, 2008, the N.D.Cal. 08-70460-HRL warrant was void as a matter of law.
When the government was finally ready to execute the search warrant, they amended the
original N.D.Cal. 08-70460-HRL warrant application and resubmitted it in the Northern
District of California. Notwithstanding the fact that the N.D.Cal. 08-70460-HRL warrant
was void as a matter of law, the amended affidavit contained no new information (later than
July 23, 2008) that could arguably establish that probable cause still existed to search
apartment No. 1122.[1095] Magistrate Judge Trumbull reissued the previously returned
warrant with a handwritten “AMENDED” notation added towards the top of the document.
[1096] On August 3, 2008, the government executed the N.D.Cal. 08-70460-HRL warrant
and physically seized the aircard, the host laptop computer, physical data storage devices,
encrypted virtual drives, and other evidence from inside apartment No. 1122.[1097]

17. IRS-CI Agent Daun continues to execute the N.D.Cal. 08-70460-
HRL/PVT search warrant more than three years after the
defendant's arrest.

85. After the government seized all physical data storage devices (e.g., hard drives)
from apartment No. 1122, IRS-CI Agent Daun made an exact duplicate (i.e., a forensic
image) of each of the hard drives. IRS-CI Agent Daun created the images by copying each

1092. See EXHIBIT 42 of 1st Consolidated Exhibits (Dkt. #587-3) (August 13, 2008 email
by FBI Agent Murray, sent to FBI Agent Huntsberry et al.).

1093. EXHIBIT 26 of 1st Consolidated Exhibits (Dkt. #587-2) (August 7, 2008 USPIS
Investigation Details Report entry by USPIS Inspector Wilson).

1094. See Affidavit for the amended N.D.Cal. 08-70460-HRL warrant application by IRS-CI
Agent Fleischmann, p. 1-2 (Dkt. #464-2, p. 3-4).

1095. See Procedural History, Section III(G), supra (discussing procedural aspects of
N.D.Cal. 08-70460-HRL warrant).

1096. See Dkt. #464-1 (warrant).

1097. See Dkt. #464-1 (warrant return).
seized hard drive, bit-for-bit, to government hard drives. After the images were made, IRS-CI Agent Daun conducted searches within all of the images and within the encrypted virtual drives contained therein. Although no time line was provided, the defendant assumes that IRS-CI Agent Daun's search was conducted within 30 days of August 3, 2008, which is in accordance with the terms of the N.D.Cal. 08-70460-HRL/PVT warrant.

IRS-CI Agent Daun conducted the search for the purpose of locating data meeting the descriptions of items to be seized listed in paragraphs 2-19 of the search warrant. As a result of her search, IRS-CI Agent Daun made a PDF summary of the files that fell within the scope of the search warrant. The PDF summary was originally provided to the defense via discovery on February 25, 2010. According to the summary, IRS-CI agent Daun extracted all files that fell within the scope of the warrant and then copied some

1098. See EXHIBIT 087 of 2nd Consolidated Exhibits (Dkt. #821-5) (Computer Forensic Report by IRS-CI Agent Daun RE: search of physical storage devices and virtual drives seized from apartment No. 1122).

1099. An encrypted virtual drive operates and functions the same as a physical hard drive with the only difference being that it exists as a large “container file” saved on a physical hard drive. Software is used to mount the encrypted virtual drive causing it to appear within the host operating system as a physical hard drive for all intents and purposes. Once mounted, data can be written to and read from the encrypted virtual drive just like a physical hard drive.

1100. See Procedural history, Section III(H), supra (discussing and analyzing both versions of the warrant); Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122, “Computer Search Protocol For The Northern District Of California,” ¶ 5, p. 2 (Dkt. #566-2, p. 16) (“The 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.”).

1101. The computer search protocol and described files to be seized are identical in both the original (N.D.Cal. 08-70460-HRL) and amended (N.D.Cal. 08-70460-PVT) versions of the search warrant. See Procedural history, Section III(H), supra.

1102. See Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122 (Dkt. #566-2, p. 6-8) (describing specific subjects upon which a file must relate in order for the government to seize the file under the warrant).

1103. See EXHIBIT 087 of 2nd Consolidated Exhibits (Dkt. #821-5) (Computer Forensic Report by IRS-CI Agent Daun RE: search of physical storage devices and virtual drives seized from apartment No. 1122).
of those files to DVDs so that they would be isolated (i.e., seized) from the images.[1104] While conducting the search, IRS-CI Agent Daun accessed the defendant's encrypted virtual drives in order to seize files that were within the scope of the warrant.[1106] 

87. The encrypted virtual drives themselves were not copied from the images onto the DVDs or to any other storage device for the purpose of seizure because they “actually contain many more files than those that fall within the parameters of the Search Warrant and its attachments.”[1107] However, even while IRS-CI Agent Daun correctly admits that the encrypted virtual drives, as a whole, are beyond the scope of the relevant warrant, she still continues to access the drives (more than three years after the search of apartment No. 1122) in order to seize evidence for the prosecution—a clear violation of the computer search protocol contained in the N.D.Cal. 08-70460-HRL/PVT warrant.[1108]

88. Evidence in support of the above claim came into the possession of the defense via the March 22, 2012 discovery set.[1109] According to the noted discovery, IRS-CI Agent Daun re-accessed the original images (i.e., the encrypted virtual drives) in October of 2011 in order to retrieve files for the prosecution.[1110] While re-accessing the drives, IRS-CI Agent

1104. See id.

1105. IRS-CI Agent Daun did not copy (i.e., seize) any files to the DVDs that were identified by her virus scan software as being “possible threats.” See id. (“Symantec identified a few possible threats and those files were also removed. Screen shots of the virus scan findings, for those files, are included on the relevant DVD. Those additional files can be provided, upon request, on separate CD.”).

1106. See id.

1107. See EXHIBIT 087 of 2nd Consolidated Exhibits (Dkt. #821-5) (Computer Forensic Report by IRS-CI Agent Daun RE: search of physical storage devices and virtual drives seized from apartment No. 1122).

1108. See Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122, “Computer Search Protocol For The Northern District Of California,” ¶ 5, p. 2 (Dkt. #566-2, p. 16) (“The 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.”) (emphasis added)).

1109. See EXHIBIT 088 of 2nd Consolidated Exhibits (Dkt. #821-5) (March 7, 2012 IRS Memorandum for Transmittal of Electronically Stored Information by IRS-CI Agent Daun).

1110. See id. (Dkt. #821-5) (“The above file [agj_bag_liner_jagbags.co.nz.txt] is located in a DriveCrypt encrypted volume named filesalot.dcv on the Toshiba 100GB hard drive... The agj_bag_liner_jagbags.co.nz.txt file is not individually listed in the analysis reports.”).
Daun copied the file “agj_bag_liner_jagbags.co.nz.txt”—a file not even listed in her original PDF summary created within the first 30 days after August 3-4, 2008. It is clear that IRS-CI Agent Daun was/is re-accessing the encrypted virtually drives because, otherwise, she would not have been able to obtain a file not listed in her PDF summary made more than three years prior. IRC-CI Agent Daun failed, and continues to fail, to follow the terms of the N.D.Cal. 08-70460-HRL warrant with respect to the search and seizure of digital data.

18. The government failed to serve the defendant with a copies of the aircard locating mission orders or with receipts of what was seized.

89. The investigators involved in locating the aircard failed to serve the defendant with copies of the D.Ariz. 08-3286MB-LOA, 08-3298MB-LOA, or 08-7273MB-ECV orders or with receipts listing the items seized. The noted investigators also failed to serve the defendant with copies of the N.D.Cal. 08-90330MISC-RS or 08-90331MISC-RS orders. Additionally, the government has presented no evidence indicating that copies of the orders and receipts of seized items were left at the defendant's home residence at some point after the aircard was located.

90. The government made no attempt to effectively “serve” the defendant with copies of the orders until more than nine months after they were executed. The defense only learned of the existence of the orders after the prosecution provided copies to the defendant's attorney via discovery on April 14, 2009 (D.Ariz. orders) and on April 23, 2009 (N.D.Cal. orders). The orders were eventually provided to the defendant by his subsequent defense attorney, Philip Seplow, on July 30, 2009. The defendant is yet to be provided with receipts of the items seized under the orders.

V. ARGUMENT

In support of the defendant's request for suppression of evidence, the proceeding subsections address various issues that are relevant to a motion to suppress. The proceeding subsections begin with the defendant establishing his privacy, property, possessory, and liberty interests in various places, objects, information, records, resources, and combinations

1111. See id.
thereof. See Argument, Sections V(A), (B), and (C), infra. Considering the defendant's Fourth Amendment protected interests apply to all categories of searches and/or seizures, Sections V(A), (B), and (C) are outlined separately from later sections categorizing the government's actions conducted in violation of the Fourth Amendment. After establishing his Fourth Amendment protected interests, the defendant separates and categorizes all government actions according to the specific types of searches and/or seizures relevant to each action. See Argument, Section V(D) and (E), infra. Once categorized, the defendant explains how the government's actions violated the defendant's Fourth Amendment rights based on unreasonableness and lack of proper judicial authority. See Argument, Section V(F), infra. Finally, the defendant explains how the good faith exception to the exclusionary rule is inapplicable and how suppression of evidence is an appropriate remedy. See Argument, Section V(G) and Conclusion, Section VI, infra.

A. The defendant's property/possessory interests in his home, aircard, host laptop computer, and electricity provided through his utility account.

1. The defendant had a property and possessory interest in his home at apartment No. 1122.

   From October 21, 2007 through August of 2008, the defendant possessed a valid lease on apartment No. 1122 at the Domicilio apartment complex, 431 El Camino Real, Santa Clara, CA. 95050—his only home residence. The defendant applied to rent his apartment in person, entered into the lease using his alias of Steven Travis Brawner, and was the sole renter and occupant of his apartment throughout the duration of the lease. See EXHIBIT 089 of 2nd Consolidated Exhibits (Dkt. #821-5) (select documents for apartment No. 1122, leasing agreement indicating that the defendant would rent apartment No. 1122 from October 21, 2008 through April 30, 2008); EXHIBIT 090 of 2nd Consolidated Exhibits (Dkt. #821-5) (records indicating that the defendant would continue renting apartment No. 1122 “month to month” after April 30, 2008).

   See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 1, p. 1.

1112. See id.

1113. See also Dkt. #464-
Notwithstanding the fact that the defendant rented his apartment under an alias, he always legitimately paid his rent using money orders that he purchased with physical cash and management never attempted to evict the defendant or repossess the apartment. The defendant also possessed a renter's insurance policy for apartment No. 1122 further underscoring his property and possessory interests in his home. During the time the FBI conducted the aircard locating mission, the defendant's rent was fully paid and Domicilio was satisfied with the defendant as a renter and occupant of apartment No. 1122. Other than for master keys in the possession of management, the defendant possessed the only keys to apartment No. 1122 and never shared them with anyone. At the time of his arrest on August 3, 2008, the keys to apartment No. 1122 were found in the defendant's pocket.

2. The defendant had a possessory interest and continues to maintain a property interest in the aircard.

Because the defendant acquired the aircard through a legitimate purchase using his own money, Verizon Wireless' property and possessory interests were transferred to the

1. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 1, p. 1.

2. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 3, p. 2.

3. See EXHIBIT 091 of 2nd Consolidated Exhibits (Dkt. #821-5) (FBI FD-302 reports of investigation conducted on July 29 and 31, 2008 by FBI Agent Murray RE: Domicilio management indicated that the defendant paid his rent with money orders for May, June, July and August of 2008).

4. See EXHIBIT 092 of 2nd Consolidated Exhibits (Dkt. #821-5) (Leasingdesk.com eRenterPan insurance policy for Domicilio apartment No. 1122).

5. See fn. No. 1119, supra.

6. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 6-8, p. 2-3.

7. See General Facts, Section IV(B)(13), supra.
defendant. See Maryland v. Macon, 472 U.S. 463, 469 (1985) (“Here, respondent voluntarily transferred any possessory interest he may have had in the [[sold objects] to the purchaser upon the receipt of the funds.”). On May 23, 2006, the defendant went to a Verizon Wireless store in San Francisco, California and purchased the aircard using his own physical cash. [1123] Being a legitimate purchase, Verizon Wireless never complained about the defendant's purchase and never expressed an interest in repossessing the aircard throughout the duration of aircard service.[1124] Considering the aircard was neither stolen nor obtained by fraud, neither Verizon Wireless nor any other entity have ownership claims to the aircard. The defendant continues to own his aircard to this day and he maintained possession of it until the government seized it via an in-person search of his home conducted on August 3-4, 2008. [1125] 3. The defendant had a possessory interest and continues to maintain a property interest in the host laptop computer used with the aircard.

Because the defendant acquired the host laptop computer through a legitimate purchase using his own money, Lenovo's property and possessory interests were transferred to the defendant. See Macon, 472 U.S. at 469. On August 30, 2007, the defendant purchased the host laptop computer from a salesman who works for Lenovo.[1126] In order to purchase the computer, the defendant used a “Wired Plastic” prepaid debit card previously purchased under his alias of Andrew Johnson, loaded it with his own physical cash through Western Union, and then provided the billing information to Lenovo.[1127][1128] Records

1123. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 2, p. 1-2.
1124. See id.
1125. See Submission Of Materials Related To Search Warrant No. 08-70460, Authorized By Magistrate Judge Patricia V. Trumbull, Northern District Of California, On July 30, 2008 (Dkt. #464-1, p. 21) (N.D.Cal. 08-70460-HRL search warrant (amended) return listing the aircard as “Verizon Wireless Card #P/N PC5740VW.”).
1126. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 4, p. 2-3.
1127. See id.
1128. See EXHIBIT 085 of 2nd Consolidated Exhibits (Dkt. #821-5) (report of investigation by USPIS Inspector James L. Wilson indicating that the defendant's laptop was purchased
relating to the defendant's purchase of his laptop from Lenovo were found on his computer
by the government.\[1129\] Being a legitimate purchase, Lenovo never reported the purchase
as being fraudulent and never expressed an interest in repossessing the host laptop computer.
\[1130\] The prepaid debit card used to make the purchase is still in good standing with an
active “card status” and an active “account status.”\[1131\] Considering the host laptop
computer was neither stolen nor obtained by fraud, neither Lenovo nor any other entity have
ownership claims to the computer. The defendant continues to own his laptop computer to
this day and he maintained possession of it until the government seized it via an in-person
search of his home conducted on August 3-4, 2008.\[1132\]

4. The defendant had a property and possessory interest in his
home electricity purchased from Silicon Valley Power.

Because he paid for his home's electricity through a utility account, the defendant had
a property and possessory interest in that resource. The defendant's electricity was provided
by Silicon Valley Power of Santa Clara, account No. 00070682-04.\[1133\] The defendant paid
his electricity bill each month, under his alias of Steven Brawner,\[1134\] with money orders he

\[1129\] See defendant's declaration accompanying this memorandum RE: Data extracted from
hard drive images corresponding to seized hard drives connected to Daniel Rigmaiden's
home computer, ¶ 8, p. 4 & Attachment No. 14 (the defendant's laptop purchase records
found on his computer by the government).

\[1130\] See EXHIBIT 084 of 2nd Consolidated Exhibits (Dkt. #821-5) (The defendant's
Lenovo purchase account records showing a $0.00 balance due and the host laptop computer
purchase being paid in full.).

\[1131\] See EXHIBIT 086 of 2nd Consolidated Exhibits (Dkt. #821-5) (The defendant's
prepaid debit card account records showing the card and account to be active.);

\[1132\] See Submission Of Materials Related To Search Warrant No. 08-70460, Authorized
By Magistrate Judge Patricia V. Trumbull, Northern District Of California, On July 30,
2008 (Dkt. #464-1, p. 21) (N.D.Cal. 08-70460-HRL search warrant (amended) return listing
the host laptop computer as “IBM Thinkpad S/N #LV-C4398 With Mouse, Keys, Docking
Station & Power Cord.”).

\[1133\] See EXHIBIT 095 of 2nd Consolidated Exhibits (Dkt. #821-5) (the defendant's bill and
collection letter from Silicon Valley Power for apartment No. 1122).

\[1134\] See id. (Note: due to the illegible handwriting of Domicilio management, the bill
misspelled “Brawner” as “Branner”).
purchased using his own physical cash.\[[1135]\] During the four months leading up to the aircard locating mission, the defendant paid electricity bills in the approximate amounts of $50, $40, $30, and $20.\[[1136]\] During the time of the aircard locating mission, both the defendant's home computer and aircard operated together by using the electricity the defendant purchased for use at apartment No. 1122.\[[1137]\]

5. The defendant had a property and possessory interest in his Internet access bandwidth purchased from Verizon Wireless.

Because he paid for his Internet access bandwidth through his aircard account, the defendant had a property and possessory interest in that resource. The defendant's Internet access was provided by Verizon Wireless through his aircard account having wireless account number 270691733.\[[1138]\] The defendant purchased Internet access numerous times by personally visiting Verizon Wireless stores to pay his aircard account bill using his own physical cash.\[[1139]\] On June 27, 2008, Verizon Wireless advised FBI Agent Murray that recent payments for the aircard service were received as follows: “April 10 (physical cash payment of $160), April 24 (internal credit balance), June 12 (physical cash payment of $270) and June 24 (internal credit balance).”\[[1140]\] The government also has a surveillance video of the defendant paying his aircard account bill on June 12, 2008.\[[1141]\] Although the

\[1135. \text{See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 11, p. 3.} \]

\[1136. \text{See EXHIBIT 094 of 2nd Consolidated Exhibits (Dkt. #821-5).} \]

\[1137. \text{See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 12, p. 3-4.} \]

\[1138. \text{See Procedural History, Section III(A), supra (discussing procedural aspects of D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615).} \]

\[1139. \text{See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 8, p. 4.} \]

\[1140. \text{EXHIBIT 077 of 2nd Consolidated Exhibits (Dkt. #821-4).} \]

\[1141. \text{See EXHIBIT 075 of 2nd Consolidated Exhibits (Dkt. #821-4) (images of the defendant paying his aircard account bill while wearing his “Black Adidas 'Clima 365'” pants with three white stripes, extracted from June 12, 2008 video camera footage for Verizon Wireless store located at 768 Market St., San Francisco, CA, 94102); EXHIBIT 074 of 2nd Consolidated Exhibits (Dkt. #821-4) (FBI FD-302 report of investigation conducted on July 17, 2008 by FBI Agent Murray RE: subpoenaed DVD of June 12, 2008 video camera} \]
resolution of the video is too low to positively identify the defendant, it still corroborates the defendant's claim because the clearly visible Adidas pants worn by the defendant in the video[1142] are identical to the Adidas pants seized from the defendant's home by the government on August 3-4, 2008.[1143]

B. The defendant's liberty interest in using his aircard, host laptop computer, and aircard service to access the Internet for the purpose of satisfying his own personal and political interests, etc.

From May 23, 2006 through August 3, 2008, the defendant had a liberty interest in his Internet connection accessed through his aircard and host laptop computer because he used the connection to pursue his own personal and political interests and for leisure activities. In Soldal, the Supreme Court noted that under a seizure analysis one's “liberty interest... is also protected by the Fourth Amendment.” Soldal v. Cook County, 506 U.S. 56, 61 (1992) (internal citations and quotation marks omitted). For example, in a case involving law enforcement detaining luggage, “the police conduct intrude[d] both the suspect's possessory interest in his luggage as well as his liberty interest in proceeding with his itinerary.” United States v. Place, 462 U.S. 696, 708 (1983).

An analysis of the defendant's use of the aircard Internet connection supports his liberty interest of the type discussed in Place. For example, from approximately June 5, 2007 to October 9, 2007, the defendant used the aircard, host laptop computer, and aircard service to advance the beliefs and ideals of the 2008 Ron Paul Presidential Campaign by engaging in interactive televised debates.[1145] Up to the time of his arrest, the defendant

---
1142. See fn. No. 1142, supra (referencing exhibit containing pictures).
1143. See EXHIBIT 076 of 2nd Consolidated Exhibits (Dkt. #821-4) (government's picture (cropped) of the defendant's “Black Adidas 'Clima 365' pants with three white stripes" seized from apartment No. 1122 on August 3-4, 2008); EXHIBIT 083 of 2nd Consolidated Exhibits (Dkt. #821-5) (N.D.Cal. 08-70503-PVT search warrant return listing the defendant's “Black Adidas 'Clima 365' pants with three white stripes”).
1144. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 21-25, p. 7-9.
1145. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 23, p. 8 (“By using my aircard and aircard account to participate in web based polls to vote Ron Paul as...”)
also used his aircard to associate with other Ron Paul supporters via Internet services such as web based polls, YouTube videos, and chatrooms. [1146] At the time of the seizure on August 3-4, 2008, the defendant's home computer contained various political material including Ron Paul videos [1147] and web pages [1148] relating to the 2008 Ron Paul Presidential Campaign that were all downloaded by the defendant via the aircard service. Additionally, from October 21, 2007 through August 3, 2008, the defendant used his aircard, host laptop computer, and aircard service as his only Internet connection for his home computer at apartment No. 1122. [1149] For example, the defendant used his home Internet connection to visit websites such as youtube.com, costco.com, funtrivia.com, digg.com, facebook.com, dictionary.com and many others. [1150]

C. The defendant's reasonable expectation of privacy in various places, objects, records, resources, and combinations thereof.

Establishing a reasonable expectation of privacy is a higher standard than establishing a mere property or possessory interest. “The existence of a property right is but one element in determining whether expectations of privacy are legitimate.” Oliver v. United States, 466 U. S. 170, 183 (1984). When conducting a Katz reasonable-expectation-of-privacy analysis,

the debate winner for each debate, I expressed myself by affecting the debate candidate overall online poll rankings that were aired to viewers and published on the web.”

1146. See id., ¶ 24, p. 9.

1147. See defendant's declaration accompanying this memorandum RE: Data extracted from hard drive images corresponding to seized hard drives connected to Daniel Rigmaiden's home computer; ¶ 6-7, p. 2-4 & Attachment Nos. 05-12 (screenshots of select video frames of various YouTube Flash videos relating to the 2008 Ron Paul Presidential Campaign downloaded by the defendant using his home computer and aircard Internet connection prior to his arrest).

1148. See id., ¶ 4-5, p. 2 & Attachment Nos. 02-04 (PDF prints of web pages relating to the 2008 Ron Paul Presidential Campaign archived by the defendant using his home computer and aircard Internet connection prior to his arrest).

1149. See also EXHIBIT 096 of 2nd Consolidated Exhibits (Dkt. #821-5) (letter/notice that no Comcast Cable Communications, LLC customer or subscriber information (i.e., no Internet service) is associated with 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050).

1150. See defendant's declaration accompanying this memorandum RE: Internet activity reflected by the 1,836,140 aircard destination IP addresses seized by the government, Attachment No. 01 (Chart Of Excerpt Of Websites Accessed By Aircard From May 11, 2008 Through July 9, 2008).
the Fourth Amendment applies when an individual has “exhibited an actual (subjective) expectation of privacy” and the individual's subjective expectation of privacy is “one that society is prepared to recognize as reasonable.” Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Determining whether a defendant has a reasonable expectation of privacy is considered a two-part test addressing both the subjective and objective component. See Smith v. Maryland, 442 U.S. 735, 740-41 (1979). A subjective expectation of privacy is shown to be objectively reasonable “either by references to concepts of real or personal property law or to understandings that are recognized and permitted by society.” United States v. Thomas, 447 F.3d 1191, 1197-98 (9th Cir. 2006) (internal quotation marks omitted) (citing Minnesota v. Carter, 525 U.S. 83, 88 (1998)). In Nerber, the Ninth Circuit indicated that court's should consider “the totality of the circumstances... including but not limited to the nature of the government intrusion,” United States v. Nerber, 222 F.3d 597, 600 (9th Cir. 2000), when determining whether an individual had a reasonable expectation of privacy. Therefore, following Nerber, the Court should consider the numerous Fourth Amendment intrusions conceded by the government when determining whether the defendant had a reasonable expectation of privacy. See Argument, Section V(D), (E) and (F), infra (discussing searches and seizures). The proceeding subsections apply the above cited case law while establishing the defendant's reasonable expectation of privacy in various places, objects, records, resources, and combinations thereof.

1. The defendant had a reasonable expectation of privacy in his home residence, i.e., apartment No. 1122.

   a. The defendant's reasonable expectation of privacy in his home as a baseline matter.

   Apartment No. 1122 was the defendant's home for approximately 9.5 months until his arrest on August 3, 2008. As explained below, the totality of the circumstances supports the defendant's reasonable expectation of privacy in that Fourth Amendment protected space. See United States v. $40, 955.00 in United States Currency, 554 F.3d 752, 757 (9th Cir. 2009) (Determining whether an individual “had a legitimate expectation of privacy in the home,...
[requires] looking at the totality of circumstances.”). The defendant rented apartment No. 1122 solely as a home residence and conducted no business from within the apartment or through the apartment mailing address.[1151] See New York v. Berger, 482 U.S. 691, 700 (1987) (“An expectation of privacy in commercial premises... is different from, and indeed less than, a similar expectation in an individual's home.”). The defendant kept personal belongings at his residence such as his electric razor, toothbrush, dental picks, comb, and clothing.[1152] The defendant slept at his residence, ate at his residence, used his home Internet connection at his residence, and paid for the Silicon Valley Power electricity provided to his residence.[1153] When he rented apartment No. 1122, the defendant was mindful of the virtually impenetrable Domicilio security features protecting its residents[1154][1155][1156][1157] and those features played a large role in his choice to rent apartment No. 1122.[1158] See United States v. Sandoval, 200 F.3d 659, 600 (9th Cir. 2000) (Finding that defendant had a subjective expectation of privacy because the area surrounding his home was “virtually impenetrable.”). Additionally, other than for very brief periods, the

1151. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 1, p. 1.

1152. See EXHIBIT 083 of 2nd Consolidated Exhibits (Dkt. #821-5) (N.D.Cal. 08-70503-PVT search warrant return listing the defendant's household items and clothing).

1153. See Argument, Section V(A)(4), supra (discussing defendant's property and possessory interest in his Silicon Valley Power account No. 00070682-04 and referencing supporting declaration and exhibits).

1154. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 2, p. 1-2.

1155. See EXHIBIT 31 of 1st Consolidated Exhibits (Dkt. #587-2) (Domicilio apartment complex brochure indicating “built in intrusion alarms.”).

1156. See General Facts, Section IV(B)(12), supra (discussing electronic gates at Domicilio).

1157. See EXHIBIT 32 of 1st Consolidated Exhibits (Dkt. #587-2) (Google Maps screen shot showing how road vehicle access areas nearest to apartment No. 1122 are approximately 248 ft, 300 ft, 364 ft, and 455 ft away from the residence).

1158. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 2, p. 1-2.
defendant always kept his blinds closed and door locked.\[1159\] See Nerber, 222 F.3d at 603 (Noting an individual's actions in “closing the door, drawing the blinds, and exercising dominion over the room...” while finding a reasonable expectation of privacy in the invaded space.). The defendant never invited a stranger into his home and he never answered his door to an uninvited or unexpected visitor.\[1160\] The defendant's reasonable expectation of privacy is also supported by his exclusive property and possessory rights to apartment No. 1122 as the sole lease holder and occupant.\[1161\] See Thomas, 447 F.3d at 1197-98.

b. The defendant's use of an alias does not act to destroy his reasonable expectation of privacy in his home.

Use of an alias had no effect on the defendant's reasonable expectation of privacy in his home residence. Notwithstanding the fact that the defendant rented his apartment under an alias, he always legitimately paid his rent using money orders that he purchased with physical cash and management never attempted to evict the defendant or repossess the apartment.\[1162\] In the context of a hotel room rented through credit card fraud, the Ninth Circuit held that “the occupant’s protected Fourth Amendment expectation of privacy is not finally extinguished until the hotel justifiably takes 'affirmative steps to repossess the room.'” United States v. Cunag, 386 F.3d 888 (9th Cir. 2004); see also United States v. Bautista, 362 F.3d 584, 590 (9th Cir. 2004) (same). In Cunag, the noted “fraud” was actually theft considering the lessee attempted to pay for the room using a stolen credit card. In the present case, the defendant's reasonable expectation of privacy in apartment No. 1122 is well above Cunag's considering no theft was committed. The defendant did not attempt to defraud the Domicilio apartment complex out of due rent but simply rented the apartment under his alias. The defendant was a model tenant\[1163\] for over nine months and paid his rent each and

\[1159\] See id., ¶ 4, p. 2.
\[1160\] See id.
\[1161\] See Argument, Section V(A)(1), supra (discussing defendant's property and possessory interest in apartment No. 1122 and referencing supporting declaration and exhibits).
\[1162\] See id.
\[1163\] Domicilio was satisfied enough with the defendant as a renter that he was invited to
every month using legitimate money orders.[1164] Even if renting an apartment under an
alias can somehow be construed as “defrauding” the Domicilio apartment complex, the
defendant is still protected by the reasoning of Cunag and Bautista considering management
was unaware of the issue and never took steps to evict the defendant. *See, e.g.*, Cunag, 386
F.3d 888, 895 (“[A] justifiable affirmative act of repossession by the lessor is the factor that
finally obliterates any cognizable expectation of privacy a lessee might have.” (internal
citation and quotation marks omitted)); *see also* United States v. Young, 573 F.3d 711, 719-
720 (9th Cir. 2008) (“Here, the district court acknowledged the possibility of fraud, but...
hotel management was completely unaware of such a possibility and that, as a result, the
alleged fraud did not destroy Young's expectation of privacy in the room...”).

Under a slightly different analysis, individuals who are not lease holders still maintain
a reasonable expectation of privacy in a residence when that residence is their home or
overnight resting place. *See Carter*, 525 U.S. 83 at 90 (“[A]n overnight guest in a home may
claim the protection of the Fourth Amendment...” if there is “a degree of acceptance into the
household.”); United States v. Davis, 932 F.2d 752, 757 (9th Cir. 1991) (finding a legitimate
expectation of privacy existed where the guest had previously lived in the apartment, kept a
key, stored his personal belongings there, and continued to pay a portion of the rent). As
established *supra*, the defendant meets all of the Davis requirements. Notably, the
defendant's “ongoing obligation to pay the rent” provides for “partial or joint control over the
premises.” *Id.*[1165] “[A] defendant who lacks an ownership interest may still have standing
to challenge a search, upon a showing of 'joint control' or 'common authority' over the
property searched.” *Thomas*, 447 F.3d at 1198. Additionally, apart from the nonexistent
theft, any finding of generic “illegality,” vis-a-vis the lease for apartment No. 1122, does not
renew his lease on March 18, 2008. *See EXHIBIT 090* of *2nd Consolidated Exhibits* (Dkt.
#821-5).

1164. *See Argument*, Section V(A)(1), *supra* (discussing defendant's property and
possessory interest in apartment No. 1122 and referencing supporting declaration and
exhibits).

1165. *See also* United States v. Johns, 851 F.2d 1131, 1135-36 (9th Cir. 1998) (defendant
who was co-renter of storage unit and paid a portion of the rent had a reasonable expectation
of privacy even though defendant's name did not appear on the rental agreement).
destroy the defendant's reasonable expectation of privacy in his home. See United States v. Barajas-Avalos, 359 F.3d 1204, 1214 (9th Cir. 2004) (Interpreting Sandoval to hold that “a search of the interior of a makeshift tent violated the appellant's reasonable expectation of privacy even though he was camped illegally...” (citing Sandoval, 200 F.3d at 661)); United States v. Watson, 950 F.2d 505, 507 (8th Cir. 1991) (Reasonable expectation of privacy remains even while property purchased under a fictitious name because “[l]egal ownership of a house, however, is not necessary to have a legitimate expectation of privacy in it; present dominion or control is sufficient.”).

c. The defendant's reasonable expectation of privacy in his home encompasses all effects contained therein and all geolocation records related to those effects.

As an initial matter, all of the government's hyper-technical arguments asserting that the defendant loses his reasonable expectation of privacy because of aliases, alleged illegal activity, and the third-party disclosure rule[1166] is precluded by Ninth Circuit and Supreme Court precedent. As further explained below, the defendant's reasonable expectation of privacy in his home provides protection for (1) all of his possessions within his home including his aircard and host laptop computer, and (2) the geolocation records[1167] showing the location of those objects and of the defendant within his home. As explained in Alderman, the defendant's reasonable expectation of privacy in his home protects any object within that Fourth Amendment protected space regardless of any additional application of Katz:

If the police make an unwarranted search of a house and seize tangible property belonging to third parties—even a transcript of a third-party conversation—the homeowner may object to its use against him, not because he had interest in the seized items as “effects” protected by the Fourth Amendment, but because they were the fruits of an unauthorized search of his house, which is itself expressly protected by the Fourth Amendment.


1166. The third-party disclosure rule established in the Supreme Court's Miller and Smith opinions is discussed infra.

1167. The noted geolocation records include cell site location information seized from Verizon Wireless and Domicilio gate key access records seized from Quality Alarm Service.
Similar to *Alderman*, the Supreme Court in *Karo* reasoned that respondents had no legitimate expectation of privacy in a can of ether containing a beeper placed there by the government but still found that “those with privacy interests in the house” where the beeper was used could still challenge use of the beeper under the Fourth Amendment. *United States v. Karo*, 468 U.S. 705, 718 (1984).[1168] The government's arguments relating to use of aliases, alleged illegal activity, and the third-party disclosure rule are also at odds with the Ninth Circuit opinion in *United States v. Issacs*, 708 F.2d 1365 (9th Cir. 1983). In *Issacs*, the Ninth Circuit found that “[t]he government's concession that Issacs had a legitimate expectation of privacy in the invaded place... precludes its contention that he had none in the items found there.” *Issacs*, 708 F.2d at 1368 (citation and quotation marks omitted).[1169] In the present case, the government already conceded that the “Defendant still had a reasonable expectation of privacy in the apartment itself...” Government’s Memorandum Regarding Law Enforcement Privilege And Request For An Ex Parte And In Camera Hearing If Necessary, p. 22 fn. 3 (Dkt. #465, p. 22). Additionally, the defendant explained how he maintained a reasonable expectation of privacy in his home in Section V(C)(1)(a), *supra*. Therefore, “the distinction the government seeks to draw between an expectation of privacy in the space invaded and the items seized is untenable.” *Issacs*, 708 F.2d at 1368.

2. **The defendant had a reasonable expectation of privacy in his aircard and host laptop computer.**

   a. **The defendant's reasonable expectation of privacy in his aircard and host laptop computer as a baseline matter.**

   An analysis of the facts and relevant case law supports a finding that the defendant had a subjective expectation of privacy in his aircard and host laptop computer that society is prepared to accept as reasonable. It is generally understood by society that personal

---

1168. See also *United States v. Coverson*, No. 3:09-CR-00075-TMB, Doc. #301, p. 12-13 (D.Alaska, Jun. 30, 2011) (Holding that defendant could raise Fourth Amendment challenge to government's electronic tracking of a sham package to his residence despite having no reasonable expectation of privacy in the package containing the beeper.).

1169. In *Issacs*, the Ninth Circuit found that the defendant had a reasonable expectation of privacy in journals seized from his personal safe even while he flat out denied ownership of the journals. See *Issacs*, 708 F.2d 1365.
computers and communications devices are considered to be highly private. See, e.g., United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (“[A]s a general matter an individual has an objectively reasonable expectation of privacy in his personal computer[.]” (citing United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007))); United States v. Davis, 787 F. Supp. 2d 1165, 1170 (D.Or. 2011) (As a general matter, “[a] person has a reasonable expectation of privacy in his personal cell phone...”). The defendant was also the sole owner and possessor of the aircard and host laptop computer. Although not a requirement, “ownership and possession of... the good... is certainly an important factor in determining whether a defendant has a legitimate expectation of privacy in it.” $40,955.00 in United States Currency, 554 F.3d at 756. Additionally, the defendant never once let anyone use his aircard or host laptop computer for any purpose and he always stored the devices behind lock and key in his home or kept them with him at all times for the sole purpose of preventing other people from using them. See Rakas v. Illinois, 439 U.S. 128, 143 fn. 12 (1978) (“One of the main rights attaching to property is the right to exclude others.”). Likewise, the defendant never consented to having FBI agents access or use his aircard and host laptop computer for their own purpose.

In the context of the government's aircard locating mission, the defendant was not publicly exposing his location or the location of the aircard within the confines of apartment No. 1122. The government did not have a prior visual or informational fix on either the

1170. When the defendant's home computer was seized, it contained his personal files such as documents and videos relating to his political associations. See defendant's declaration accompanying this memorandum RE: Data extracted from hard drive images corresponding to seized hard drives connected to Daniel Rigmaiden's home computer.

1171. See Argument, Sections V(A)(2) and (3), supra (referencing supporting declaration and exhibits).

1172. See also United States v. Salvucci, 448 U.S. 83, 92 (1980) (“[P]roperty ownership is clearly a factor to be considered in determining whether an individual’s Fourth Amendment rights have been violated...” (citation omitted)).

1173. See Argument, Sections V(A)(2) and (3), supra (referencing supporting declaration and exhibits).

1174. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 3, p. 6.

1175. The defendant always kept his blinds drawn and door locked. See Argument, Section
location of the aircard or the defendant prior to using geolocation techniques and
surveillance equipment to locate the aircard and the defendant precisely inside his home.

[1176] The defendant's subjective expectation of privacy in his location and in the location of
the aircard was objectively reasonable considering it is well understood by society that “the
Fourth Amendment draws ‘a firm line at the entrance to the house,’” Kyllo v. United States,
533 U.S. 27, 40 (2001) (internal citation omitted), and “[i]ndiscriminate monitoring of
property that has been withdrawn from public view would present far too serious a threat to
privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.”
Karo, 468 U.S. at 716.

b. The defendant's use of aliases does not act to destroy his
reasonable expectation of privacy in his aircard and host
laptop computer.

Any government claim that an abstract association with an alias caused the defendant
to lose his reasonable expectation of privacy in the aircard and host laptop computer, while
those items were located in his home, is at odds with fundamental Fourth Amendment
interpretation. See Argument, Section V(C)(1)(c), supra; Alderman, 394 U.S. at 176-77
(reasonable expectation of privacy in home protects all items within). However, even if the
Court rejects an application Alderman, the defendant still maintained a reasonable
expectation of privacy in his aircard and host laptop computer vis-a-vis any use of an alias.
First, the defendant acquired the aircard and host laptop computer through legitimate
purchases using his own money.[1177] Neither device was stolen or fraudulently obtained
and the defendant continues to own the devices to this day. Second, the defendant did not
provide any name when making the cash purchase of the aircard[1178] so any government

V(C)(1)(a), supra (referencing supporting declaration); Nerber, 222 F.3d at 603.

1176. See Government's Memorandum RE Motion For Discovery (Dkt. #674, p. 2) (“[T]he
United States will agree to allow the Court to factually assume, that, at the conclusion of the
July 16, 2008, aircard tracking operation, the FBI located the aircard within Unit 1122 of the
Domocilio [sic] Apartments.” (footnote omitted)); see also January 4, 2012 Court Order
(Dkt. #723, p. 15) (noting the government's concession).

1177. See Argument, Sections V(A)(2) and (3), supra (discussing defendant's property and
possessory interest in his laptop computer and aircard and referencing supporting declaration
and exhibits).

1178. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden
argument relating to an alias is largely inapplicable to that device. Third, the alias provided
when purchasing the host laptop computer was done solely for billing/shipping
purposes[1179] and was not done to commit a theft.[1180] There is simply no support for the
government's “use of aliases” argument with respect to the aircard and host laptop computer.

The government continues to rely on United States v. Caymen, 404 F.3d 1196 (9th Cir.
2005) in support of its argument that using an alias to obtain an item is a type of “fraud” that
somehow destroys one's reasonable expectation of privacy in that item.[1181] In Caymen, the
Ninth Circuit reiterated the lower court's analogy that Caymen's fraudulent use of a credit

card to purchase a computer is the same as “a person going into a computer store, stealing a

computer, claiming that he paid for it, and using it as if it was his own.” Id. at 1200. The

Ninth Circuit upheld the warrantless search of Caymen's computer because “[t]he Fourth

Amendment does not protect a defendant from a warrantless search of property that he

stole...” Id. (“Caymen did not submit an affidavit or other evidence supporting his claim that

he had honestly purchased and owned the laptop.”). The government is comparing apples to

oranges because, as previously noted, neither the aircard nor the host laptop computer were

stolen. Caymen was also not in possession of the computer at the time of the search. See id.
at 1199. In the present case, the defendant was in possession of both the aircard and host

laptop computer during the time of the aircard locating mission. The Caymen court noted

that if Caymen had been in possession of the computer at the time of the search then it would

“raise the questions at issue in cases where a guest is still using a room that he obtained by

fraudulent use of a credit card.” Id. (footnote omitted) (citing Cunag, 386 F.3d 888; Bautista,

362 F.3d 584). In other words, had Caymen been in possession of the stolen computer, he

would have maintained his reasonable expectation of privacy at least until the store took

owns the aircard and used the aircard service as a home Internet connection, ¶ 2, p. 1-2.

1179. See id., ¶ 4, p. 2-3; Argument, Section V(A)(3), supra.

1180. See id. (explaining how Lenovo records indicate a legitimate purchase and how the

Wired Plastic prepaid debit card used by the defendant to make the purchase is still in good

standing).

1181. See, e.g., Government's Response To Motion For Discovery (Dkt. #602, p. 7 fn. 2)

(citing Caymen); Government's Memorandum RE Motion For Discovery (Dkt. #746, p.2

(same)).
3. The defendant had a reasonable expectation of privacy in the aircard account.

First, whether the defendant had a reasonable expectation of privacy in the aircard account is completely irrelevant to the FBI's execution of the N.D.Cal. 08-90330MISC-RS order and use of its own surveillance equipment. The aircard was not connected to Verizon Wireless but instead to the FBI's emulated cellular network while technical agents used their portable/transportable wireless device locators to locate the aircard inside the defendant's home. Whether the defendant had a reasonable expectation of privacy in the aircard account only holds marginal relevance to the government's seizure of stored aircard account records in the possession of Verizon Wireless.

Under ordinary circumstances, a user's baseline reasonable expectation of privacy in a wireless account would be taken as a given and the analysis would continue on to a third-party disclosure rule test applicable to the seized records. However, the defendant opened the aircard account while using his alter ego of Travis Rupard, which is a factor some courts take into consideration when determining whether an account user had a reasonable expectation of privacy in seized account records. See, e.g., United States v Suarez-Blanca, No. 1:07–CR–0023–MHS/AJB, 2008 WL 4200156, p. 7 (N.D.Ga., Apr. 21, 2008) (addressing "challenge [to] law enforcement's ability to obtain historical cell cite information" relating to account opened under fictitious name); United States v. Skinner, No. 3:06–CR–100, 2007 WL 1556596, p. 4 (E.D.Tenn., May 24 2007) (addressing government obtaining "latitude and longitude data provided from the telephone company" for account opened under fictitious name); United States v. Davis, No. 10-CR-00339-HA, 2011 WL 2036463, p. 3 (D.Or., May 24, 2011) (addressing "privacy interest in the cell phone records" relating to account opened under fictitious name). Each court in the cases cited above found that obtaining a wireless account under a fictitious name partially contributed to its finding...
that the account user had no reasonable expectation of privacy in the account records. The
cases cited above were decided based on a totality of the circumstances and, as explained
below, the facts of the present case are easily distinguishable.

In Suarez-Blanca, the court found that a defendant had no reasonable expectation of
privacy in cell site information because “he simply [] failed to tie himself in any way to the
subscriber[.]”  

Suarez-Blanca, 2008 WL 4200156 at p. 7 (emphasis added). In Skinner, the
court found that a defendant did not have standing to object to the government obtaining
latitude and longitude data from the wireless carrier “because he neither purchased the phone
nor was the listed subscriber[ ] [and] the phone was purchased [by another] and provided...
solely for effectuating drug trafficking.”  

Skinner, 2007 WL 1556596 at p. 15. In Davis, the court found that a defendant had no reasonable expectation of privacy in various cell
phone records in part because he “presented no evidence... that he used an alias to obtain the
phone.”  

Davis, 2011 WL 2036463 at p. 3. Contrary to the above, the defendant in the
present case (1) purchased and owns the aircard, (2) purchased and owns the host
laptop computer, (3) personally signed up for aircard service as Travis Rupard,

1182. In making its conclusion, the Skinner court partially relied on Diaz which is contrary
to controlling Ninth Circuit precedent discussed in Cunag, Bautista, and Cayman. See
Skinner, 2007 WL 1556596 at p. 17 (Holding cell phones analogous to hotel rooms and
noting the Diaz finding that “[w]here a hotel room was procured under a false name and paid
for with a fraudulent credit card, no legitimate expectation of privacy in the room existed.”
(D.V.I., Sept. 10, 1998)). Diaz was decided not on the issue of aliases but because the
renters “were the equivalent of the off-season burglar and not the paying hotel guest.”  

Diaz, 1998 U.S. Dist. LEXIS 14539 at p. 72. As previously indicated, the defendant in the present
case legitimately purchased his possessions and legitimately paid his rent and bills.

1183.  See Argument, Section, V(A)(2), supra (establishing the defendant's property and
possessory interest in the aircard).

1184.  See Argument, Section V(A)(3), supra (establishing the defendant's property and
possessory interest in the host laptop computer).

1185.  See defendant's declaration accompanying this memorandum RE: Daniel Rigmaden
owns the aircard and used the aircard service as a home Internet connection, ¶ 7, p. 3-4.
was the subscriber to the aircard account for more than two years,

had billing records saved on his computer,

was using the aircard, host laptop computer, and aircard service as a home Internet connection for purposes that were not criminal in nature,

(7) repeatedly paid the aircard account bill by personally visiting Verizon Wireless stores, and (8) interacted with Verizon Wireless employees as Travis Rupard. The government also has a video of the defendant paying the aircard account bill as Travis Rupard.

Even if the defendant was in violation of the Verizon Wireless service contract due to use of an alias, the Ninth Circuit “previously held that a privacy interest exists even if a defendant is in technical violation of a leasing contract.” Thomas, 447 F.3d at 1198 (citation omitted).

See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 7, p. 3-4.

See defendant's declaration accompanying this memorandum RE: Data extracted from hard drive images corresponding to seized hard drives connected to Daniel Rigmaiden's home computer, ¶ 8, p. 4 & Attachment No. 15 (the defendant's Verizon Wireless aircard account bill found on his computer by the government); see also EXHIBIT 079 of 2\textsuperscript{nd} Consolidated Exhibits (Dkt. #821-4) (June 25, 2008 email from IRS-CI Agent Daun to IRS-CI Agent Medrano et al.: RE: aircard account login records found on the defendant's computer seized from apartment No. 1122 with tr_verizon_info.txt attachment).

See defendant's declaration accompanying this memorandum RE: Internet activity reflected by the 1,836,140 aircard destination IP addresses seized by the government, Attachment No. 01 (Chart Of Excerpt Of Websites Access by Aircard From May 11, 2008 Through July 9, 2008); defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 21-25, p. 7-9.

See Argument, Section V(B), supra (explaining the defendant's legitimate use of the aircard including First Amendment protected activity).

Nevertheless, the Ninth Circuit “previously rejected the argument that a person lacks a subjective expectation of privacy simply because he is engaged in illegal activity...” Sandoval, 200 F.3d at 660 (citing United States v. Gooch, 6 F.3d 673 (9\textsuperscript{th} Cir. 1993)).

See Argument, Section V(A)(5), supra; Defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 8, p. 4.

See id., ¶ 9, p. 4.

See EXHIBIT 075 of 2\textsuperscript{nd} Consolidated Exhibits (Dkt. #821-4) (images of the defendant paying his aircard account bill while wearing his “Black Adidas 'Clima 365'” pants with three white stripes, extracted from June 12, 2008 video camera footage for Verizon Wireless store located at 768 Market St., San Francisco, CA, 94102); EXHIBIT 074 of 2\textsuperscript{nd} Consolidated Exhibits (Dkt. #821-4) (FBI FD-302 report of investigation conducted on July 17, 2008 by FBI Agent Murray RE: subpoenaed DVD of June 12, 2008 video camera footage for Verizon Wireless store located at 768 Market St., San Francisco, CA, 94102 where aircard payment was made).
In further support of the defendant's reasonable expectation of privacy in the aircard account, the wireless industry does not mind the use of aliases to sign up for wireless service. At the 2009 IIS World Conference, a law enforcement representative informed the wireless industry that he had previously obtained phone records in the name of “Mickey Mouse” and asked why wireless carriers cannot implement a system that would prevent use of fictitious names when applying for cell phone service. In response to the question, Sprint-Nextel employee Paul Taylor answered, “It's called revenue.... Where you don't have it, sales go up.” After law enforcement further pressed the issue, the host of the panel, who has ten years of telecommunications industry experience, further explained that “those..., DEA, investigations we used to see with the prepaid calls, those people be putting five hundred bucks a day on those phone calls, they're some of the best customers that a company had...” Use of aliases to sign up for wireless service is a practice that is recognized and tolerated by the wireless industry so it should not act to vitiate the defendant's reasonable expectation of privacy in the aircard account.

4. The defendant had a reasonable expectation of privacy in his historical cell site location information seized from Verizon Wireless.

a. The defendant's reasonable expectation of privacy is grounded by the government's search by inference.

Using the historical cell site location information seized from Verizon Wireless, the government was able to infer that the defendant was located precisely in his home at various times over a 38 day period. See Kyllo, 533 U.S. at 33-34 (Rejecting the “dissent's extraordinary assertion that anything learned through 'an inference' cannot be a search[.]”).

The FBI's real-time locating efforts conducted on July 16-17, 2008 allowed the government to...
to discover the aircard's stationary location as being precisely inside apartment No 1122. 

This discovery allowed for the government to use the first and second sets of previously obtained historical cell site location information to infer that the aircard and the defendant were located precisely inside apartment No. 1122 during the prior 38 day period. A search-by-inference of this type is often noted by legal scholars and judges while explaining why government acquisition of cell site location information implicates one's reasonable expectation of privacy. Various courts have also noted in their opinions that the government “could violate Karo if it use[s] cell site information to surveil a target in a private home that could not be observed from public spaces.” In Re: Application Of The United states For An Order For Prospective Cell Site Location Information On A Certain Cellular Telephone, 460 F.Supp.2d 448, 462 (S.D.N.Y. 2006) (“Kaplan (dj) 2006 Opinion”). The government using historical cell site location information to infer the

1198. See Government's Memorandum RE Motion For Discovery (Dkt. #674, p. 2) (“[T]he United States will agree to allow the Court to factually assume, that, at the conclusion of the July 16, 2008, aircard tracking operation, the FBI located the aircard within Unit 1122 of the Domocilio [sic] Apartments.” (footnote omitted)); see also January 4, 2012 Court Order (Dkt. #723, p. 15) (noting the government's concession).

1199. See EXHIBIT 02 of 1st Consolidated Exhibits (Dkt. #587-1) (Historical cell site location information obtained via the D.Ariz. 08-3298MB-LOA order on July 12, 2008 and covering aircard connections from June 10, 2008 12:24am through July 11, 2008 1:56pm.)

1200. See EXHIBIT 05 of 1st Consolidated Exhibits (Dkt. #587-1) (Historical cell site location information obtained via the D.Ariz. 08-7273MB-ECV order on July 31, 2008 and covering aircard connections from July 11, 2008 1:57pm through July 17, 2008 11:59am.).

1201. As previously explained in the General Facts, Section IV(B)(2), supra, the historical cell site location information allowed the government to learn that the aircard remained stationary in an area including apartment No. 1122.

1202. See Freiwald, Susan, Professor of Law, USF School of Law, “Cell Phone Location Data And The Fourth Amendment: A Question Of Law, Not Fact,” Maryland Law Review, 70 Md. L. Rev. 681, p. 725 (2011) (If agents know “where a target lives and his telephone number” then “location data that shows the target's cell phone communicated with the cell tower closest to his home indicates that the target was likely at home and on the telephone during that time.” (footnote omitted)).

1203. See ECPA Reform and the Revolution in Location Based Technologies and Services, 111th Cong. 2nd sess. (Jun. 24, 2010) (Prepared Statement of the Honorable Stephen Wm. Smith, United States Magistrate Judge, Southern District of Texas), p. 86 (PDF, p. 90) (“[W]hen law enforcement already knows the business and residential addresses of the target (or the target's family, friends, and associates), a single phone call signal captured from a single tower may be all that's needed to reliably pinpoint a target's exact location at a given time.”).
defendant's location within his home implicates the defendant's reasonable expectation of privacy in that information.\[1204\]

Additionally, the defendant's 38 day's worth of historical cell site location information allowed for the government to infer that the defendant was a consistent homebody who rarely leaves his apartment. This sort of prolonged surveillance further implicates the defendant's reasonable expectation of privacy in his location records. See United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), affirmed on other grounds 556 U.S. ___, 181 L. Ed. 2d 911 (2012) (Finding a reasonable expectation of privacy in prolonged geolocation surveillance, whether in the home or not, because it “reveals types of information not revealed by short term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble.”); \[1205\] United States v. Jones, 556 U.S. ___, 181 L. Ed. 2d 911, 934 (2012) (Alito, J. concurring) (The line where long term GPS surveillance became a search “was surely crossed before the 4-week mark.”); In The Matter Of An Application Of The United States Of America For An Order Authorizing The Release Of Historical Cell-Site Information, 10-MC-897 (NGG), Doc. #006, 2011 U.S. Dist. LEXIS 93494, p. 18 (E.D.N.Y., Aug. 22, 2011) (“Garaufis (dj) 2011 Opinion”) (Holding that “cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location records...”).

b. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in his historical cell site location information seized from Verizon Wireless.

In United States v. Miller, 425 U.S. 435 (1976), the Supreme Court rejected a Fourth Amendment challenge to a subpoena for bank records on the grounds that such documents were not “private papers” but were instead “the business records of the banks[.]” in which a 1204. In Nerber, the Ninth Circuit considered “the totality of the circumstances... including but not limited to the nature of the government intrusion,” Nerber, 222 F.3d at 600, when determining whether an individual had a reasonable expectation of privacy.

1205. The Ninth Circuit's Pineda-Moreno decision does not undermine the defendant's argument because Pineda-Moreno did not raise the issue of whether prolonged electronic surveillance constitutes a search and the type of geolocation surveillance at issue in Pineda-Moreno was conducted outside the home—not inside the home. See United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010). Nevertheless, Pinedo-Moreno is no longer good law. See Jones, 181 L. Ed. 2d 911.
customer “can assert neither ownership nor possession.” Id. at 440. In Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court expanded upon Miller and reasoned that the government's acquisition of an individual's dialed telephone numbers does not implicate the Fourth Amendment because “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” Id. at 743-44. In the present case, the government attempts to equate the defendant's geolocation records in the possession of Verizon Wireless to the business documents discussed in Miller and to the dialed telephone numbers discussed in Smith.[1206] The subsections that follow explain why Miller and Smith do not undermine the defendant's reasonable expectation of privacy in his historical cell site location information.

i. The government's reliance on Miller fails because Verizon Wireless was not party to the defendant's communications and his cell site location information does not constitute routine business records.

First, the reasoning in Miller does not apply because Verizon Wireless was not acting as a party to any transaction and was instead acting as a neutral service provider intermediary. The Supreme Court's basis for its holding in Miller was that “banks are not neutrals in transactions involving negotiable instruments, but parties to the instruments,” and the records “pertain to transactions to which the bank was itself a party.” Miller, 425 U.S. at 440, 441 (brackets, ellipsis, and citation omitted). In contrast, Verizon Wireless was not party to the defendant's communications and was instead a provider of an “electronic communications service” which “provides to users thereof the ability to send or receive wire or electronic communications” to others. 18 U.S.C. § 2510(15). The reasoning in Miller that banking activities are analogous to confiding in one's friend[1207] carries over poorly to geolocation records relating to electronic communications confided in by individuals apart

1206. See, e.g., Government’s Memorandum Regarding Law Enforcement Privilege And Request For An Ex Parte And In Camera Hearing If Necessary, p. 19 (Dkt. #465, p. 19) (“defendant does not have a reasonable expectation of privacy concerning the cell-site records maintained by Verizon Wireless. These cell-site records are the business records maintained by a third-party carrier as part of the ordinary course of business,...” (citing Smith)).

1207. See Miller, 425 U.S. at 443.
from the wireless carrier. The second reason *Miller* is inapplicable is because the historical cell site location information seized by the government does not constitute Verizon Wireless' routine business records. The *Miller* court indicated that there is no reasonable expectation of privacy in bank checks and deposit slips considering they are “exposed to their employees in the ordinary course of business” and are “business records of the banks.” *Miller*, 425 U.S. at 442, 440. In contrast, the Verizon Wireless Excel documents listing the defendant's historical cell site location information look nothing like a customer bill or other business document. \[1208\] Additionally, the metadata\[1209\] for the Excel documents provided to the government by Verizon Wireless indicates that the records were compiled by Verizon Wireless' Law Enforcement Resource Team on the same day the records were given to the FBI.\[1210\] The Excel documents were clearly created upon government instruction using records drawn from a set of raw technical data and are not themselves preexisting Verizon Wireless business records. This fact becomes further evident by comparing the original set of historical cell site information, compiled into an Excel document by Verizon Wireless employee Marko Denton on July 12, 2008,\[1211\] to the duplicate set of historical cell site information covering
the same date/time range but compiled into an Excel document by Verizon Wireless employee John Profaca on August 1, 2008. The two documents contain the same historical cell site location information, covering June 10, 2008 through July 11, 2008, but are formatted entirely different and even contain different categories of supportive cell site information. The documents show that they were not kept in the ordinary course of business and were instead created on-the-fly by Verizon Wireless law enforcement liaisons using raw data maintained solely for law enforcement purposes. See, e.g., In The Matter Of The Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government, 534 F.Supp.2d 585, 615 (W.D.Pa. 2008), vacated on other grounds, 620 F.3d 304 (3rd Cir. 2010) (“Lenihan (mj) 2008 Opinion”) (Rejecting the third-party disclosure rule because historical cell site location information is not used in the “ordinary course of the provision of telephone communications services” and is instead “retained principally, if not exclusively, in response to Government directive.” (footnote omitted)). Notably, Verizon Wireless considers its records of the “Cell towers used by phone” to be so insignificant to its business model that it only stores them for “1 rolling year.”

1212. See EXHIBIT 03 of 1st Consolidated Exhibits (Dkt. #587-1) (Verizon Wireless August 1, 2008 response to D.Ariz. 08-3298MB-LOA order fulfilled by John Profaca, Verizon Wireless law enforcement liaison).

1213. Entire columns of data present in the cell site information provided by John Profaca on August 1, 2008—namely, the MSID, MOU, and KBU columns—are not present in the cell site information provided to the government by Marko Denton on July 12, 2008. Additionally, various identical data fields contained in the two sets of data (covering the same date/time ranges) have different data value formats such as the “Switch” data field.

1214. Mj’s order vacated on other grounds by In The Matter Of The Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government, 620 F.3d 304 (3rd Cir. 2010).

ii. The government's reliance on Smith fails because the defendant did not knowingly or voluntarily convey his location information to Verizon Wireless.

The reasoning in Smith does not apply because the defendant did not knowingly or voluntarily convey his geolocation information to Verizon Wireless. The Supreme Court's basis for its holding in Smith was that “[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company... [and] that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.” Smith, 442 U.S. at 742. Contrary to the dialed numbers in Smith, the defendant had no idea that Verizon Wireless collected historical cell site location information on his aircard use. Additionally, the defendant's aircard account bills do not list geolocation information. See Lenihan (mj) 2008 Opinion, 534 F.Supp.2d at 590 fn. 20 (“Although historic call-specific registration information was at one time important for [] [wireless carrier] billings, e.g., roaming charges, with the advent of truly national networks and comprehensive cell phone 'plans', it has become increasingly irrelevant to service fees.”); In re Application Of The United States Of America For Historical Cell Site Data, 747 F.Supp.2d 827, 844 (S.D.Tex. 2010) (“Smith (mj) 2010 Opinion”) (Rejecting application of the third-party disclosure rule because “[u]nlike the bank records in Miller or the phone numbers dialed in Smith, cell site data is neither tangible nor visible to a cell phone user.”); In The Matter Of The Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government, 620 F.3d at 317 (Reasoning that “it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information.” (emphasis in original)).

1216. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 12, p. 5.

1217. Compare EXHIBIT 02 of 1st Consolidated Exhibits (Dkt. #587-1) (Verizon Wireless historical cell site information for the aircard provided in response to D.Ariz. 08-3298MB-LOA order) with defendant's declaration accompanying this memorandum RE: Data extracted from hard drive images corresponding to seized hard drives connected to Daniel Rigmaiden's home computer, ¶ 8, p. 4 & Attachment No. 15 (the defendant's Verizon Wireless aircard account bill found on his computer by the government).
In the last case cited above, the Third Circuit rejected a government argument that historical cell site location information is sent voluntarily and instead agreed with the Electronic Frontier Foundation that “the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller[.]” \(\text{Id. at 318} \) (internal citation omitted).

The same reasoning that applies to cell phones making telephone calls applies equally well to the defendant using his aircard to make cellular data connections.\(^{1219}\) Considering the defendant lacked the requisite knowledge and intent, the third-party disclosure rule should not act to vitiate his reasonable expectation of privacy in his historical cell site location information.

iii. In any event, the Court should find an exception to the third-party disclosure rule considering Verizon Wireless is a service provider intermediary and location information is objectively recognized as highly private.

Even if the Court finds that the defendant accessing Verizon Wireless cell sites amounts to a voluntary disclosure of cell site location information, Verizon Wireless' mere ability to access that information does not defeat the defendant's reasonable expectation of privacy in records showing his location. Various courts have reached the same conclusion while addressing disclosure of communications content accessible by third-party service provider intermediaries. \(\text{See, e.g., Quon v. Arch Wireless, 529 F.3d 892, 905 (9th Cir. 2008), reversed on other grounds, California v. Quon, 130 S. Ct. 2619 (2010) ("[U]sers do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider[]" and the service provider being “able to access the contents of the messages for its own purposes is irrelevant."); United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (An “ISP's control over [][a user's] emails and ability to access them under certain limited}

\(1218\). \(\text{See also U.S. Dep't of Justice, Electronic Surveillance Manual, Electronic Surveillance Unit, Office of Enforcement Operations, Criminal Division (Washington, DC: rev. June 2005), p. 40 ("The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user.").}\)

\(1219\). The Third Circuit's reasoning applies even more so in the present case considering the defendant's aircard data connections did not even require him to dial any telephone numbers and only required that he click a “connect” button using his laptop computer.
circumstances will not be enough to overcome an expectation of privacy.”); United States v. Long, 64 M.J. 57, 63 (C.A.A.F. 2006) (Consent to monitoring did not imply consent to “engage in law enforcement intrusions... in a manner unrelated to the maintenance of the e-mail system.”).[1220]

The cases cited above apply what Judge Garaufis recently referred to as the “content exception” to the third-party disclosure rule. See Garaufis (dj) 2011 Opinion, 2011 U.S. Dist. LEXIS 93494 at p. 26-30. “In such cases, society's recognition of a particular privacy right as important swallows the discrete articulation of Fourth Amendment doctrine in Smith.” Id. at p. 30 (footnote omitted). Similar to the “content exception,” Judge Garaufis found an exception to the third-party disclosure rule for historical cell site location information because (1) unlike the bank in Miller, the information is in the possession of a “service-provider intermediary” as opposed to a party to the transaction, and (2) unlike the phone numbers is Smith, records pertaining to one's location are “objectively recognized as highly private.” Id. at p. 34-38. Judge Garaufis also noted that “there is no meaningful Fourth Amendment distinction between content and other forms of information, the disclosure of which to the Government would be equally intrusive and reveal information society values as private.” Id. at p. 34.

In the present case, Verizon Wireless was acting as a service provider intermediary and the seized historical cell site location information showed that the defendant was located within his home at specific times over a 38 day period. Such intrusiveness lends to the

1220. In other contexts, various courts have held that “third party” access does not always vitiate a reasonable expectation of privacy in a place or object. See, e.g., Bond v. United States, 529 U.S. 334, 338-39 (2000) (a police officer's exploratory squeezing of soft-sided luggage on a bus is a search, even though a traveler knows that members of the public may touch his baggage when putting their own luggage on the rack); United States v. Fultz, 146 F.3d 1102 (9th Cir. 1998) (defendant who lived “on and off” with his friend and stored many of his belongings in closed boxes in friend's garage had a reasonable expectation of privacy in his belongings, even though those belongings were kept in a place that was not exclusively controlled by him); Stoner v. California, 376 U.S. 483, 489 (1964) (search of hotel room without warrant violated Fourth Amendment even though one who engages a hotel room gives implied permission to hotel personnel to enter to perform their duties); Chapman v. United States, 365 U.S. 610, 616-18 (1961) (search of house occupied by tenant violated Fourth Amendment even though landlord had authority to enter house for some purposes).
reasoning that the third-party disclosure rule “is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.” United States v. Jones, 556 U.S. ___, 181 L. Ed. 2d 911, 926 (2012) (Sotomayor, J. concurring) There are currently more than 300 million wireless subscribers in the United States[1221] who use their wireless devices for numerous mundane tasks such as saying hello, chatting, reporting on one's whereabouts, checking in on where someone else is, doing things related to work,[1222] and accessing the Internet.[1223] Society's saturated use of wireless devices merits adopting Judge Garaufis' reasoning and finding an exception to the third-party disclosure rule.

5. The defendant had a reasonable expectation of privacy in his real-time cell site sector location information seized from Verizon Wireless.

a. The defendant's reasonable expectation of privacy in his real-time cell site sector location information based on its necessary use in pinpointing the defendant within his home.

The defendant had a reasonable expectation of privacy in his real-time cell site sector location information considering the government used that information to locate the aircard and the defendant within his home.[1224] On July 16, 2008, Verizon Wireless provided the FBI with real-time cell site sector location information which was thereafter used by agents to narrow down the geographical area of where to search for the aircard using the StingRay


1223. See id., p. 31 (37% of people surveyed in April of 2009 indicated that they use “Mobile wireless broadband, such as an AirCard, to access the internet[]” (footnote omitted)); id., p. 33 (38% of people surveyed in September of 2010 indicated that they use their cell phones to “Access the internet[]” (footnote omitted)); id., p. 35 (46% of people surveyed in April of 2009 indicated that they “use their cell phones to access the internet” anywhere from “Several times a day” to “3-5 days a week[].”).

1224. In Nerber, the Ninth Circuit considered “the totality of the circumstances... including but not limited to the nature of the government intrusion,” Nerber, 222 F.3d at 600, when determining whether an individual had a reasonable expectation of privacy.
and related equipment. Locating the aircard within the defendant's home would not have been possible if FBI technical agents were not using the SF-Martinez DCS-3000 Pen/Trap device to collect real-time cell site sector location information generated in response to the FBI's surreptitious phone calls placed to the aircard. The government's dependency on real-time cell site sector location information is made apparent by the FBI's forced generation of that data over the initial six hour period technical agents were searching for the aircard using their own equipment. As previously noted in the context of historical cell site location information, various courts have noted that the government “could violate Karo if it use[s] cell site information to surveil a target in a private home that could not be observed from public spaces.” Kaplan (dj) 2006 Opinion, 460 F.Supp.2d at 462.[1225] The same argument applies to the real-time cell site sector location information used by the FBI to surveil the defendant while he was located inside his home.

b. The defendant's reasonable expectation of privacy in his real-time cell site sector location information is supported by various statutes establishing his privacy interests.

The defendant had a reasonable expectation of privacy in his real-time cell site sector location information because federal statutes acted to protect the geolocation information generated by the FBI's surreptitious voice calls. Although the aircard only facilitates electronic communications and has no telephone capabilities, the government remotely configured the aircard to respond to its voice calls over a six hour period. The geolocation data generated in response to the government's voice calls is protected by the Wireless Communication and Public Safety Act[1226] (WCPSA), 47 U.S.C. § 222(f), and the Communications Assistance For Law Enforcement Act[1227] (CALEA), 47 U.S.C. § 1002(a).

1225. The only difference between the government's use of real-time and historical cell site location information is that the former was used as a necessary element of obtaining an absolute precise real-time location of the aircard using the StingRay and related equipment while the latter was used in conjunction with the former to obtain an inferred precise historical location of the aircard over the previous 38 day period. Other than the long-term surveillance element present with historical, both expectations of privacy are essentially synonymous because they both depend upon the defendant's undisputed reasonable expectation of privacy in his home.

(2), both of which provide support for the defendant's reasonable expectation of privacy in his real-time cell site sector location information. Relevant sections of WCPSA require that “without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to — [] call location information concerning the user of a commercial mobile service,” 47 U.S.C. § 222(f), “[e]xpect as required by law,” 47 U.S.C. § 222(c)(1), or in various emergency situations, see 47 U.S.C. § 222(d)(4). Relevant sections of CALEA indicate that an order for installation and use of a Pen/Trap device cannot “require by law” that a wireless carrier provide “any information that may disclose the physical location of the subscriber...” unless the Pen/Trap statutes are supplemented with additional adequate authority. See 47 U.S.C. § 1002(a)(2) and (a)(2)(B). The WCPSA and CALEA are sources outside the Fourth Amendment that support the defendant's reasonable expectation of privacy in his real-time cell site sector location information obtained by the SF-Martinez DCS-3000 Pen/Trap device. See Rakas, 439 U.S. at 143 fn. 12 (A “legitimate expectation of privacy must have a source outside the Fourth Amendment[.]”); Miller, 425 U.S. at 443 (looking to the Bank Secrecy Act to determine if an individual has a reasonable expectation of privacy in bank records).

c. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in his real-time cell site sector location information seized from Verizon Wireless.

In Section V(C)(4)(b) et seq., supra, the defendant explained: (1) the government's reliance on Miller fails because Verizon Wireless was not party to the defendant's communications and his cell site location information does not constitute routine business records; (2) the government's reliance on Smith fails because the defendant did not knowingly or voluntarily convey his location information to Verizon Wireless; and (3) in any event, the Court should find an exception to the third-party disclosure rule considering Verizon Wireless is a service provider intermediary and location information is objectively 1228. Considering the defendant was being located within a Fourth Amendment protected space, the required additional adequate authority should have been a probable cause warrant authorizing seizure of real-time cell site location information.
recognized as highly private. The same reasoning explained in Section V(C)(4)(b) et seq., supra,[1229] addressing why the third-party disclosure rule is inapplicable to the defendant's historical cell site location information, equally applies to the defendant's real-time cell site sector location information. There are also additional reasons as to why the third-party disclosure rule does not apply to the defendant's real-time cell site sector location information as explained in the proceeding subsections.

i. The government's reliance on Smith fails because the defendant correctly knew that Verizon Wireless did not have network infrastructure in place to obtain real-time cell site sector location information for aircard data connections.

In Section V(C)(4)(b)(ii), supra, the defendant explained that the reasoning in Smith does not apply to historical cell site location information because the defendant did not knowingly or voluntarily convey his geolocation information to Verizon Wireless.[1230] In addition to those arguments also applying here, there is further evidence showing an unknowing and involuntary disclosure of real-time (as opposed to historical) cell site location information by the defendant. First, the defendant's knowledge at the time was that real-time location information would only be conveyed to Verizon Wireless for cell phones engaged in 911 emergency phone calls.[1231] The defendant did not think that Verizon Wireless' ability to locate cell phones in emergency situations extended to aircards in general because aircards are incapable of dialing 911 or any phone number for that matter.[1232] The defendant's belief was reasonable considering relevant federal rules requiring geolocation for wireless devices only apply to emergency 911 cellular telephone calls made by cell phones, and not to

---

1229. Argument, Section V(C)(4)(b) et seq., supra, is hereby incorporated into this section by reference.

1230. See also Lenihan (mj) 2008 Opinion, 534 F.Supp.2d at 615 (Cell site location information is not “voluntarily and knowingly conveyed by cell phone users (certainly not in the way of transactional bank records or dialed telephone numbers)...” (emphasis in original)).

1231. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 13, p. 5.

1232. See General Facts, Section IV(A)(1), supra.
Second, the defendant correctly assessed that Verizon Wireless' network infrastructure was incapable of recording real-time cell site sector location information for aircard data connections regardless of any federal rules. The only way the FBI was able to obtain real-time cell site sector location information for the aircard was to engage in two separate Fourth Amendment seizures of the aircard: (1) having Verizon Wireless remotely program the aircard to act as a telephone, and (2) placing surreptitious voice calls to the aircard in order to force it to generate the sought after geolocation data. These additional unreasonable seizures do not act to vitiate the defendant's reasonable expectation of privacy vis-a-vis his unknowing and involuntary disclosure of real-time cell site sector location information to Verizon Wireless.

**ii. The government's reliance on Smith fails because the FBI was pinging the aircard in order to force it to generate real-time cell site sector location information.**

The defendant's argument that he did not knowingly or voluntarily convey his geolocation information to Verizon Wireless is further supported by the government forcing generation of real-time cell site sector location information by placing 32 surreptitious phone calls to the aircard. In *Forest*, the Sixth Circuit addressed a motion to suppress and rejected application of the third-party disclosure rule because “[u]nlike the defendant in

---

1233. Beginning in 1996, and continuing over several years, the Federal Communications Commission (FCC) issued a series of Enhanced 911 rules requiring that the majority of cell phones be locatable while making 911 emergency phone calls. Specifically, cell phones that use network based location services must be able to provide information about their location within “100 meters for 67 percent of calls, 300 meters for 95 percent of calls” by September 11, 2012. 47 C.F.R. § 20.18(h)(1) and (i) (2008).

1234. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 13, p. 5.

1235. See General Facts, Section IV(B)(6), supra (explaining how at the time of the aircard locating mission, Verizon Wireless had not yet configured its network IAPs to provide FBI DCS-3000 servers with real-time cell site location information relating to 1xEV-DO Rel. 0 data connections for aircards).

1236. See id., Section IV(B)(5), supra.

1237. See id., Section IV(B)(6), supra.

1238. See id.
Smith,” appellant “did not voluntarily convey his cell site data to anyone...” because “[t]he agent dialed [[Appellant’s] phone number and the dialing caused [[Appellant's] phone to send out signals.” United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004) (emphasis and citation omitted). Likewise, in United States v. Benford, even while finding that the third-party disclosure rule applied to historical cell site location information, the court still noted that “the situation might be different if the Government dialed an individual's cell phone number for the purpose of obtaining cell-site data to locate the individual.” Id., U.S. Dist. LEXIS 29453, No. 2:09-cr-00086-JTM-APR, Doc. #037, p. 5 (N.D.Ind., Mar. 26, 2010).

Additionally, nearly all published opinions involving judges who issue less-than-probable-cause orders for use of Pen/Trap devices to obtain real-time cell site location information do so in part because the government is not asking to place repeated calls to the wireless device in order to facilitate geolocation. See, e.g., In The Matter Of The Application Of The United States Of America For An Order: (1) Authorizing The Installation And Use Of A Pen Register And Trap And Trace Device, And (2) Authorizing Release Of Subscriber And Other Information, 622 F. Supp.2d 411, 419 (S.D.Tex. 2007) (Approving acquisition of real-time cell site location information via a Pen/Trap device as long as the government does “not place repeated calls to the cell phones in an effort to continuously track the location of the subscriber(s) or customer(s) using the Target Devices.”); In the Matter Of The Application Of The United States Of America For An Order: (1) Authorizing The Installation And Use Of A Pen Register And Trap And Trace Device, And (2) Authorizing Release Of Subscriber And Other Information, 433 F.Supp.2d 804, 806 (S.D.Tex. 2006) (Approving acquisition of real-time cell site location information via a Pen/Trap device in part because the government did not intend “to place calls to a particular cell phone repeatedly or otherwise to track on a continuous basis the location of a cell phone when no call is being placed or received.”). In the present case, not only was the government placing repeated phone calls to the aircard, the calls were not even being answered and could not have been answered considering the aircard does not have telephone capabilities. The FBI's actions in repeatedly forcing the aircard to generate real-time cell site sector location information (unbeknownst to the
6. The defendant had a reasonable expectation of privacy in his encrypted and encoded aircard signals sent over the air interface.

   a. The defendant's reasonable expectation of privacy in his “sealed” aircard signals is supported by an *Ex Parte Jackson* analogy.

   The 1xEV-DO Rel. 0 aircard signals that were accessed by the FBI right out of the air would have normally been encrypted, encoded, and inaccessible if being sent to/from a Verizon Wireless cell site. Even if the defendant's encrypted signals could have been captured, computer hardware capable of decrypting the signals (for signal identification and communications interception purposes) will not exist until the year 2017 at the absolute earliest. The 1xEV-DO Rel. 0 communications protocol encrypts and encodes transmitted signals so that they are “sealed” for transport similar to any other sealed container. The sealing of the signals acts to prevent unauthorized individuals from gaining access to signaling information and communications content. The sealed signals are similar to sealed letters and packages placed in the mail for delivery in the sense that their contents are expected to remain private. See *Ex Parte Jackson*, 96 U.S. 727, 733 (1878) (It is a Fourth Amendment search to “invade the secrecy of letters and such sealed packages in the mail[.]”). Based on this analogy, the defendant had a reasonable expectation of privacy in his encrypted and encoded aircard signals because they were inaccessible to third-party eavesdroppers under normal circumstances, *i.e.*, while the aircard was connected to actual Verizon Wireless cell sites.

   b. The defendant's reasonable expectation of privacy in his “sealed” aircard signals vis-a-vis signaling data showing the location of the aircard and the defendant within his home.

   The FBI surreptitiously forced the aircard to disconnect from Verizon Wireless and

1239. See *Technical Explanations*, Section II(B)(3)(c)(iv), *supra* (explaining the 1xEV-DO Rel. 0 encryption process at the security layer).
1240. See *id.*
then surreptitiously forced the aircard to connect to FBI controlled emulated cell sites.\footnote{1241} Whenever the aircard was connected to one of the FBI's emulated cell sites, technical agents used the equipment to mimic a Verizon Wireless cellular network in order to capture, read, and measure the defendant's encrypted and encoded aircard signals.\footnote{1242} Even if the Court approves of the FBI gaining access to encrypted and encoded aircard signals by pretending to be Verizon Wireless, the defendant still had a reasonable expectation of privacy in those signals because they contained information communicating the location of the aircard and the defendant within his home.\footnote{1243} The FBI's surveillance equipment used the aircard signals to triangulate the precise location of the aircard and the defendant through geolocation techniques, \textit{i.e.}, time-of-flight, power-distance, angle of arrival, received signal measurements, statistical functions, and data fusion.\footnote{1244} Use of the defendant's encrypted and encoded aircard signals in this manner implicates the defendant's reasonable expectation of privacy in those signals because they permitted "[i]ndiscriminate monitoring of property that ha[d] been withdrawn from public view" and this presents "far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."\footnote{Karo, 468 U.S. at 716.} Because of the highly private nature of geolocation information, the defendant's subjective expectation of privacy in his encrypted and encoded aircard signals was objectively reasonable.

c. **The defendant's reasonable expectation of privacy in his "sealed" aircard signals is supported by FCC regulations banning the operation of cellular networks without an FCC license.**

In order to gain access to the defendant's encrypted and encoded aircard signals, the FBI had to operate its own cellular network through use of its own cell site emulators. The defendant neither authorized nor expected to have his aircard access cell sites that were not

\footnote{1241. See General Facts, Section IV(B)(9)(a), \textit{supra}.} \footnote{1242. See \textit{id.}, Section IV(B)(e), (f) and (g), \textit{supra}.} \footnote{1243. In \textit{Nerber}, the Ninth Circuit considered "the totality of the circumstances... including but not limited to the nature of the government intrusion," \textit{Nerber}, 222 F.3d at 600, when determining whether an individual had a reasonable expectation of privacy.} \footnote{1244. See \textit{id.}, Section IV(B)(9)(g), \textit{supra}.}
part of the Verizon Wireless cellular network. The defendant only expected to have his aircard send and receive radio waves to/from cell sites that were part of the actual Verizon Wireless cellular network. The defendant's subjective expectation of privacy to this effect was objectively reasonable in light of federal statutes banning the operation of cellular networks that transmit on reserved frequency bands (i.e., spectrum assignments) without a license from the Federal Communications Commission (FCC). Federal law states that “[n]o person shall use or operate any apparatus for the transmission of energy or communications or signals by radio... upon any other mobile station within the jurisdiction of the United States, except under and in accordance with this Act and with a license in that behalf granted under the provisions of this Act.” 47 U.S.C. § 301 et seq. (License for radio communication or transmission of energy). The noted “Act” is in reference to Act June 19, 1934, ch 656, granting the FCC the authority to, inter alia, regulate licensed radio frequency bands. See 47 U.S.C. § 151 et seq. Federal law also states that “[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this Act...” 47 U.S.C. § 333 (Willful or malicious interference).

1245. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 15, p. 6.

1246. See id.

1247. “Spectrum Assignment: Federal government authorization for the use of specific frequencies within a given spectrum allocation, usually in a specific geographic location. Mobile communications assignments are granted to both private users such as businesses, and commercial providers such as wireless and paging operators. Spectrum auctions and/or frequency coordination processes, which consider potential interference to existing users, may apply.” CTIA [website], Wireless Glossary of Terms Q-S, http://www.ctia.org/media/industry_info/index.cfm/AID/10406 (last accessed: Aug., 30, 2011).

1248. The frequency bands relevant to 1xEV-DO Rel. 0 are listed in TIA/EIA/IS-856-1, cdma2000 High Rate Packet Data Air Interface Specification, § 9.2.1.1.1.1, p. 9.6-9.22.

interference). These statutes banning radio transmissions without a license are sources outside the Fourth Amendment\textsuperscript{1250} that provide support for the defendant's reasonable expectation of privacy in his aircard signals that were only revealed after FBI technical agents transmitted radio waves to the aircard via an unauthorized cellular network.

d. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in his "sealed" aircard signals seized by the FBI.

General background information on the third-party disclosure rule is provided in Section V(C)(4)(b) et seq.,\textit{supra}.\textsuperscript{1251} The third-party disclosure rule does not apply to the FBI seizing the defendant's encrypted and encoded aircard signals considering the FBI collected the signals directly from the aircard over the air interface and not from Verizon Wireless, \textit{i.e.}, the so-called "third party." \textit{See In Re Application Of The United States Of America For An Order For Disclosure Of Telecommunications Records And Authorizing The Use Of A Pen Register And Trap And Trace}, 405 F.Supp.2d 435, 438 (S.D.N.Y. 2005) (In the context of cell site location information, signaling data may not be “obtained by the Government directly” and must instead be “transmitted from the provider digitally to a computer maintained by the Government.”). Such a practice would not provide the government protection under the third-party disclosure rule articulated in \textit{Miller} and \textit{Smith}.

"Drawing an analogy to \textit{Miller}, police are not acquiring financial information from a third party bank, but are searching the target directly and seizing the bank statement held with a reasonable expectation of privacy. There is simply no third party involved."\textsuperscript{1252} Additionally, the FBI was using radar interrogation techniques to force the aircard to send out signals while portraying its surveillance equipment as Verizon Wireless cell sites. \textit{See}
also Section V(C)(5)(c)(ii), supra (the third-party disclosure rule of Miller and Smith does not apply because the FBI forced the defendant's aircard to send out signals).

7. The defendant had a reasonable expectation of privacy in the data contained on the storage device within his aircard.

The defendant had a subjective expectation of privacy in the data stored on the aircard's internal storage device because (1) he did not allow anyone physical access to the aircard, and (2) any stored data sent to Verizon Wireless from the aircard was encrypted/encoded and inaccessible to anyone eavesdropping on transmitted signals.

The defendant's subjective expectation of privacy was objectively reasonable because courts have recognized that “an individual has the same expectation of privacy in a pager, computer or other electronic data storage and retrieval device as in a closed container...” United States v. Blas, No. 90-CR-162, 1990 U.S. Dist. LEXIS 19961, p. 56 (E.D.Wis., Dec. 4, 1990). This reasonable expectation of privacy is also “analogous to that in a personal address book or other repository for such information.” United States v. Chan, 830 F.Supp. 531, 534 (N.D.Cal. 1993); see also United States v. James, No. 1:06 CR 134 CDP DDN, 2008 U.S. Dist. LEXIS 29840, p. 25-26 (E.D.Mo., Mar. 4, 2008) (“Many courts have found that people have a reasonable expectation of privacy in the somewhat unsophisticated information stored in mere pages.” (listing cases)). The authorities cited above provide sufficient support for the defendant's reasonable expectation of privacy in all data stored on his aircard.

Later in this memorandum, the defendant challenges the FBI's remote surreptitious search of the aircard in order to seize the Electronic Serial Number (ESN) contained on the aircard's internal storage device. A search and seizure of this nature should not be confused with obtaining the ESN of a wireless device via subpoena served on a wireless carrier. In order to further differentiate the two issues, the proceeding subsections explain why an ESN stored on an individual's wireless device is considered highly private and why an ESN seized

1253. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection, ¶ 2, p. 1-2.

1254. See Technical Explanations, Section II(B)(3)(c)(iv), supra (explaining the 1xEV-DO Rel. 0 encryption process at the security layer).
directly from a wireless device is not Pen/Trap data obtained from a third-party.

a. The ESN data stored on a wireless device is considered to be highly private.

The ESN data stored on a wireless device is highly private considering it links what would otherwise be an unknown device to the owner of the device through the associated wireless account. For example, in order to identify the defendant's aircard prior to collecting signals for triangulation purposes, the FBI sent a HardwareIDRequest message from its emulated cell site to the receive antenna of what was then an unknown device.\[1255\] The aircard, being the unknown device, responded by transmitting back its stored ESN to the FBI's emulated cell site.\[1256\] The FBI logged the ESN it received directly from the aircard and then compared it to the ESN it previously received from Verizon Wireless via subpoena.\[1257\] By matching the two separately obtained ESNs, the FBI determined that its surveillance equipment was accessing the defendant's aircard. If it was not for obtaining the aircard's ESN directly from its internal storage, the FBI would have never been able to locate the aircard and the defendant within his home.

An additional reason as to why stored ESN data is highly private is that it acts to protect the integrity of cellular service. Prior to modern day cellular systems, an ESN captured off the air interface could be used by a criminal to clone the respective wireless device for the purpose of receiving unauthorized cellular service. “Every cell phone is designed to have a unique factory-set electronic serial number (ESN) and mobile identification number (MIN). 'Cloned' cell phones are those reprogrammed to transmit the ESN and MIN of another (legitimate) telephone when calls are made. Swindlers obtain those numbers by monitoring radio wave transmissions and intercepting calls in progress.” Newton, Michael, *The Encyclopedia of High-Tech Crime and Crime-Fighting*, Checkmark Books, New York, NY (2004), p. 52. See also *United States v. Bailey*, 41 F.3d 413, 418 (9th

\[1255\] See General Facts, Section IV(B)(9)(d), supra.

\[1256\] See id.

\[1257\] See id.; see also Procedural History, Section III(A), supra (discussing D.Ariz. subpoenas used to obtain the aircard's ESN from Verizon Wireless).
(Cir. 1994) (“[T]he ESN and MIN are not just part of an after-the-fact billing device; they are part of a system designed to permit access only by those so entitled because of an account.”).

For the 1xEV-DO Rel. 0 cellular system relevant to the aircard, more is needed to clone a wireless device but an eavesdropped ESN alone may still be used to conduct various denial-of-service attacks on 1xEV-DO Rel. 0 service. For example, an attacker in possession of the defendant's ESN could launch de-registration spoofing\footnote{See Hanser, Christopher, et al., Security in Mobile Telephony: The Security Levels in the Different Handy Generations, “Possible 3G attacks and security architecture responses,” Seminar Paper, University of Uppsala, Sweeden, \url{available at http://www.it.uu.se/edu/course/homepage/sakdat/ht05/assignments/pm/programme/mobile_telephony.pdf} (last accessed: Dec. 20, 2011), p. 7.} and location update spoofing\footnote{See id.} attacks on aircard service.

**b. The FBI obtaining the aircard's stored ESN using cell site emulators does not amount to using a pen register or trap and trace device.**

As previously explained, the FBI pretended to be as Verizon Wireless while using an FBI controlled cell site emulator to transmit a HardwareIDRequest message to the aircard's receive antenna.\footnote{See General Facts, Section IV(B)(9)(d), supra.} In response to the HardwareIDRequest message, the aircard transmitted its stored ESN directly back to the FBI's cell site emulator.\footnote{See id.} The FBI seizing the aircard's stored ESN in this manner does not amount to using a pen register or trap and trace device because it simply does not resemble use of such devices. In a Central District of California case,\footnote{See In The Matter Of The Application Of The United States Of America For An Order Authorizing The Use Of A Cellular Telephone Digital Analyzer, 885 F.Supp. 197 (C.D.Cal. 1995).} the court reasoned that use of a digital analyzer\footnote{Unlike cell site emulators that actively communicate with target wireless devices, digital analyzers are passive radio wave receivers that only receive signals that are already being transmitted. These passive receivers do not transmit signals or otherwise communicate with cell phones or other wireless devices.} to obtain an ESN off the air interface could be considered a Pen/Trap device\footnote{See id. at 201 (“As contemplated for use by applicant, the digital analyzer takes on some of the characteristics of a pen register and some of the characteristics of a trap and trace device.”)} because (1) the ESNs would...
be in plain view and passively collected via use of a radio receiver,\footnote{See id. at 198-99 (Noting that the government intended to use “a portable device that can detect signals emitted by a cellular telephone.”).} (2) the ESN collection would be incidental to legitimate incoming and outgoing calls,\footnote{See id. at 200 (Noting that agents would “conduct surveillance of the subjects of the investigation, and when they observe a subject using a cellular telephone, they will turn on the digital analyzer. The analyzer will then display the ESN, the telephone number of the cellular telephone being used, and the telephone number of the party being called on the cellular telephone.”).} and (3) all ESNs would otherwise be voluntarily transmitted through the air by the cell phone users.\footnote{See id. at 199 (Noting that the ESNs would be “voluntarily exposed and known to others.”).}

\footnote{1265. See id. at 198-99 (Noting that the government intended to use “a portable device that can detect signals emitted by a cellular telephone.”).}

\footnote{1266. See id. at 200 (Noting that agents would “conduct surveillance of the subjects of the investigation, and when they observe a subject using a cellular telephone, they will turn on the digital analyzer. The analyzer will then display the ESN, the telephone number of the cellular telephone being used, and the telephone number of the party being called on the cellular telephone.”).}

\footnote{1267. See id. at 199 (Noting that the ESNs would be “voluntarily exposed and known to others.”).}

As explained below, the digital analyzer applicable to the C.D.Cal. case is distinguishable from the cell site emulators applicable to the present case for numerous reasons.

First, the aircard’s ESN was not in plain view considering it would have ordinarily been encrypted, encoded, and inaccessible to digital analyzers.\footnote{1268. Unlike the 1995 technology addressed in the C.D.Cal. digital analyzer case, ESNs belonging to 1xEV-DO Rel. 0 wireless device are not voluntarily exposed and known to others.}

The FBI technical agents circumvented these security measures by forcing a connection with the aircard over the air interface while pretending to be Verizon Wireless. Once connected, the FBI technical agents used active radio wave transmissions to send specially crafted messages to the aircard which forced it to reveal its ESN. Second, the aircard was not communicating with Verizon Wireless and no call or data connection was in progress when the FBI completed steps to seize the aircard’s ESN directly from its internal storage.\footnote{1269. Prior to seizing the ESN, the FBI forced the aircard to disconnect from Verizon Wireless causing the aircard to be denied Internet access service. Additionally, the ESN was seized by the FBI while the aircard was in the session establishment phase which occurs prior to establishing a data connection. See Technical Explanations, Section II(B)(3)(c)(iii), supra (explaining 1xEV-DO Rel. 0 sessions).}

\footnote{1268. Unlike the 1995 technology addressed in the C.D.Cal. digital analyzer case, ESNs belonging to 1xEV-DO Rel. 0 wireless device are not voluntarily exposed and known to others.}

\footnote{1269. Prior to seizing the ESN, the FBI forced the aircard to disconnect from Verizon Wireless causing the aircard to be denied Internet access service. Additionally, the ESN was seized by the FBI while the aircard was in the session establishment phase which occurs prior to establishing a data connection. See Technical Explanations, Section II(B)(3)(c)(iii), supra (explaining 1xEV-DO Rel. 0 sessions).}

c. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in the ESN stored on his aircard

General background information on the third-party disclosure rule is provided in Section V(C)(4)(b) et seq., supra.\[1270\] The third-party disclosure rule does not apply to the FBI seizing the ESN stored on the defendant's aircard considering the FBI obtained it directly from the aircard itself and not from Verizon Wireless—the so-called “third party.” See also Section V(C)(6)(d), supra (supporting legal argument). The defendant in no way “voluntarily conveyed” the aircard's ESN to anyone considering (1) the FBI forced the aircard to reveal its ESN by pretending to be Verizon Wireless, (2) the aircard was not engaged in a data connection or “call,” (3) the FBI sent the aircard specially crafted radio waves instructing it to transmit its ESN, and (4) the ESN that was transmitted through the air via radio waves would have ordinarily been encrypted/encoded and inaccessible to anyone using a passive eavesdropping device. Additionally, just like in Hicks, the fact that the government already obtained the aircard's electronic serial number through a previous investigation involving subpoenas\[1271\] does not affect the subsequent Fourth Amendment search to record the serial number directly from the device bearing it. See Arizona v. Hicks, 480 U.S. 321, 324-25 (1987) (causing stereo equipment serial numbers to become visible was a Fourth Amendment search even while officer's headquarters had the serial numbers on record from a previous investigation).

---

1270. Argument, Section V(C)(4)(b) et seq., supra, is hereby incorporated into this section by reference.
1271. See Procedural History, Section III(A), supra, (discussing procedural aspects of D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615 used to obtain the aircard's ESN from Verizon Wireless).
8. The defendant had a reasonable expectation of privacy in his historical electronic gate location information seized from Quality Alarm Service.

a. The defendant's reasonable expectation of privacy is grounded by the government's search by inference.

The Domicilio apartment complex is a gated community protected by Quality Alarm Service's private access electronic gates at all entrances.[1272] When the defendant rented apartment No. 1122, he was assigned and given an electronic gate access key (referred to by Domicilio as "fobs") so that he could unlock and enter through the exterior gates at the Domicilio apartment complex.[1273] Whenever the defendant entered the Domicilio property to return to his home, he used his electronic gate key resulting in a record being created within the accessed fob reader corresponding to the gate accessed.[1274] On July 24, 2008, the defendant's historical electronic gate key access location information was seized from Quality Alarm Service by the government.[1275] Using the seized geolocation information, the government was able make various documented inferences including: (1) the defendant entered his home once every 3.6 days, (2) the defendant's estimated next entry to his home will be Saturday, July 26, 2008 or Sunday, July 27, 2008, between the hours of 12:01am and 7:00am, and (3) the defendant last entered his home on July 23, 2008.[1276][1277] The same arguments contained in Section V(C)(4)(a), supra,[1278] relating to the government intrusions

[1272] See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 7, p. 2-3.

[1273] See id., ¶ 8-9, p. 3; EXHIBIT 093 of 2nd Consolidated Exhibits (Dkt. #821-5) (Domicilio apartment complex, apartment No. 1122, electronic gate access key fob receipt (fob No. 58261)).

[1274] See Procedural History, Section III(G), supra (discussing procedural aspect of D.Ariz. Grand Jury Subpoena No. 07-03-709); General Facts, Section IV(B)(12), supra (discussing the government obtaining and using the defendant's historical electronic gate key access location information).

[1275] See id.

[1276] See id.

[1277] Because the electronic gates at the Domicilio apartment complex can be pushed open from the inside without using an electronic gate access key, the geolocation records at issue do not contain information on when the defendant exited his home. Therefore, no inferences can be made about the length of time spent by the defendant within his home during the times between the logged entry dates.

[1278] Argument, Section V(C)(4)(a), supra, is hereby incorporated into this section by
with respect to historical cell site location information, similarly apply here as well. See, e.g., *Kyllo*, 533 U.S. at 33-34 (Rejecting the “dissent's extraordinary assertion that anything learned through 'an inference' cannot be a search[.]”). Although the two types of geolocation data are different, the government used both sets of data in the same manner when analyzed from a legal perspective. The government using historical electronic gate location information to infer the defendant's past and future locations within his home implicates the defendant's reasonable expectation of privacy in that information.[1279]

b. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in his historical electronic gate location information seized from Quality Alarm Service.

In Section V(C)(4)(b) *et seq.*, *supra*, the defendant explained three primary reasons as to why the third-party disclosure rule does not apply to his historical cell site location information seized from Verizon Wireless: (1) *Miller* does not apply because Verizon Wireless was not party to the defendant's communications and his cell site location information does not constitute routine business records; (2) *Smith* does not apply because the defendant did not knowingly or voluntarily convey his location information to Verizon Wireless; and (3) in any event, the Court should find an exception to the third-party disclosure rule considering Verizon Wireless is a service provider intermediary and location information is objectively recognized as highly private. The same general reasoning explained in Section V(C)(4)(b) *et seq.*, *supra*,[1280] regarding why the third-party disclosure rule is inapplicable to the defendant's historical cell site location information, applies equally well to the defendant's historical electronic gate location information seized from Quality Alarm Service. The third reason noted above (i.e., third-party rule exception), explained in reference.

[1279] In *Nerber*, the Ninth Circuit considered “the totality of the circumstances... including but not limited to the nature of the government intrusion,” *Nerber*, 222 F.3d at 600, when determining whether an individual had a reasonable expectation of privacy.

[1280] *Argument*, Section V(C)(4)(b) *et seq.*, *supra*, is hereby incorporated into this subsection by reference.
Section V(C)(4)(b)(iii), supra,[1281] is generic enough to incorporate into this subsection without additional analysis. However, the first two reasons noted above are more fact dependent and therefore require additional analysis in order to apply to the defendant's historical electronic gate location information. The required additional analysis in support of applying arguments in Section V(C)(4)(b)(i) and (ii), supra, to the defendant's historical electronic gate location information are explained in the proceeding subsections.

i. *Miller* does not apply because Quality Alarm Service was not party to the defendant's transactions and his electronic gate location information does not constitute routine business records.

First, the reasoning in *Miller* does not apply because Quality Alarm Service was not acting as a party to any gate access transaction between the defendant and Domicilio but was instead acting as a government agent. The Supreme Court's basis for its holding in *Miller* was that “banks are not neutrals in transactions involving negotiable instruments, but parties to the instruments,” and the records “pertain to transactions to which the bank was itself a party.” *Miller*, 425 U.S. at 440, 441 (brackets, ellipsis, and citation omitted). In contrast, Quality Alarm Service was simply the company that installed the electronic gates at the Domicilio apartment complex and it had no direct access to the historical electronic gate location information generated by each fob reader. The only way Quality Alarm Service was able to comply with the government's subpoena was to enter the Domicilio property with FBI Agent Murray and then physically access each fob reader in order to obtain the sought after geolocation records.[1282] The reasoning in *Miller* that banking activities are analogous to confiding in one's friend[1283] carries over poorly to the defendant's geolocation information retrieved by FBI Agent Murray and Quality Alarm Service from the Domicilio property.

1281. *Argument*, Section V(C)(4)(b)(iii), supra, is hereby incorporated into this subsection by reference in support of applying reason No. 3 to the defendant's historical electronic gate location information seized from Quality Alarm Service.

1282. See *General Facts*, Section IV(B)(12), supra.

1283. See *Miller*, 425 U.S. at 443.
The second reason *Miller* is inapplicable is because the historical electronic gate location information seized by the government does not constitute Quality Alarm Service's routine business records. The *Miller* court indicated that there is no reasonable expectation of privacy in bank checks and deposit slips considering they are “exposed to their employees in the ordinary course of business” and are “business records of the banks.” *Miller*, 425 U.S. at 442, 440. In contrast, the historical electronic gate location information at issue in the present case was not a routine business record of even Domicilio—let alone Quality Alarm Service. Domicilio had no need for the seized geolocation data and even previously crashed its database containing the records.[1284] The operations of Quality Alarm Service also had no need for the defendant's geolocation data and retrieving the records was such a foreign concept to its business model that an employee canceled his day off and plans with his family to spend all day retrieving the records with FBI Agent Murray.[1285] In fact, the retrieval of the geolocation data was more like a government executed search warrant than compliance with a subpoena requesting routine business records.

**ii. *Miller* does not apply because the defendant did not knowingly or voluntarily convey his location information to anyone.**

The reasoning in *Smith* does not apply because the defendant did not knowingly or voluntarily convey his location information to Domicilio or to Quality Alarm Service. The Supreme Court's basis for its holding in *Smith* was that “[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company... [and] that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.” *Smith*, 442 U.S. at 742. Contrary to the dialed numbers in *Smith*, the defendant had no idea that the fob readers at the Domicilio apartment complex were recording his electronic gate access activity.[1286] Considering the

---

1284. See General Facts, Section IV(B)(12), supra.
1285. See id.
1286. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 10, p. 3.
defendant lacked the requisite knowledge and intent, the third-party disclosure rule should not act to vitiate his reasonable expectation of privacy in his historical electronic gate access records. However, even if it can be said that the defendant voluntarily conveyed geolocation data to Domicilio, the government obtained that data from Quality Alarm Service, which is an entity entirely separate from Domicilio—the true so-called third-party.

9. **The defendant had a reasonable expectation of privacy in his aircard destination IP addresses seized from Verizon Wireless.**

   a. **The 1.8 million destination IP addresses reveal communications content and other Fourth Amendment protected information.**

   The defendant had a reasonable expectation of privacy in his 1.8 million destination IP addresses seized from Verizon Wireless by the government. The defendant's subjective expectation of privacy is supported by his efforts to anonymize and untie himself from the IP address records by signing up for his aircard account under an alias. The defendant's subjective expectation of privacy is objectively reasonable because the 1.8 million destination IP addresses correspond to websites the defendant visited[^1287] and the massive amount of data contained on those websites allows for the government to create an accurate map of the defendant's interests, associations, and habits. In *Forrester*, the Ninth Circuit held that there is no reasonable expectation of privacy in destination IP addresses because “[a]t best, the government may make educated guesses about what was... viewed on the websites based on its knowledge of the... IP addresses—but this is no different from [use of a pen register resulting in] speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed.” *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). However, the Ninth Circuit conditioned its ruling by stating that it “does not imply that more intrusive techniques or techniques that reveal more content information are also constitutionally identical to the use of a pen register;” *Id.* at 511.[^1288]

[^1287]: See defendant's declaration accompanying this memorandum RE: Internet activity reflected by the 1,836,140 aircard destination IP addresses seized by the government.

[^1288]: Additionally, society's expectations of privacy regarding web browsing habits have been solidified since *Forrester*. In a recent front page article, *The Wall Street Journal* reported on how “Google Inc. and other advertising companies have been bypassing the...
In the present case, the government obtaining 1.8 million of the defendant's destination IP addresses and associated data[^1289] is not constitutionally identical to use of a pen register and is more resemblant of a wiretap used to obtain communications content.

First, by using the total amount of data downloaded during a given IP connection, the government can pair that connection to a specific image or other file downloaded by the defendant from the website associated with the relevant IP address[^1290]. Such an analysis provides precise content information and goes beyond what was discussed in *Forrester*.

Second, the pen register analogy in *Forrester* does not apply because it is impossible for an individual to place or receive 1.8 million phone calls during the 60 day period the defendant accessed the 1.8 million Internet resources[^1291]. The defendant would need to complete a privacy settings of millions of people using Apple Inc.'s Web browser on their iPhones and computers—tracking the Web-browsing habits of people who intended for that kind of monitoring to be blocked.” Angwin, Julia and Valentino-DeVries, Jennifer, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, The Wall Street Journal, p. A1 (Feb. 17, 2012) available at http://online.wsj.com/article/SB1000142405297020488040457722538045659176.html (last accessed: Apr. 12, 2012). Prior to the article going public, “Google disabled its code after being contacted by The Wall Street Journal.” *Id*. The front page placement of the article and Google's “damage control” reaction shows that an individual's subjective expectation of privacy in his/her web browsing habits is one that society is presently prepared to accept as objectively reasonable.

[^1289]: Among other information, the Grand Jury subpoenas requested that Verizon Wireless provide connection time, date, source IP address, source port and destination port, data transfer volume, and method of connection to system (telnet, ftp, http) for all IP addresses accessed by the defendant. See *Procedural History*, Section III(A), supra (discussing procedural aspects of D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615).

[^1290]: Similarly, the D.Ariz. 08-3286MB-LOA court order requested that Verizon Wireless provide connection source IP address, connection time and date, disconnect time and date, data transfer volume, connection IP destination, and method of connection to system (telnet, ftp, http). See *id.*, Section III(B), supra (discussing procedural aspects of D.Ariz. 08-3286MB-LOA court order).

[^1291]: The defendant's destination IP addresses covered his aircard use from May 11, 2008 through July 9, 2008. See *Procedural History*, Section III(A), supra (discussing procedural aspects of D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615); *id.*, Section III(B), supra (discussing procedural aspects of D.Ariz. 08-3286MB-LOA court order).
new phone call approximately once every 2.82 seconds—for 60 days straight without
stopping—in order to match the 1,836,140 destination IP addresses accessed via the aircard
during the relevant time frame. Such a vast amount of destination IP addresses allows for
detailed profiling of the defendant's interests, associations, and habits that could never be
obtained from 60 days worth of dialed phone numbers. The remainder of this subsection
provides precise examples of the type of private communications content that can be gleaned
from the 1.8 million seized destination IP addresses.[1292]

The 1.8 million seized destination IP addresses show that the defendant visited
truthalliance.net (2 hits), prisonplanet.tv (24 hits), antiwar.com (8 hits), epic.org (13 hits),
eff.org (8 hits), and lewrockwell.com (57 hits).[1293] The contents of those websites indicate
that the defendant's political associations are in the pro-civil-liberties, antiwar, and limited
government realm. The government obtaining records showing that the defendant visited the
above websites acts to curtail his First Amendment right to freedom of association. See
NAACP v. Alabama, 357 U.S. 449, 462 (1958) (Recognizing “the vital relationship between
freedom to associate and privacy in one’s associations.”);[1294] see also Zurcher v. Stanford,
Daily, 436 U.S. 547, 564 (1978) (“[T]he requirements of the Fourth Amendment must be
applied with 'scrupulous exactitude’” when First Amendment protected materials are seized.
(citation omitted)). The 1.8 million seized destination IP addresses also show that the
defendant visited builditsolar.com (10 hits), theelectricbicyclestore.com (5 hits),
safesolutionsinc.com (3 hits), healthfreedomusa.org (20 hits), and herbs.org (5 hits).[1295]

1292. The examples provided in this section are only the tip of the iceberg. Through further
analyses, the 1,836,140 seized destination IP addresses could yield hundreds of similar
inferences telling of the defendant's interests, associations, and habits.

1293. See defendant's declaration accompanying this memorandum RE: Internet activity
reflected by the 1,836,140 aircard destination IP addresses seized by the government,
Attachment No. 01 (Chart Of Excerpt Of Websites Accessed By Aircard From May 11, 2008
Through July 9, 2008).

1294. The Supreme Court held that the state compelling the NAACP to disclose the names
and addresses of its members was a “substantial restraint upon the... right to freedom of
association,” because “it may induce members to withdraw from the Association and
dissuade others from joining it because of fear of exposure...” Id. at 462–63.

1295. See defendant's declaration accompanying this memorandum RE: Internet activity
reflected by the 1,836,140 aircard destination IP addresses seized by the government,
Attachment No. 01 (Chart Of Excerpt Of Websites Accessed By Aircard From May 11, 2008

- 245 -
The contents of those websites indicate that the defendant had an interest in energy conservation, the environment, and products that do not contain genetically modified organisms (e.g., non GMO foods). The 1.8 million seized destination IP addresses also show that the defendant visited frugalsquirrels.com (30 hits), edenfoods.com (159 hits), and doughboyssurplus.com (147 hits).[1296] The contents of those websites indicate that the defendant had an interest in long term food storage—an activity that the Department of Homeland Security (DHS) now scrutinizes with an evil eye.[1297] The probability of the government gleaning all of the above inferences from mere phone records is extremely low.

Additional inferences act to distinguish the 1.8 million seized destination IP addresses from dialed phone numbers. While using his aircard, the defendant visited pccables.com (5 hits)[1298]—a website specializing in selling cables and cable related accessories for computers. It is an obvious inference that the defendant was shopping for computer cables when he visited pccables.com. Information of this type cannot be gleaned from a list of dialed phone numbers gathered via a pen register. For example, if the defendant called a

Through July 9, 2008).

1296. See id.

1297. In one of many “Communities Against Terrorism” flyers handed out by the Bureau of Justice Assistance (BJA) and the FBI, the government warned military surplus stores that people who “[m]ake bulk purchases of items to include: [] Meals Ready to Eat” is a suspicious activity indicative of possible “terrorism.” BJA/FBI/JRIC, Tripwire, Communities Against Terrorism: Potential Indicators of Terrorist Activities Related to Military Surplus Stores, download from http://www.publicintelligence.net/fbi-suspicious-activity-reporting-flyers (last access: Mar. 18, 2012); EXHIBIT 082 of 2nd Consolidated Exhibits (Dkt. #821-4) (flyer attached). See also An Insider, Beware of Homeland Security Training for Local Law Enforcement, Mar. 30, 2011, http://www.survivalblog.com/2011/03/beware_of_homeland_security_tr.html (last accessed: Mar. 18, 2012) (DHS says stockpiling food is characteristic of domestic terrorism). The innocent practice of long term food storage, often engaged in by religious groups and those interested in feeding their families during a crisis, is now a government persecuted activity. Due to overbearing DHS policy on the issue, it is objectively reasonable for an individual to conceal his/her interest in long term food storage from the government.

1298. See defendant's declaration accompanying this memorandum RE: Internet activity reflected by the 1,836,140 aircard destination IP addresses seized by the government, Attachment No. 01 (Chart Of Excerpt Of Websites Accessed By Aircard From May 11, 2008 Through July 9, 2008).
local Best Buy[1299] or Fry's Electronics[1300] to shop for computer cables, the government would need to listen in on the defendant's phone conversation in order to learn what he sought to purchase. The government logging the defendant's access to pccables.com accomplished what would have required a Title III wiretap authorization had the defendant been using a phone to do his shopping. The defendant also visited waynewichernmillinery.com (44 hits)[1301]—website of world renowned hat designer, Wayne Wichern. It is an obvious inference that the defendant was not shopping for just any old hat, but a finely crafted Wayne Wichern. Just like the computer cables, information of this type cannot be gleaned from pen register data. Even if the defendant called a local hat store that sells only hats, such as the JORCAL Hat Co. retail outlet in San Jose, CA.[1302] or Hats Of The Fillmore in San Francisco, CA.,[1303] it would be impossible for the government to know what brand of hat the defendant was looking for without listening in on the phone conversation.

As a final example of intrusiveness, the seized destination IP addresses show 1,187 hits to youtube.com with precise access dates and times.[1304] An analysis of the YouTube


1301. See defendant's declaration accompanying this memorandum RE: Internet activity reflected by the 1,836,140 aircard destination IP addresses seized by the government, Attachment No. 01 (Chart Of Excerpt Of Websites Accessed By Aircard From May 11, 2008 Through July 9, 2008).

1302. See Jorcal, Inc. [website], JORCAL Hat Co.- San Jose, http://www.jorcalinc.com (last accessed: Mar. 18, 2012) (“We are your premier source for today's hottest hats in the San Francisco Bay Area, Northern California and San Jose. We are just minutes outside of downtown San Jose.”); EXHIBIT 080 of 2nd Consolidated Exhibits (Dkt. #821-4) (website home page attached).


1304. See defendant's declaration accompanying this memorandum RE: Internet activity
logs allows for the government to map out the times of day and to what extent the defendant watched YouTube videos, which is the modern day equivalent of his cable TV watching habits.[1305] Additionally, taking into account “more sophisticated systems that are already in use or in development[,]” Kyllo, 533 U.S. at 36, the phasing out of IPv4 and the phasing in of IPv6 will allow for the government to use a 2703(d) order to obtain not only access times, but an exact list of the Web TV programs watched by any individual. Because IPv6 will “comfortably allow a billion unique IP addresses for every person on earth[,]”[1306] it logically follows that IPv6 will result in a unique destination IP address identifying each individual Web TV show being aired on the Internet. The outcome of IPv6 will allow for the government to obtain precise Web TV watching habits using less-than-probable-cause orders similar to the “retroactive” D.Ariz. 08-3286MB-LOA order used in the present case. At least in the context of cable TV in the USA, government tracking of this nature—without a finding of clear and convincing evidence—is prohibited by the Cable Communications Policy Act of 1984, 47 U.S.C. § 521 et seq.[1307] Aside from the future implications of IPv6, reflected by the 1,836,140 aircard destination IP addresses seized by the government, Attachment No. 01 (Chart Of Excerpt Of Websites Accessed By Aircard From May 11, 2008 Through July 9, 2008).

1305. “A former NBC programming chief is launching three YouTube channels in the coming months. The creator of the CBS juggernaut 'CSI' is filming a series of YouTube thrillers. Stars like Tom Hanks and Kevin Spacey are at work on new shows for Yahoo and Netflix.... Google, which owns YouTube, is paying an array of producers, from seasoned pros like Mr. Robbins to self-made Web stars, to create 100 new video 'channels.' Google is giving each channel up to $5 million in funding, according to people familiar with the deals.” Jurgensen, John, Web TV’s New Lineup, The Wall Street Journal, p. D1 (Feb. 17, 2012), available at http://online.wsj.com/article/SB10001424052970204883304577223630028525366.html (last accessed: Apr. 12, 2012).


1307. “A cable operator may disclose [][personally identifiable information concerning a subscriber] if the disclosure is—[] to a government entity as authorized under... [18 U.S.C §§ 2510 et seq., 2701 et seq., or 3121 et seq.], except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator.” 18 U.S.C. § 551(c)(2) and (D) (emphasis added). If the governmental entity wants to obtain video programming records, it must engage in a court proceeding and provide “clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case;” additionally, the subject of the information must be “afforded the opportunity to appear and contest such entities claim.” 18 U.S.C. § 551(h) et seq.
spy companies are already offering IPv4 Deep Packet Inspection and Processing (DPP/DPI) surveillance products that are capable of tracking YouTube watching habits using “signaling” information currently obtainable through less-than-probable-cause orders.

b. The third-party disclosure rule does not vitiate the defendant's reasonable expectation of privacy in his 1.8 million destination IP addresses.

General background information on the third-party disclosure rule is provided in Section V(C)(4)(b) et seq., supra. The third-party disclosure rule does not apply to the government's seizure of the defendant's 1.8 million destination IP addresses because the data seized is highly private. Similar to historical cell site location information, Verizon Wireless' mere ability to access the defendant's destination IP addresses does not mean that he loses his reasonable expectation of privacy in that data. See Argument, Section V(C)(4)(b)(iii), supra (discussing recognized exceptions to the third-party disclosure rule). Due to the private nature of the defendant's 1.8 million destination IP addresses, the “content exception” to the third-party disclosure rule should apply. See id. (discussing “content exception”). In a concurring opinion, Supreme Court Justice Sotomayor recently noted her “doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.” Jones, 181 L. Ed. 2d at 926 (Sotomayor, J. concurring). Therefore, “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” Id.


1309. Argument, Section V(C)(4)(b) et seq., supra, is hereby incorporated into this section by reference.
10. The defendant had/has a reasonable expectation of privacy in his data contained on his hard drives, encrypted virtual drives, and the forensic images created therefrom—as they are in the possession of the government.

The defendant had and continues to have a reasonable expectation of privacy in the non-seized data contained on his hard drives, encrypted virtual drives, and the forensic images created therefrom. The noted data containers are all currently in the possession of the government and have been since before September 2, 2008—the date the 30 day window ended for searching the defendant’s data for evidence. The defendant’s reasonable expectation of privacy in the noted data containers is supported by the computer search protocol contained in the N.D.Cal. 08-70460-HRL/PVT warrant: “The 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.”[1310] According to the computer search protocol, the government was authorized to search the noted data containers between August 3, 2008 (initial warrant execution date) and September 2, 2008. However, after that window of time expired, the defendant's reasonable expectation of privacy in the noted data containers was fully restored.

With respect to copies of data (e.g., original copies on physical hard drives, forensic images taken of physical hard drives, and copies of the encrypted virtual drives), “the government may retain the copies (1) to preserve evidence, or (2) because the copies are contraband, a forfeitable instrumentality of a crime, or fruit of a crime.”[1311] Any data that is contraband, forfeitable, or fruit of a crime has already been seized and isolated onto a series of DVDs by IRS-CI Agent Daun.[1312] Additionally, the government's authority to preserve evidence does not permit agents to re-access the forensic images and encrypted virtual drives at their leisure. See Walter v. United States, 447 U.S. 649 (1980) (FBI screening of films was a Fourth Amendment search even while agents gained lawful access to the film reels). While

---

1310. Procedural history, Section III(H), supra (discussing and analyzing both versions of the warrant); Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122, “Computer Search Protocol For The Northern District Of California,” ¶ 5, p. 2 (Dkt. #566-2, p. 16).
1311. Id., ¶ 5, p. 2-3 (Dkt. #566-2, p. 16-17).
1312. See General Facts, Section IV(B)(17), supra.
the physical hard drives, forensic images, and encrypted virtual drives are preserved in
government possession, the defendant maintains a reasonable expectation of privacy in all
data contained therein. Indeed, the government agrees that the data containers “actually
contain many more files than those that fall within the parameters of the Search Warrant and
its attachments.”[1313][1314]

D. Explanation of five different types of searches and/or seizures and
why they are relevant to the defendant's arguments.

The actions conducted by the government to locate the aircard and the defendant can
be classified into five different categories of search and/or seizure:

<table>
<thead>
<tr>
<th>#</th>
<th>Category Of Search And/Or Seizure</th>
<th>Requires reasonable expectation of privacy analysis?</th>
<th>Requires property/possessory interest analysis?</th>
<th>Requires liberty interest analysis?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Non-trespassory search that violates privacy resulting in the obtaining of information.</td>
<td>YES</td>
<td>VARIES*</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Trespassory search resulting in the obtaining of information.</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>3</td>
<td>Search that violates privacy by way of seizure of records containing private information.</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>4</td>
<td>Seizure that interferes with property/possessory interest in an “effect.”</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>5</td>
<td>Seizure that interferes with an individual's liberty interest in a protected activity.</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>

The precise category applicable to each of the government's independent searches
and/or seizures is relevant to the defendant's arguments largely because some require the

1313. See EXHIBIT 087 of 2nd Consolidated Exhibits (Dkt. #821-5) (Computer Forensic
Report by IRS-CI Agent Daun RE: search of physical storage devices and virtual drives
seized from apartment No. 1122).

1314. See also defendant's declaration accompanying this memorandum RE: Data
extracted from hard drive images corresponding to seized hard drives connected to Daniel
Rigmaiden's home computer
defendant to establish only a property or possessory interest while others require him to establish only a reasonable expectation of privacy. For example, for searches and seizures falling into categories No. 1 and 3 in the table above, the defendant need only establish a reasonable expectation of privacy in the place, effect, or record searched and/or seized because having a property/possessory interest is not required. In contrast, for searches and seizures falling into category No. 2 and 4, the defendant need only establish a property or possessory interest because having a reasonable expectation of privacy is not required. The precise category of search and/or seizure is also relevant because some government actions fall into more than one of the five listed categories in a way that the defendant need only establish either a reasonable expectation of privacy or a property/possessory interest (but not both) in order for the relevant government action to be a Fourth Amendment violation. Additionally, many searches and/or seizures act to implicate the defendant's reasonable expectation of privacy or property/possessory interest in more than one applicable place, object, information, record, resource, or combinations thereof. For example, sending radio waves into apartment No. 1122 to search out the aircard (RE: category No. 1 search) violates the defendant's reasonable expectation of privacy in his home and in his aircard. Under this scenario, as long as the defendant is successful in establishing a reasonable expectation of privacy in either his home or his aircard, the government action qualifies as a Fourth Amendment violation. Later in this memorandum (see Argument, Section V(D), infra) the defendant classifies each intrusive government action into one or more of the five categories of search and/or seizure listed in the table above. In support of the defendant's classifications, the proceeding subsections provide a further explanation of the five different categories of searches and/or seizures applicable to the defendant's arguments.

1. Non-trespassory search that violates privacy resulting in the obtaining of information; [Katz reasonable-expectation-of-privacy analysis].

This category of search and seizure (listed as No. 1 in the table above) requires neither a government trespass nor a property/possessory interest and occurs when the government violates an individual's reasonable expectation of privacy in order to obtain information. For
example, the non-trespassory search in *Kyllo* involved agents using a thermal imaging
device, which operates passively “somewhat like a video camera showing heat images[,]” to
scan Kyllo's home from a public street. *Kyllo*, 533 U.S. at 29-30. The Supreme Court held
that the agents' use of the thermal imaging device was a Fourth Amendment search even
while there was no trespass upon Kyllo's real property or chattel. *See Kyllo*, 533 U.S. at 34.
In a different context, the non-trespassory search in *Hicks* involved police officers making an
authorized physical entry into a home but then moving stereo components in order to bring
the components' serial numbers into view. *See Hicks*, 480 U.S. at 324. The Supreme Court
held that the act of an officer moving the stereo equipment in order to learn the serial
numbers was a Fourth Amendment search even while he was lawfully inside the residence
(*i.e.*, no trespass to real property). *See id.* at 325. As a final example, the non-trespassory
search in *Walter* involved FBI agents having lawful possession of an individual's film reels
but then using a projector to view the images stored on the film. *See Walter*, 447 U.S. at 651.
The Supreme Court held that the act of screening the films was a Fourth Amendment search
even while the agents gained lawful access to the films (*i.e.*, no trespass to chattel). The
above cases were decided based on reasonable expectations of privacy belonging to the
individuals who sought to exclude evidence obtained during the relevant searches. *See also
Katz*, 389 U.S. at 361 (Harlan, J., concurring) (The Fourth Amendment applies when an
individual has “exhibited an actual (subjective) expectation of privacy” and the individual's
subjective expectation of privacy is “one that society is prepared to recognize as
reasonable.”).

2. **Trespassory search resulting in the obtaining of information;**

   **[Jones trespass-to-obtain-information analysis]**.

This category of search and seizure (listed as No. 2 in the table above) does not
require an individual to have a reasonable expectation of privacy in the searched place and/or
effect, but does require a property/possessory interest, and occurs when the government
conducts a trespass on real property or chattel for the purpose of obtaining information.
Aside from any reasonable expectation of privacy, it is a Fourth Amendment search when
“the Government obtains information by physically intruding on a constitutionally protected area...” Jones, 181 L. Ed. 2d at 919 fn. 3. In Jones, the Supreme Court noted that the “Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.” Id. at 920-21. Under California common law, “[t]respass to [real] property is the unlawful interference with its possession[,]” Elton v. Anheuser-Busch Beverage Group, Inc., 50 Cal. App. 4th 1301, 1306 (1996) (citation omitted), and trespass to chattel “lies where an intentional interference with the possession of personal property has proximately caused injury.” Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1556 (1996) (citation omitted).[1315] However, if there is no physical entry upon land or deposit of particulate matter, trespass to real property requires injury in the form of physical damage in order to be actionable in California. See San Diego Gas & Electric Co. v. Superior Court, 13 Cal. 4th 893, 936 (1996). In the context of a Jones trespass-to-obtain-information analysis, the “injury” requirement applicable to trespass to real property or chattel is satisfied by the government “obtaining information” while conducting a trespassory search. See Jones, 181 L. Ed. 2d at 927 & fn. 1 (Alito, J. Concurring) (noting how the majority found a trespassory search upon Jone's vehicle (i.e., his chattel or “effect”) even though “there was no actual damage to the vehicle to which the GPS device was attached.”).

Although the Jones Court reiterated the Fourth Amendment's trespassory search, it also noted that “[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis.” Jones, 181 L. Ed. 2d at 922. As imagined by the majority in Jones, some electronic intrusions involve merely the transmission of electronic signals without trespass. For example, the FBI using a DCS-3000 Pen/Trap device to receive real-time cell site location information corresponding to a voluntarily placed phone call would be an electronic intrusion without trespass. There is no trespass because the data generated would be in response to the user's ordinary use of the cellular network and would not require specially crafted signals to be transmitted to the cell phone hardware.[1316]

1315. California trespass law is relevant to the defendant's arguments because the applicable trespass-to-obtain-information searches occurred in California.

1316. This example assumes that the government was not engaging in “pinging” or placing
However, other electronic intrusions involving the transmission of electronic signals amount to trespasses to chattel and/or real property. For example, the FBI using a cell site emulator to force a cell phone to generate and transmit geolocation information would be an electronic intrusion with trespass. A trespass is involved because such an act has nothing to do with the cell phone's ordinary use of the cellular network and requires specially crafted location finding interrogation signals to be transmitted to the cell phone hardware.[1317] Support for the concept of an electronic intrusion with trespass to chattel is found in California case law. See Thrifty-Tel, Inc., 46 Cal. App. 4th 1566 fn. 6 (Finding that “the electronic signals generated by the Bezenek boys' activities were sufficiently tangible to support a trespass cause of action.”); Ebay, Inc. v. Bidder's Edge, 100 F.Supp.2d 1058, 1069 (N.D.Cal. 2000) (Finding that “it appears likely that the electronic signals sent by BE to retrieve information from eBay's computer system are also sufficiently tangible to support a trespass cause of action.”);[1318] see also Baggett v. Hewlett-Packard Co., 582 F.Supp.2d 1261, 1269 (C.D.Cal. 2007) (“[T]respass to chattel claims survive even when the ultimate trespass is not accomplished by a human act.”). In the context of trespass to real property, support for the concept of an electronic intrusion with trespass is also found in California case law. See San Diego Gas & Electric Co., 13 Cal. 4th at 936 (electric and magnetic fields emanating onto real property from power lines may be a trespass if physical damage results).[1319]

surreptitious phone calls to the phone.

1317. See, e.g., General Facts, Section IV(B)(9)(e), supra.

1318. In both Thrifty-Tel, Inc. and Ebay, Inc., the plaintiff suffered injury in the context of a trespass to chattel civil claim. Although not required by Jones, the defendant in the present case also suffered “traditional” injury as a result of the FBI's various trespassory searches. For a period of 16 hours on July 16-17, 2008, the FBI denied the defendant access to the Internet, stole his electricity and computing power, and deactivated signaling encryption thus forcing his aircard to transmit private information in plaintext. In the context of a civil action, the above injuries are measurable losses sufficient to support a trespass to chattel claim. See, e.g., Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1353 (2003) (“[T]he decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers' functioning.”).

1319. Additionally, in the context of radio wave transmissions, relevant science supports the concept of a particulate matter trespass to real property, which requires no physical damage. All electromagnetic radiation, including radio waves, consist of tiny particles called photons. See Technical Explanations, Section II(A). Photons emanating from the sun are capable of physically moving a comet's gaseous tail as the comet flies through space. See id. It logically follows that the photons transmitted by the FBI in the present case were sufficiently
3. Search that violates privacy by way of seizure of records containing private information; [Katz reasonable-expectation-of-privacy analysis].

This category of search and seizure (listed as No. 3 in the table above) occurs when the government obtains an individual's records from a third-party while the individual maintains a reasonable expectation of privacy in the information contained within the records. For example, the Sixth Circuit held in Warshak that “[i]t only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.” Warshak, 631 F.3d at 286. In the context of historical cell site location information, Judge Garaufis applied similar reasoning and found that “cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location records and [] the Government's obtaining these records constitutes a Fourth Amendment search.” Garaufis (dj) 2011 Opinion, 2011 U.S. Dist. LEXIS 93494 at p. 18. The above reasoning can be applied to any type of third-party record as long as the individual alleging the Fourth Amendment violation can establish a reasonable expectation of privacy in the seized record.

4. Seizure that interferes with property/possessory interest in an “effect”; [Jacobsen meaningful-interference-with-possessory-interest analysis].

This category of seizure (listed as No. 4 in the table above) does not involve a search and occurs when the government's seizure of property merely interferes with an individual's property or possessory interest in that property. See United States v. Jacobsen, 466 U.S. 109, 113 (1984). In Soldal, the Supreme Court rejected the argument that the Fourth Amendment “protect[s] only against seizures that are the outcome of a search.” Soldal, 506 U.S. at 68. The Soldal court was also “unconvinced that any of the Court's prior cases supports the view that the Fourth Amendment protects against unreasonable seizures of property only where tangible to be agents by which a particulate matter trespass was committed upon the defendant's real property. See Elton, 50 Cal. App. 4th at 1306 (Trespass to real property “may be accomplished by the casting of substances or objects upon the [] property from without its boundaries..., even invisible particles of fluoride compounds[.]” (citations omitted)).
privacy or liberty is also implicated.” *Id.* at 65. The Fourth Amendment “protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all.” *Katz*, 389 U.S. at 350. The above reasoning can be applied to any type of seizure (not resulting from a search) as long as the individual alleging the Fourth Amendment violation can establish a mere property or possessory interest in the seized effect.

5. **Seizure that interferes with an individual's liberty interest in a protected activity;** [Soldal meaningful-interference-with-liberty-interest analysis].

This category of seizure (listed as No. 5 in the table above) does not involve a search and occurs when the government merely interferes with an individual's liberty interest in a protected activity. In *Soldal*, the Supreme Court noted that one's “liberty interest... is also protected by the Fourth Amendment[]” under a seizure analysis. *Soldal*, 506 U.S. at 61 (internal citations and quotation marks omitted). For example, the Ninth Circuit in *Sokolow* analyzed a government seizure of luggage and “Sokolow's liberty interest in proceeding with his trip...” *United States v. Sokolow*, 831 F.2d 1413, 1429 (9th Cir. 1988). The above reasoning can be applied to any type of situation where the government interferes with an individual's liberty interest in a Fourth Amendment protected activity.

**E. Identification and classification of the government's Fourth Amendment searches and seizures.**

1. **The government's unauthorized and otherwise illegal Fourth Amendment searches and seizures relating to the aircard locating mission.**

In determining whether there was a Fourth Amendment violation, “the question is whether the challenged search and seizure violated the Fourth Amendment rights of a criminal defendant who seeks to exclude the evidence obtained during it. That inquiry in turn requires a determination of whether the disputed search and seizure has infringed an interest of the defendant which the Fourth Amendment was designed to protect.” *Rakas*, 439 U.S. at 140. In the present case, the defendant's Fourth Amendment protected interests were established in Section V(A), (B) and (C), *supra* (i.e., possessory, property, liberty, and
privacy interests in various places, objects, information, records, resources, and combinations thereof). The government has already conceded that “the aircard tracking operation was a Fourth Amendment search and seizure.”[1320] The government also agreed to not challenge the defendant's identification and classification of its actions into independent Fourth Amendment searches and/or seizures and will instead argue other points in opposition to this motion.[1321] Thus, the only remaining task relevant to this subsection is to (1) identify each independent government search and/or seizure including the place/item searched and what was seized, and (2) classify each independent government search and/or seizure into one or more of the five categories listed in Section V(D), supra.[1322]

Precisely identifying each government search and/or seizure is required because many are not resemblant of traditional “entry” searches and are instead separate, multi-step searches and seizures acting to implicate the defendant's Fourth Amendment rights from multiple angles. The concept of multi-step searches and seizures, albeit in the context of computer searches, was identified in an academic paper by Orin S. Kerr.[1323] The same

1320. See Government's Memorandum Re Motion For Discovery (Dkt. #674, p. 1) (footnote omitted); see also January 4, 2012 Court Order (Dkt. #723, p. 14-15) (“[F]or purposes of Defendant's motion to suppress, the government agrees that the Court may assume that the aircard tracking operation was a Fourth Amendment search and seizure.”).

1321. See, e.g., January 27, 2012 Status Conference, Partial Transcript of Proceedings [MR. BATTISTA], p. 22 (“...I think we may end up arguing with the defendant as to whether or not it's reasonable or not reasonable, whether or not it exceeded the scope of the warrant or whatever....”).

1322. If there is any dispute as to whether any given government action is a Fourth Amendment search and/or seizure as explained by the defendant, the Court indicated that it would allow the defendant to present further arguments in support of his classifications. See January 27, 2012 Status Conference, Partial Transcript of Proceedings [THE COURT], p. 27-28 (“If we get to a gray area, I'm not going to -- I'm not going to say: Well, you didn't prove intrusiveness in this gray area, so I'll at least give you an opportunity to make that argument before I do that if there is a gray area that we haven't covered, but I really don't think there will be one.”).

1323. See Kerr, Orin S., Search Warrants in an Era of Digital Evidence, 75 Miss. L.J. 85, 86-87 (2005) (“The existing law governing the warrant process presumes single-step searches common to the collection of traditional physical evidence. In these cases, the investigators enter the place to be searched, seize the property named in the warrant, and leave. With computer searches, however, the one-step search process is replaced by a two-step search process. The investigators enter the place to be searched; seize the computer hardware; take the hardware off-site; and then later search the equipment for data that may be evidence of crime. Two searches occur instead of one. The physical search comes first and the electronic search comes second. Further, in most cases the two searches are quite distinct. They occur at different times, in different places, and are usually performed by
general “multi-step” principal applies to many of the searches and seizures conducted by the
government to locate the aircard.[1324] Aside from identification, classifying each

government search and/or seizure is also required because different types of searches and
seizures act to infringe different Fourth Amendment protected interests (i.e., property,
possessory, liberty, or privacy interests). *See Argument*, Section V(D), *supra*. The
proceeding subsections consist of a series of tables that identify and classify each
independent government action and list which of the defendant's Fourth Amendment
protected interests were infringed by each action.[1325]

   a. **The government obtaining the defendant's 1.8 million
destination IP addresses relating to his use of the aircard
was a Fourth Amendment search and seizure.**

   The government conducted a Fourth Amendment search and seizure when it forced
Verizon Wireless to turn over the defendant's 1.8 million destination IP addresses revealing
communication content and other private information relating to the defendant's use of his
aircard Internet access service.[1326]

   The government action addressed in this subsection falls into the following categories
of Fourth Amendment searches and/or seizures: (1) search that violates privacy by way of
seizure of records containing private information (*Katz* reasonable-expectation-of-privacy
analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>N/A</td>
<td>1. 1.8 million destination IP</td>
<td>1. Communications content and other</td>
<td>1. Communications content and other</td>
</tr>
</tbody>
</table>

1324. In the proceeding subsections, the defendant identifies each separate, multi-step
search and/or seizure using a series of “progression tables.”

1325. When addressing Fourth Amendment protected interests in the context of the aircard,
if the defendant establishes a protected interest in either the aircard or host laptop computer
it will be sufficient to provide him “standing” to challenge the relevant search and/or seizure.
Such reasoning is supported by the fact that the aircard was attached to the host laptop
computer and was dependent upon the software, electricity, and computing power provided
by the host laptop computer.

1326. *See General Facts*, Section IV(B)(1), *supra*. 
In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Katz* reasonable-expectation-of-privacy analysis, the defendant needs to establish a reasonable expectation of privacy (but not necessarily a property, possessory, or liberty interest) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.8 million destination IP addresses corresponding to the defendant's use of the aircard Internet access service;</td>
<td>Section V(C)(9) et seq., <em>supra</em>.</td>
</tr>
</tbody>
</table>

b. The government obtaining the defendant's historical cell site location information relating to his use of the aircard was a Fourth Amendment search and seizure.

The government conducted a Fourth Amendment search and seizure when it forced Verizon Wireless to turn over the defendant's historical cell site location information, which was used to infer that the aircard and the defendant were located inside apartment No. 1122 on various occasions over a 38 day period.\[1327]\[1328\]

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) search that violates privacy by way of seizure of records containing private information (*Katz* reasonable-expectation-of-privacy analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details: N/A</td>
<td>1. Historical cell site location information relating to aircard while inside a private</td>
<td>1. Location of the aircard and the defendant inside apartment No. 1122.</td>
<td>1. Aircard (via cell site information).</td>
<td>2. Apartment No. 1122 (via cell site information).</td>
</tr>
</tbody>
</table>

1327. *See Argument, Section V(C)(4)(a), *supra* (explaining the search by inference).

1328. The defendant is seeking suppression of all historical cell site location information—regardless of when or how it was obtained.
In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Katz* reasonable-expectation-of-privacy analysis, the defendant needs to establish a reasonable expectation of privacy (but not necessarily a property, possessory, or liberty interest) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Historical cell site location information corresponding to the defendant's use of the aircard Internet access service;</td>
<td>Section V(C)(4) <em>et seq.</em>, <em>supra</em></td>
</tr>
</tbody>
</table>

### c. The FBI using triangulation and location signature techniques on the defendant's historical cell site location information was a Fourth Amendment search and seizure.

The government conducted a Fourth Amendment search and seizure when it used triangulation and location signature techniques on the defendant's historical cell site location information to eliminate 93.9% of the government's initial aircard location estimate.[1329]

The triangulation and location signature techniques assisted the government in making the inference that the aircard and the defendant were located inside apartment No. 1122 over a 38 day period.[1330]

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) non-trespassory search that violates privacy resulting in the obtaining of information (*Katz* reasonable-expectation-of-privacy analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>1. Aircard.</td>
<td>1. Location of the aircard and the</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>


1330. *See id.*
2. Apartment No. 1122.

2. Apartment No. 1122.

defendant inside apartment No. 1122.

In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a Katz reasonable-expectation-of-privacy analysis, the defendant needs to establish a reasonable expectation of privacy (but not necessarily a property, possessory, or liberty interest) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(C)(1) et seq., supra</td>
</tr>
</tbody>
</table>

### d. Verizon Wireless writing data to the aircard via OTAPA was a Fourth Amendment seizure.

The government conducted a Fourth Amendment seizure of the defendant's aircard and home computer when Verizon Wireless, acting as an agent for the government, used Over-the-Air Parameter Administration (OTAPA) to write data to the aircard.\[1331\] The purpose of writing data to the aircard in this context was to ensure that the aircard would recognize the FBI's emulated cellular network as an authorized Verizon Wireless cellular network during the real-time portion of the aircard locating mission.\[1332\]

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) seizure that interferes with property/possessory interest in an “effect” (Jacobsen meaningful-interference-with-possessory-interest analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>N/A</td>
<td>1. Aircard.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

1331. See id., Section IV(B)(5), supra.
1332. See id.
In order for the seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Jacobsen* meaningful-interference-with-possessory-interest analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (i.e., aircard);</td>
<td>Section V(A)(2), <em>supra</em></td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (i.e., host laptop computer);</td>
<td>Section V(A)(3), <em>supra</em></td>
</tr>
</tbody>
</table>

**e. Verizon Wireless reprogramming the aircard via OTAPA, or flashing its firmware over-the-air, was a Fourth Amendment seizure.**

The government conducted a Fourth Amendment seizure of the defendant's aircard and home computer when Verizon Wireless, acting as an agent for the government, used Over-the-Air Parameter Administration (OTAPA) to set the aircard's manufacturer specific NAM parameters (or used IOTA-DM firmware over-the-air (FOTA) to flash the aircard's firmware) to reprogram the aircard. The purpose of reprogramming the aircard in this context was to force the aircard to respond to the FBI's surreptitious voice calls (used as a denial-of-service attack) and to force it to generate real-time cell site sector location information.

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) seizure that interferes with property/possessory interest in an “effect” (*Jacobsen* meaningful-interference-with-possessory-interest analysis). The government action addressed in this subsection can be

---

1333. *See id.*, Section IV(B)(5), *supra*.
1334. *See id.*
charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>N/A</td>
<td>1. Aircard.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Host laptop computer.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order for the seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Jacobsen* meaningful-interference-with-possessor-interest analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (<em>i.e.</em>, aircard);</td>
<td>Section V(A)(2), <em>supra</em></td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (<em>i.e.</em>, host laptop computer);</td>
<td>Section V(A)(3), <em>supra</em></td>
</tr>
</tbody>
</table>

f. The FBI using the SF-Martinez DCS-3000 Pen/Trap device to obtain the defendant's real-time cell site sector location information relating to his use of the aircard was a Fourth Amendment search and seizure.

The FBI conducted a Fourth Amendment search and seizure when it (1) forced the aircard to generate real-time cell site sector location information (over a six hour period) while the aircard was inside apartment No. 1122 and not engaged in a call, and (2) forced Verizon Wireless to provide the SF-Martinez DCS-3000 Pen/Trap device with the generated geolocation data.\[1335\][1336] The purpose of generating and obtaining the aircard's real-time cell site sector location information was to narrow the geographical area of where to search

1335. *See id.*, Section IV(B)(6), *supra*.

1336. The defendant is seeking suppression of all real-time aircard cell site location information—regardless of when or how it was obtained.
for the aircard and the defendant using the StingRay and KingFish.\footnote{1337} The FBI technical agents forced the aircard to generate the real-time cell site sector location information by placing surreptitious voice calls to the aircard after reprogramming it to respond to the calls.\footnote{1338}

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) trespassory search resulting in the obtaining of information (\textit{Jones} trespass-to-obtain-information analysis), and (2) non-trespassory search that violates privacy resulting in the obtaining of information (\textit{Katz} reasonable-expectation-of-privacy analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>1. Aircard (via over-the-air signals from Verizon cell site but generated by FBI). 2. Host laptop computer (via over-the-air signals from Verizon cell site but generated by FBI). 3. A private residence (\textit{i.e.}, Apartment No. 1122) (via over-the-air signals from Verizon cell site but generated by FBI).</td>
<td>1. Real-time cell site location information relating to the aircard while inside apartment No. 1122 and \textbf{not engaged in a call}.</td>
<td>1. Aircard (via cell site information). 2. Apartment No. 1122 (via cell site information).</td>
<td>1. Location of the aircard and the defendant inside apartment No. 1122.</td>
</tr>
</tbody>
</table>

In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a \textit{Jones} trespass-to-obtain-information analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (\textbf{but not all}) of the

\footnote{1337} See id. \footnote{1338} See id., Section IV(B)(5), supra.
In the alternative, in order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Katz* reasonable-expectation-of-privacy analysis, the defendant needs to establish a reasonable expectation of privacy (but not necessarily a property, possessory, or liberty interest) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (i.e., aircard);</td>
<td>Section V(A)(2), <em>supra</em></td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (i.e., host laptop computer);</td>
<td>Section V(A)(3), <em>supra</em></td>
</tr>
<tr>
<td>3</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(A)(1), <em>supra</em></td>
</tr>
</tbody>
</table>

The FBI forcing Verizon Wireless to obtain and provide real-time geolocation information relating to the location of the aircard was a Fourth Amendment search and seizure.

The FBI conducted a Fourth Amendment search and seizure when it forced Verizon Wireless to obtain and provide real-time geolocation information showing, at the very least, the distance between a Verizon Wireless cell site and the aircard. The purpose of

---

1339. To clarify, the defendant asserts that the government action addressed in this subsection is a Fourth Amendment search and seizure under both a *Jones* trespass-to-obtain-information analysis and *Katz* reasonable-expectation-of-privacy analysis.

1340. *See id.*, Section IV(B)(7), *supra*. 

- 266 -
obtaining the aircard's real-time geolocation information was to narrow the geographical area
of where to search for the aircard and the defendant using the StingRay and KingFish.\[1341\]
Precise details on the information seized and how it was obtained by Verizon Wireless
remains a mystery considering the government destroyed the evidence obtained from
Verizon Wireless\[1342\] and refuses to produce the FBI technical agents for defense
questioning.\[1343\]

At the very least, the government action addressed in this subsection falls into the
following categories of Fourth Amendment searches and/or seizures: (1) non-trespassory
search that violates privacy resulting in the obtaining of information (\textit{Katz} reasonable-
expectation-of-privacy analysis). However, because the government prejudiced the defense
by destroying the evidence it seized from Verizon Wireless,\[1344\][1345\] the defendant is
unable to confirm whether a \textit{Jones} trespass-to-obtain-information search occurred. The
government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>1. Possibly the aircard (via over-the-air signals transmitted to the aircard by Verizon Wireless). [UNKNOWN DUE TO GOVERNMENT DESTRUCTION OF EVIDENCE]</td>
<td>1. Real-time aircard geolocation information while aircard was inside Apartment No. 1122.</td>
<td>1. Aircard (via geolocation information).</td>
<td>1. Location of the aircard and the defendant inside apartment No. 1122.</td>
</tr>
<tr>
<td>2. Possibly the host laptop computer (via over-the-air signals transmitted)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1341. \textit{See id.}
1342. \textit{See id.}, Section IV(B)(15), \textit{supra}.
1343. \textit{See}, \textit{e.g.}, January 4, 2012 Court Order (Dkt. #723).
1344. \textit{See} accompanying \textit{Memorandum RE: Destruction Of Evidence}.
1345. There is additional prejudice suffered by the defendant due to the government's
destruction of the real-time aircard geolocation information relevant to this section. \textit{See id.}
In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Jones* trespass-to-obtain-information analysis,[1346] the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (<em>i.e.</em>, aircard);</td>
<td>Section V(A)(2), <em>supra</em></td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (<em>i.e.</em>, host laptop computer);</td>
<td>Section V(A)(3), <em>supra</em></td>
</tr>
<tr>
<td>3</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(A)(1), <em>supra</em></td>
</tr>
</tbody>
</table>

In the alternative, in order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Katz* reasonable-expectation-of-privacy analysis, the defendant needs to establish a reasonable expectation of privacy.

1346. There is sufficient evidence to show a search and seizure under a *Katz* reasonable-expectation-of-privacy analysis. However, the evidence needed to show a search and seizure under a *Jones* trespass-to-obtain-information analysis has been destroyed by the government.
privacy (but not necessarily a property, possessory, or liberty interest) in at least one \( \text{but not all} \) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card ( (i.e., \text{aircard}) );</td>
<td>Section V(C)(2) ( \text{et seq.} ), supra</td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 ( (i.e., \text{host laptop computer}) );</td>
<td>Section V(C)(2) ( \text{et seq.} ), supra</td>
</tr>
<tr>
<td>3</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(C)(1) ( \text{et seq.} ), supra</td>
</tr>
</tbody>
</table>

h. The FBI using surreptitious phone calls to deny the defendant access to the Internet for six hours \( (i.e., \text{denial-of-service attack}) \) was a Fourth Amendment seizure.

The FBI technical agents conducted a Fourth Amendment seizure of the defendant's aircard Internet access service, aircard, and home computer when they used 32 surreptitious phone calls to consistently boot the defendant's aircard off the Internet over a six hour period. \[1347\] The purpose of placing surreptitious phone calls to the aircard was to force it to disconnect from its 1xEV-DO Rel. 0 data connection and enter the Idle State so that its air interface connection could be hijacked by the StingRay and KingFish. \[1348\]

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: \( (1) \) seizure that interferes with property/possessory interest in an “effect” \( (\text{Jacobsen meaningful-interference-with-possessory-interest analysis}) \), and \( (2) \) seizure that interferes with an individual's liberty interest in a protected activity \( (\text{Soldal meaningful-interference-with-liberty-interest analysis}) \).

The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>N/A</td>
<td>1. Aircard Internet access service.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Aircard.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1347. \textit{See id.}, Section IV(B)(8), \textit{supra}.

1348. \textit{See id.}
In order for the seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Jacobsen* meaningful-interference-with-possessory-interest analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (**but not all**) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (<em>i.e.</em>, aircard);</td>
<td>Section V(A)(2), <em>supra</em></td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (<em>i.e.</em>, host laptop computer);</td>
<td>Section V(A)(3), <em>supra</em></td>
</tr>
</tbody>
</table>

In the alternative, in order for the seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Soldal* meaningful-interference-with-liberty-interest analysis, the defendant needs to establish a liberty interest (but not a property/possessory interest or reasonable expectation of privacy) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to seizure:</th>
<th>Liberty interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The defendant's use of the aircard Internet access service provided by Verizon Wireless;</td>
<td>Section V(B), <em>supra</em></td>
</tr>
</tbody>
</table>

i. The FBI forcing the aircard to handoff its 1xEV-DO Rel. 0 connection to the emulated cellular network broadcast by the StingRay and KingFish was a Fourth Amendment seizure.

The FBI technical agents conducted a Fourth Amendment seizure of the defendant's aircard and home computer when they forced the aircard to connect to their emulated cellular network broadcast by the StingRay and KingFish. The FBI technical agents forced the aircard to disconnect from its legitimate 1xEV-DO Rel. 0 data connection provided by

---

1349. *See id.*, Section IV(B)(9)(a) and (h) ¶ 62, *supra*. 

- 270 -
Verizon Wireless\textsuperscript{1350} so that it would handoff its connection to the stronger signal being broadcast by the StingRay and then later the KingFish.\textsuperscript{1351} The purpose of forcing the handoff (\textit{i.e.,} Idle State route update) was so that FBI technical agents could seize complete control of the aircard.\textsuperscript{1352}

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (I) seizure that interferes with property/possessory interest in an “effect” (\textit{Jacobsen} meaningful-interference-with-possessory-interest analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Seached place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Seached place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>N/A</td>
<td>1. Aircard.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Host laptop computer.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order for the seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a \textit{Jacobsen} meaningful-interference-with-possessory-interest analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (\textbf{but not all}) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (\textit{i.e.,} aircard);</td>
<td>Section V(A)(2), \textit{supra}.</td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (\textit{i.e.,} host laptop computer);</td>
<td>Section V(A)(3), \textit{supra}.</td>
</tr>
</tbody>
</table>

\textsuperscript{1350} See \textit{id.}, Section IV(B)(8), \textit{supra}.

\textsuperscript{1351} See \textit{id.}, Section IV(B)(9)(a), \textit{supra}.

\textsuperscript{1352} See \textit{id.}, Section IV(B)(9) et seq., \textit{supra}.
j. The FBI repeatedly writing data to the aircard using the StingRay and KingFish was a Fourth Amendment seizure.

The FBI technical agents conducted a Fourth Amendment seizure of the defendant's aircard and home computer when they used the StingRay and KingFish to repeatedly write data to the aircard's internal storage device.\[1353][1354] The purpose of writing data to the aircard was so that the FBI technical agents could continue to communicate with the aircard over the air interface while the StingRay and KingFish conducted geolocation techniques in cell site emulator mode.\[1355]

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (I) seizure that interferes with property/possessory interest in an “effect” (Jacobsen meaningful-interference-with-possessory-interest analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>N/A</td>
<td>1. Aircard.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Host laptop computer.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order for the seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a Jacobsen meaningful-interference-with-possessory-interest analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1353.</td>
<td>See id., Section IV(B)(9)(b), supra.</td>
<td></td>
</tr>
<tr>
<td>1354.</td>
<td>The FBI writing data to the aircard using the StingRay and KingFish is completely separate from Verizon Wireless writing data to the aircard using a cell site. The two separate acts have different Fourth Amendment implications due to how the authorizations are construed in the N.D.Cal. 08-90330MISC-RS order.</td>
<td></td>
</tr>
<tr>
<td>1355.</td>
<td>See id.</td>
<td></td>
</tr>
</tbody>
</table>
The FBI technical agents conducted a Fourth Amendment seizure of the defendant's aircard and home computer when they disabled standard 1xEV-DO Rel. 0 air interface encryption while communicating with the aircard using the StingRay and KingFish.\[1356\] While encryption was disabled, the FBI forced the aircard to transmit its stored ESN and other data used for geolocation making that data available to anyone using a passive eavesdropping device.

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) seizure that interferes with property/possessory interest in an “effect” \(Jacobsen\ meaningful-interference-with-possessory-interest\ analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>N/A</td>
<td>1. Aircard.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Host laptop computer.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order for the seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a \(Jacobsen\ meaningful-interference-with-possessory-interest\ analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one \(\textbf{not all}\) of the following:

1356. \textit{See id.}, Section IV(B)(9)(c), \textit{supra}. 
1. The FBI using the StingRay and KingFish to remotely access and download data from the aircard was a Fourth Amendment search and seizure.

The FBI technical agents conducted a Fourth Amendment search and seizure when they (1) used the StingRay and KingFish to remotely access the aircard's internal storage device over the air interface, and (2) used the StingRay and KingFish to download the aircard's stored ESN.\[1357\] The purpose of downloading the aircard's stored ESN via the StingRay and KingFish was to identify the aircard amongst other wireless devices in the target area.\[1358\]

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) trespassory search resulting in the obtaining of information (*Jones* trespass-to-obtain-information analysis), and (2) non-trespassory search that violates privacy resulting in the obtaining of information (*Katz* reasonable-expectation-of-privacy analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>1. Aircard (via over-the-air signals sent from StingRay and KingFish).</td>
<td>1. ESN data stored on aircard's internal storage device.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>2. Host laptop computer (via over-the-air signals sent from StingRay and KingFish).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. A private residence (<em>i.e.</em>, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[1357\] See *id.*, Section IV(B)(9)(d), *supra*.

\[1358\] See *id.*
In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Jones* trespass-to-obtain-information analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (<em>i.e.</em>, aircard);</td>
<td>Section V(A)(2), <em>supra</em></td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (<em>i.e.</em>, host laptop computer);</td>
<td>Section V(A)(3), <em>supra</em></td>
</tr>
<tr>
<td>3</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(A)(1), <em>supra</em></td>
</tr>
</tbody>
</table>

In the alternative, in order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Katz* reasonable-expectation-of-privacy analysis,[1359] the defendant needs to establish a reasonable expectation of privacy (but not necessarily a property, possessory, or liberty interest) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (<em>i.e.</em>, aircard);</td>
<td>Section V(C)(2) <em>et seq.</em>, <em>supra</em></td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (<em>i.e.</em>, host laptop computer);</td>
<td>Section V(C)(2) <em>et seq.</em>, <em>supra</em></td>
</tr>
<tr>
<td>3</td>
<td>ESN data stored on aircard's internal storage device;</td>
<td>Section V(C)(7) <em>et seq.</em>, <em>supra</em></td>
</tr>
<tr>
<td>4</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(C)(1) <em>et seq.</em>, <em>supra</em></td>
</tr>
</tbody>
</table>

1359. To clarify, the defendant asserts that the government action addressed in this subsection is a Fourth Amendment search and seizure under both a *Jones* trespass-to-obtain-information analysis and *Katz* reasonable-expectation-of-privacy analysis.
m. The FBI using the StingRay and KingFish to send location finding interrogation signals into the defendant's home and aircard was a Fourth Amendment search and seizure.

The FBI technical agents conducted a Fourth Amendment search and seizure when they used the StingRay and KingFish to transmit beams of location finding interrogation signals into apartment No. 1122 and the aircard. The purpose of transmitting location finding interrogation signals was to remotely search apartment No. 1122 in order to locate the aircard.

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) trespassory search resulting in the obtaining of information (Jones trespass-to-obtain-information analysis), and (2) non-trespassory search that violates privacy resulting in the obtaining of information (Katz reasonable-expectation-of-privacy analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>1. Aircard (via over-the-air signals sent from StingRay and KingFish).</td>
<td>1. Aircard. 2. Host laptop computer. 3. Location of the aircard and the defendant inside apartment No. 1122.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>2. Host laptop computer (via over-the-air signals sent from StingRay and KingFish).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. A private residence (i.e., Apartment No. 1122) (via over-the-air signals sent from StingRay and KingFish).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order for the search and seizure addressed in this subsection to be a potential

1360. See id., Section IV(B)(9)(e), supra.
1361. See id.
violation of the defendant's Fourth Amendment rights under a Jones trespass-to-obtain-information analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (i.e., aircard);</td>
<td>Section V(A)(2), supra</td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (i.e., host laptop computer);</td>
<td>Section V(A)(3), supra</td>
</tr>
<tr>
<td>3</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(A)(1), supra</td>
</tr>
</tbody>
</table>

In the alternative, in order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a Katz reasonable-expectation-of-privacy analysis, the defendant needs to establish a reasonable expectation of privacy (but not necessarily a property, possessory, or liberty interest) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (i.e., aircard);</td>
<td>Section V(C)(2) et seq., supra</td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (i.e., host laptop computer);</td>
<td>Section V(C)(2) et seq., supra</td>
</tr>
<tr>
<td>3</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(C)(1) et seq., supra</td>
</tr>
</tbody>
</table>

The FBI using the StingRay and KingFish to collect the aircard's signal transmissions sent in response to the location finding interrogation signals was a Fourth Amendment search and seizure.

The FBI technical agents conducted a Fourth Amendment search and seizure when they used the StingRay and KingFish to collect the aircard's signal transmissions sent in response to the location finding interrogation signals. The FBI using the StingRay and KingFish to collect the aircard's signal transmissions sent in response to the location finding interrogation signals was a Fourth Amendment search and seizure.

1362. To clarify, the defendant asserts that the government action addressed in this subsection is a Fourth Amendment search and seizure under both a Jones trespass-to-obtain-information analysis and Katz reasonable-expectation-of-privacy analysis.
response to the previously transmitted location finding interrogation signals. The purpose of collecting the aircard's location finding response signals was to subject them to geolocation measurements while triangulating the location of the aircard and the defendant inside his home.

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) trespassory search resulting in the obtaining of information (Jones trespass-to-obtain-information analysis), and (2) non-trespassory search that violates privacy resulting in the obtaining of information (Katz reasonable-expectation-of-privacy analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>1. Aircard (via over-the-air signals sent from StingRay and KingFish).</td>
<td>1. Location finding response signals transmitted by aircard (used for geolocation by StingRay and KingFish).</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>2. Host laptop computer (via over-the-air signals sent from StingRay and KingFish).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a Jones trespass-to-obtain-information analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (i.e., aircard);</td>
<td>Section V(A)(2), supra</td>
</tr>
</tbody>
</table>

1363. See id., Section IV(B)(9)(e), supra.
1364. See id.
In the alternative, in order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a *Katz* reasonable-expectation-of-privacy analysis, the defendant needs to establish a reasonable expectation of privacy (but not necessarily a property, possessory, or liberty interest) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (i.e., aircard);</td>
<td>Section V(C)(2) et seq., <em>supra</em></td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (i.e., host laptop computer);</td>
<td>Section V(C)(2) et seq., <em>supra</em></td>
</tr>
<tr>
<td>3</td>
<td>Aircard signals transmitted over the air interface (i.e., location finding response signals);</td>
<td>Section V(C)(6) et seq., <em>supra</em></td>
</tr>
</tbody>
</table>

**o. The FBI using the StingRay and KingFish to conduct triangulation techniques on aircard signals transmitted in response to interrogation was a Fourth Amendment search and seizure.**

The FBI technical agents conducted a Fourth Amendment search and seizure when they used the StingRay and KingFish to conduct triangulation techniques on the aircard's location finding response signals sent in response to interrogation. The purpose of conducting triangulation techniques on the aircard's collected signals was to first narrow down the location of the aircard and the defendant to the the Domicilio apartment complex (using the StingRay) and then to pinpoint the location of the aircard and the defendant inside apartment No. 1122 (using the KingFish).

The government action addressed in this subsection falls into the following categories.
of Fourth Amendment searches and/or seizures: (i) non-trespassory search that violates privacy resulting in the obtaining of information (Katz reasonable-expectation-of-privacy analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>1. Aircard.</td>
<td>1. Geolocation data showing the location of the aircard and the defendant inside apartment No. 1122.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>2. Apartment No. 1122.</td>
<td>2. Location of the aircard and the defendant inside apartment No. 1122.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a Katz reasonable-expectation-of-privacy analysis, the defendant needs to establish a reasonable expectation of privacy (but not necessarily a property, possessory, or liberty interest) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(C)(1) et seq., supra</td>
</tr>
</tbody>
</table>

p. The FBI using the StingRay and KingFish to deny the defendant access to the Internet for ten hours (i.e., denial-of-service attack) was a Fourth Amendment seizure.

The FBI technical agents conducted a Fourth Amendment seizure of the defendant's aircard Internet access service, aircard, and home computer when use of the StingRay and KingFish acted to deny the aircard access to the Internet for a ten hour period. 1369 The aircard was denied access to the Internet for the noted ten hour period (while the aircard was

1369. See id., Section IV(B)(9)(i), supra.
because the StingRay and KingFish are not programmed to provide cellular service while hijacking the connection of a target wireless device.\[^{1370}\]

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) seizure that interferes with property/possessory interest in an “effect” (Jacobsen meaningful-interference-with-possessory-interest analysis), and (2) seizure that interferes with an individual's liberty interest in a protected activity (Soldal meaningful-interference-with-liberty-interest analysis).

The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>N/A</td>
<td>1. Aircard Internet access service.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Aircard.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Host laptop computer.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order for the seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a Jacobsen meaningful-interference-with-possessory-interest analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UTStarcom PC5740 broadband access card (i.e., aircard);</td>
<td>Section V(A)(2), supra</td>
</tr>
<tr>
<td>2</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (i.e., host laptop computer);</td>
<td>Section V(A)(3), supra</td>
</tr>
</tbody>
</table>

In the alternative, in order for the seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a Soldal meaningful-interference-with-liberty-interest analysis, the defendant needs to establish a liberty interest (but not a property or possessory interest) in a protected activity.

---

\[^{1370}\] See Technical Explanations, Section II(G), supra (explaining how the StingRay and KingFish do not conduct man-in-the-middle attacks).
interference-with-liberty-interest analysis, the defendant needs to establish a liberty interest (but not a property/possessory interest or reasonable expectation of privacy) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to seizure:</th>
<th>Liberty interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The defendant's use of the aircard Internet access service provided by Verizon Wireless;</td>
<td>Section V(B), <em>supra</em></td>
</tr>
</tbody>
</table>

**q. The FBI using the defendant's electricity provided to his aircard and forcing the aircard to transmit at the highest possible power was a Fourth Amendment seizure.**

The FBI technical agents conducted a Fourth Amendment seizure of the defendant's electricity, aircard, and home computer when they (1) utilized the defendant's electricity purchased for his home,[1371] and (2) forced the aircard to transmit at the highest possible power.[1372] The defendant's electricity provided to the aircard was relied upon by the StingRay and KingFish while the aircard was forced to transmit signals in response to interrogation.[1373] Furthermore, the aircard was forced to transmit at the highest possible power so that signal quality would be increased for subsequent geolocation measurements.[1374]

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) seizure that interferes with property/possessory interest in an “effect” (*Jacobsen* meaningful-interference-with-possessory-interest analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>N/A</td>
<td><strong>1. Electricity provided to aircard</strong></td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>


1372. *See id.*, Section IV(B)(9)(k), *supra*.

1373. *See id.*, Section IV(B)(9)(j), *supra*.

1374. *See id.*, Section IV(B)(9)(k), *supra*.
and laptop (i.e., apartment No. 1122 electricity).
2. Aircard
3. Host laptop computer

In order for the seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a Jacobsen meaningful-interference-with-possessory-interest analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in at least one (but not all) of the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Apartment No. 1122 electricity purchased from Silicon Valley Power (i.e., electricity provided to aircard and laptop);</td>
<td>Section V(A)(4), supra</td>
</tr>
<tr>
<td>2</td>
<td>UTStarcom PC5740 broadband access card (i.e., aircard);</td>
<td>Section V(A)(2), supra</td>
</tr>
<tr>
<td>3</td>
<td>Lenovo IBM ThinkPad S/N #LV-C4398 (i.e., host laptop computer);</td>
<td>Section V(A)(3), supra</td>
</tr>
</tbody>
</table>

FBI Agent Murray conducted a Fourth Amendment search and seizure when he and an employee from Quality Alarm Service obtained the defendant's historical geolocation information, via his Domicilio electronic gate key access records, which were used to infer that the aircard and the defendant were located inside apartment No. 1122 on specific occasions.\[1375\]

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (I) search that violates privacy by way of seizure of records containing private information (Katz reasonable-expectation-of-privacy...
The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>N/A</td>
<td>1. Historical geolocation information via Domicilio electronic gate key access records.</td>
<td>1. Apartment No. 1122.</td>
<td>1. Location of the defendant inside apartment No. 1122.</td>
</tr>
</tbody>
</table>

In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a \textit{Katz} reasonable-expectation-of-privacy analysis, the defendant needs to establish a reasonable expectation of privacy (but not necessarily a property, possessory, or liberty interest) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Historical geolocation information corresponding to the defendant entering apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(C)(8) et seq., supra</td>
</tr>
</tbody>
</table>

\textbf{s. FBI Agent Nguyen using the defendant's key to verify that it unlocked apartment No. 1122 was a Fourth Amendment search and seizure.}

FBI Agent Nguyen conducted a Fourth Amendment search and seizure when he/she used a key found on the defendant during his arrest to verify that it unlocked the front door of apartment No. 1122.\footnote{1376} The defendant was not arrested within the vicinity of apartment No. 1122 and FBI Agent Nguyen conducted the key hole search to determine if the defendant lived at (or came from) apartment No. 1122.\footnote{1377}

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) trespassory search resulting in the obtaining of information (\textit{Jones} trespass-to-obtain-information analysis). The government

\footnote{1376. \textit{See id.}, Section IV(B)(14), \textit{supra}.}  
\footnote{1377. \textit{See id}.}
action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>1. Apartment No. 1122.</td>
<td>1. Information that the defendant lived at (or came from) apartment No. 1122.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a Jones trespass-to-obtain-information analysis, the defendant needs to establish a property or possessory interest (but not a liberty interest or reasonable expectation of privacy) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(A)(1), supra</td>
</tr>
</tbody>
</table>

2. The government's unauthorized and otherwise illegal Fourth Amendment searches and seizures relating to the in-person search of apartment No. 1122.

a. Various agents entering the defendant's home to seize his possessions was a Fourth Amendment search and seizure.

On August 3-4, 2008, various agents entered apartment No. 1122 to search the defendant's possessions for evidence.\[1378\] As a result of the search, the government seized various effects belonging to the defendant including his physical data storage devices and encrypted virtual drives.\[1379\]

The government action addressed in this subsection is a traditional “entry” search resulting in the seizure of effects. Whether a defendant can challenge a traditional entry search depends on whether he can establish either a property/possessory interest in the place searched, or a reasonable expectation of privacy in the place searched or the items seized.

1378. See id., Section IV(B)(16), supra.
1379. See id.
The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Details:</th>
<th>Progression:</th>
<th>Seached place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Seached place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Apartment No. 1122.</td>
<td>➞</td>
<td>1. Physical effects including physical data storage devices and encrypted virtual drives.</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a property/possessory interest analysis, the defendant needs to establish a property or possessory interest (but not a reasonable expectation of privacy) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Property/possessory interest established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(A)(1), supra</td>
</tr>
</tbody>
</table>

In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a reasonable expectation of privacy analysis, the defendant needs to establish a reasonable expectation of privacy (but not a property/possessory interest) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Apartment No. 1122 at the Domicilio apartment complex;</td>
<td>Section V(C)(1) et seq., supra</td>
</tr>
<tr>
<td>2</td>
<td>The effects seized from apartment No. 1122 (including physical data storage devices and encrypted virtual drives), see returns for N.D.Cal. 08-70460-HRL/PVT &amp; 08-70503-PVT warrants;</td>
<td>Section V(C)(1) et seq., supra</td>
</tr>
</tbody>
</table>

b. IRS-CI Agent Daun continuing to search the forensic images of the defendant's encrypted virtual drives was/is a Fourth Amendment search and seizure.

During and after the August 3-4, 2008 search of apartment No. 1122, IRS-CI agent
Daun created forensic images of the defendant's physical data storage devices and encrypted virtual drives. Within 30 days of August 3, 2008 (as authorized by N.D.Cal. 08-70460-HRL/PVT warrant), IRS-CI Agent Daun searched the forensic images for evidence. As a result, IRS-CI agent Daun extracted all files that fell within the scope of the warrant and then copied some of those files to DVDs so that they would be isolated (i.e., seized) from the images. Once the 30 day window of time to search for and seize data had expired, IRS-CI Agent Daun continued to search the encrypted virtual drives for evidence and her searching continued at least until October of 2011.

The government action addressed in this subsection falls into the following categories of Fourth Amendment searches and/or seizures: (1) non-trespassory search that violates privacy resulting in the obtaining of information (Katz reasonable-expectation-of-privacy analysis). The government action addressed in this subsection can be charted as follows:

<table>
<thead>
<tr>
<th>Progression:</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
<th>Searched place(s), item(s), etc.</th>
<th>Seized effect(s), information, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>1. Forensic hard drive images and encrypted virtual drives.</td>
<td>1. Data contained within encrypted virtual drives.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

In order for the search and seizure addressed in this subsection to be a potential violation of the defendant's Fourth Amendment rights under a Katz reasonable-expectation-of-privacy analysis, the defendant needs to establish a reasonable expectation of privacy (but not necessarily a property, possessory, or liberty interest) in the following:

<table>
<thead>
<tr>
<th>#</th>
<th>Place, object, information, record, resource, or combination thereof relevant to search and seizure:</th>
<th>Reasonable expectation of privacy established at:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Forensic hard drive images and encrypted virtual drives in possession of government after Sept. 2, 2008 (i.e., after Section V(C)(10), supra)</td>
<td></td>
</tr>
</tbody>
</table>

1380. See id., Section IV(B)(17), supra.
1381. See id.
1382. See id.
1383. See id.
F. The searches and seizures identified in Section V(E), supra, were conducted in violation of the defendant's Fourth Amendment rights due to unreasonableness and lack of proper judicial authority.

Prior to this section, the defendant established his privacy, property, possessory, and liberty interests in various places, objects, information, records, resources, and combinations thereof. See Argument, Sections V(A), (B), and (C), supra. The defendant also separated and categorized the government's various Fourth Amendment searches and seizures and showed how they acted to infringe upon his Fourth Amendment protected interests as potential Fourth Amendment violations. See Argument, Section V(D) and (E), supra. In this section, the defendant explains how the government's Fourth Amendment searches and seizures were unreasonable and therefore actual (as apposed to potential) violations of his Fourth Amendment rights. See United States v. Sharpe, 470 U.S. 675, 682 (1985) ("The Fourth Amendment is not, of course, a guarantee against all searches and seizures, but only against unreasonable searches and seizures."). The Fourth Amendment violations explained in this section resulted from searches and seizures that were either (1) unsupported by relevant probable cause findings, (2) conducted outside the scope of what the various orders authorized, (3) conducted pursuant to orders and subpoenas that do not meet particularity requirements, or (4) otherwise conducted in general violation of the reasonableness clause of the Fourth Amendment.\[1384\] In the proceeding subsections, all Fourth Amendment violation are categorized under the order, subpoena, or warrant applicable to the challenged search and/or seizure. All violations explained in this section were unattenuated but-for causes of obtaining various evidence sought to be suppressed.

1384. See Dalia v. United States, 441 U.S. 238, 258 (1979) ("[T]he manner in which a warrant is executed is subject to later judicial review as to its reasonableness.")
1. The N.D.Cal. 08-90330MISC-RS order did not render any of the applicable searches and seizures reasonable.

The places, items, etc. searched by the government while executing the N.D.Cal. 08-90330MISC-RS order are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Searched place, item, etc.:</th>
<th>Explanation of relevant searches conducted by the government:</th>
<th>Sections addressing searches:</th>
</tr>
</thead>
</table>
| 1 | A private residence (i.e., Apartment No. 1122);                                                             | (1) sending location finding interrogation signals into the defendant's home and aircard using the StingRay and KingFish; (2) conducting triangulation techniques on the aircard's forced signal transmissions sent in response to interrogation using the StingRay and KingFish; (3) obtaining from Verizon Wireless real-time geolocation information relating to the location of the aircard while inside apartment No. 1122; | 1. Section V(E)(1)(m)  
2. Section V(E)(1)(o)  
3. Section V(E)(1)(g) |
| 2 | Aircard (i.e., UTStarcom PC5740 broadband access card);                                                      | (1) remotely accessing and downloading data from the aircard using the StingRay and KingFish; (2) sending location finding interrogation signals into the defendant's home and aircard using the StingRay and KingFish; (3) collecting the aircard's forced signal transmissions using the StingRay and KingFish; (4) conducting triangulation techniques on the aircard's forced signal transmissions sent in response to interrogation using the StingRay and KingFish; (5) obtaining from Verizon Wireless real-time geolocation information relating to the location of the aircard while inside apartment No. 1122; | 1. Section V(E)(1)(l)  
2. Section V(E)(1)(m)  
3. Section V(E)(1)(n)  
4. Section V(E)(1)(o)  
5. Section V(E)(1)(g) |
| 3 | Host laptop computer (i.e., Lenovo IBM ThinkPad S/N #LV-C4398);                                            | (1) remotely accessing and downloading data from the aircard using the StingRay and KingFish; (2) sending location finding interrogation signals into the defendant's home and aircard using the StingRay and KingFish; (3) collecting the aircard's forced signal transmissions using the StingRay and KingFish; | 1. Section V(E)(1)(l)  
2. Section V(E)(1)(m)  
3. Section V(E)(1)(n) |

The effects, information, etc. seized by the government while executing the N.D.Cal. 08-90330MISC-RS order are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Seized effect, item, etc.:</th>
<th>Explanation of relevant seizures (or preceding Sections addressing searches):</th>
</tr>
</thead>
</table>

1385. “[T]he United States agrees to rely solely on the Rule 41 tracking warrant, application, and affidavit, No. CR08-90330-MISC, to authorize the use of equipment to communicate directly with Defendant’s aircard and determine its location.” Government's Memorandum RE Motion For Discovery (footnote omitted) (Dkt. #674, p. 2).
<table>
<thead>
<tr>
<th>No.</th>
<th>Information, etc.:</th>
<th>Searches) conducted by the government:</th>
<th>Seizures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Aircard (i.e., UTStarcom PC5740 broadband access card);</td>
<td>(1) forcing the aircard to handoff its connection and establish a session with the StingRay and KingFish; (2) repeatedly writing data to the aircard using the StingRay and KingFish; (3) disabling standard encryption for aircard signals using the StingRay and KingFish; (4) sending location finding interrogation signals into the defendant's home and aircard using the StingRay and KingFish; (5) denying the defendant access to the Internet for ten hours using the StingRay and KingFish; (6) using the defendant's electricity provided to his aircard and forcing the aircard to transmit at the highest possible power;</td>
<td>1. Section V(E)(1)(i) 2. Section V(E)(1)(j) 3. Section V(E)(1)(k) 4. Section V(E)(1)(m) 5. Section V(E)(1)(p) 6. Section V(E)(1)(q)</td>
</tr>
<tr>
<td>2</td>
<td>Host laptop computer (i.e., Lenovo IBM ThinkPad S/N #LC4398);</td>
<td>(1) forcing the aircard to handoff its connection and establish a session with the StingRay and KingFish; (2) repeatedly writing data to the aircard using the StingRay and KingFish; (3) disabling standard encryption for aircard signals using the StingRay and KingFish; (4) sending location finding interrogation signals into the defendant's home and aircard using the StingRay and KingFish; (5) denying the defendant access to the Internet for ten hours using the StingRay and KingFish; (6) using the defendant's electricity provided to his aircard and forcing the aircard to transmit at the highest possible power;</td>
<td>1. Section V(E)(1)(i) 2. Section V(E)(1)(j) 3. Section V(E)(1)(k) 4. Section V(E)(1)(m) 5. Section V(E)(1)(p) 6. Section V(E)(1)(q)</td>
</tr>
<tr>
<td>3</td>
<td>ESN data stored on aircard's internal storage device;</td>
<td>(1) remotely accessing and downloading data from the aircard using the StingRay and KingFish;</td>
<td>1. Section V(E)(1)(l)</td>
</tr>
<tr>
<td>4</td>
<td>Location finding response signals transmitted by aircard;</td>
<td>(1) collecting the aircard's forced signal transmissions using the StingRay and KingFish;</td>
<td>1. Section V(E)(1)(n)</td>
</tr>
<tr>
<td>5</td>
<td>Geolocation data showing the location of the aircard and the defendant inside apartment No. 1122;</td>
<td>(1) conducting triangulation techniques on the aircard's forced signal transmissions sent in response to interrogation using the StingRay and KingFish;</td>
<td>1. Section V(E)(1)(o)</td>
</tr>
<tr>
<td>6</td>
<td>Location of the aircard and the defendant inside apartment No. 1122;</td>
<td>(1) sending location finding interrogation signals into the defendant's home and aircard using the StingRay and KingFish; (2) conducting triangulation techniques on the aircard's forced signal transmissions sent in response to interrogation using the StingRay and KingFish;</td>
<td>1. Section V(E)(1)(m) 2. Section V(E)(1)(o)</td>
</tr>
<tr>
<td>7</td>
<td>Aircard Internet access service;</td>
<td>(1) denying the defendant access to the Internet for ten hours using the StingRay and KingFish;</td>
<td>1. Section V(E)(1)(p)</td>
</tr>
</tbody>
</table>
Electricity provided to aircard and laptop (i.e., apartment No. 1122 electricity); (1) using the defendant's electricity provided to his aircard and forcing the aircard to transmit at the highest possible power; 1. Section V(E)(1)(q)

Real-time aircard geolocation information while aircard was inside Apartment No. 1122; (1) Verizon Wireless obtaining and providing the FBI real-time geolocation information relating to the location of the aircard while inside apartment No. 1122; 1. Section V(E)(1)(g)

The places, items, etc. searched by the government (via its agent, Verizon Wireless) while executing the N.D.Cal. 08-90330MISC-RS order are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Searched place, item, etc.:</th>
<th>Explanation of relevant searches conducted by Verizon Wireless as an agent for government:</th>
<th>Sections addressing searches:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A private residence (i.e., Apartment No. 1122);</td>
<td>(1) Verizon Wireless obtaining and providing the FBI real-time geolocation information relating to the location of the aircard while inside apartment No. 1122;</td>
<td>1. Section V(E)(1)(g)</td>
</tr>
<tr>
<td>2</td>
<td>Aircard (i.e., UTStarcom PC5740 broadband access card);</td>
<td>(1) Verizon Wireless obtaining and providing the FBI real-time geolocation information relating to the location of the aircard while inside apartment No. 1122;</td>
<td>1. Section V(E)(1)(g)</td>
</tr>
<tr>
<td>3</td>
<td>Host laptop computer (i.e., Lenovo IBM ThinkPad S/N #LV-C4398);</td>
<td>(1) Verizon Wireless obtaining and providing the FBI real-time geolocation information relating to the location of the aircard while inside apartment No. 1122;</td>
<td>1. Section V(E)(1)(g)</td>
</tr>
</tbody>
</table>

The effects, information, etc. seized by the government (via its agent, Verizon Wireless) while executing the N.D.Cal. 08-90330MISC-RS order are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Seized effect, information, etc.:</th>
<th>Explanation of relevant seizures conducted by Verizon Wireless as an agent for government:</th>
<th>Sections addressing seizures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Aircard (i.e., UTStarcom PC5740 broadband access)</td>
<td>(1) Verizon Wireless writing data to the aircard via OTAPA; (2) Verizon Wireless reprogramming the aircard via OTAPA or</td>
<td>1. Section V(E)(1)(d) 2. Section V(E)(1)(e)</td>
</tr>
</tbody>
</table>

1386. “A wrongful search or seizure by a private party does not violate the fourth amendment. However, where a private party acts as an instrument or agent of the state in effecting a search or seizure, fourth amendment interests are implicated” United States v. Walther, 652 F.2d 788, 791 (9th Cir. 1981) (internal citations and quotation marks omitted). Through the N.D.Cal. 08-90330MISC-RS order, the government was “exercis[ing] such coercive power” over Verizon Wireless “that it is responsible for the specific private conduct” carried out by Verizon Wireless employees. Fidelity Financial Corp. v. Fed. Home Loan Bank, 792 F.2d 1432, 1435 (9th Cir. 1986).
a. The FBI's searches and seizures conducted during execution of the N.D.Cal. 08-90330MISC-RS order exceeded the scope of the issued order.

The searches and seizures conducted by the FBI technical agents were outside the scope of the N.D.Cal. 08-90330MISC-RS order and were therefore in violation of the defendant's Fourth Amendment rights. Specifically, the FBI technical agents violated the particularity clause of the Fourth Amendment through various scope violations.  

"Whether a search exceeds the scope of a search warrant is an issue we determine through an objective assessment of the circumstances surrounding the issuance of the warrant, the contents of the search warrant, and the circumstances of the search." Hurd, 499 F.3d at 966

1387. Although scope violations and particularity violations are technically different, both are premised upon the particularity clause of the Fourth Amendment. See U.S. Const. Amend. IV (All warrants must “particularly describe[e] the place to be searched, and the... things to be seized.”). Particularity violations occur when a place or item to be searched or seized is not described in the relevant warrant with specificity. See United States v. Brobst, 558 F.3d 982, 993 (9th Cir. 2009) (“Particularity is the requirement that the warrant must clearly state what is sought.”). Scope violations occur when a place or item that was searched or seized is not at all listed in the warrant used to justify the search and/or seizure. See United States v. Hurd, 499 F.3d 963, 966 (9th Cir. 2007) (“[P]olice go beyond the scope of an authorized search warrant by searching places or seizing evidence not included in the warrant.”). A particularity violation, being applicable only to the text of the warrant itself, does not require an analysis of what was searched and/or seized. See United States v. Hotal, 143 F.3d 1223, 1227 (9th Cir. 1998) (“If a warrant fails for lack of particularity or specificity, it is simply unconstitutional – without regard to what actually occurred.”). In contrast, a scope violation requires an analysis of what was searched and/or seized so that it may be determined if the relevant warrant at all lists the place(s) searched and/or item(s) seized.
Applying the first part of the Hitchcock test, the government failed to seek a warrant to locate the aircard\[1388\] and instead submitted an application for a court order that did not seek authorization to conduct the searches and seizures occurring during the order's execution.\[1389][1390\] The government failed to seek proper judicial authorization even while FBI agents have been using wireless device locators since the early 1990s\[1391\] and are fully aware of the searches and seizures involved in their use. Applying the second part of the Hitchcock test, the order itself does not list the aircard, host laptop computer, or private residences as places to be searched.\[1392][1393\] For the items to be seized, the order does not list (1) the aircard, (2) the host laptop computer, (3) data stored on the aircard,\[1394\]

1388. See Argument, Section V(F)(1)(f), supra (explaining how none of the actions authorized by the N.D.Cal. 08-90330MISC-RS order were supported by an applicable finding of probable cause); id., Section V(F)(1)(h)(i), supra (explaining how the N.D.Cal. 08-90330MISC-RS order is not a warrant).

1389. Compare Argument, Section V(F)(1), supra (listing searches and seizures conducted by the government) with Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (application) (Dkt. #470-1) (application fails to seek authority to conduct the listed searches and seizures).

1390. “When an officer with probable cause to seize an item fails to mention that item in his application for a search warrant—for whatever reason—and seizes the item anyway, his conduct is per se unreasonable.” Horton v. California, 496 U.S. 128, 146 (1990).

1391. See Technical Explanations, Section II(G)(1), supra (noting how similar equipment was used to catch Kevin Mitnick and how a single FBI agent has used such equipment over 300 times during his career).

1392. See Procedural History, Section III(E), supra (explaining procedural aspects of the N.D.Cal. 08-90330MISC-RS order).

1393. The N.D.Cal. 08-90330MISC-RS order authorized Verizon Wireless—based on a less-than-probable-cause finding—to monitor aircard transmissions “while the agents are stationed in a public location and the [] [] aircard is [] inside private residences[,]” however, the order did not authorize either Verizon Wireless or the government to search private residences using location finding interrogation signals, triangulation techniques, or any other means. See Procedural History, Section III(E), supra. Although it would have been impossible to list the precise address of apartment No. 1122, the order still could have listed “private residences” as places to be searched.

1394. See United States v. James, No. 1:06 CR 134 CDP DDN, 2008 U.S. Dist. LEXIS
signal transmissions emanating from the aircard, (5) the location of the aircard while inside a private residence, (6) the aircard Internet access service, or (7) the electricity being provided to the aircard and host laptop computer. In fact, the operative section of the order fails to command or authorize the government to do anything—whether a search, seizure, or otherwise—and all authorized actions are solely applicable to Verizon Wireless.

Furthermore, the issuing magistrate made no findings of probable cause to search or seize anything. Applying the third and final part of the Hitchcock test, the circumstances surrounding the execution of the various searches and seizures also point towards a scope violation. While conducting the various unauthorized searches and seizures, the FBI technical agents (1) failed to keep records of what was seized, (2) made no return to the issuing magistrate, (3) did not serve the defendant with a copy of the order or a receipt of what was seized, and (4) destroyed the seized evidence once the defendant was arrested. The circumstances surrounding the issuance of the order, the contents of the

29840 (E.D.Missouri, Mar. 4, 2008) (“The retrieval of electronic data from cell phones is subject to the warrant requirement of the Fourth Amendment.”); United States v. Morales-Ortiz, 376 F.Supp.2d 1131, 1139 (D.NM. 2004) (“[O]fficers must obtain a warrant to search the memory of such devices, unless a recognized exception to the warrant requirement exists.”) (citations omitted)).

1395. See Procedural History, Section III(E), supra (explaining procedural aspects of the N.D.Cal. 08-90330MISC-RS order).

1396. The only actions authorized by the operative section of the N.D.Cal. 08-90330MISC-RS order apply solely to Verizon Wireless, i.e., to provide the government with all data, information, facilities, and technical assistance needed to locate the aircard. See id. The only mention of the government in the operative section relates to Verizon Wireless providing “to agents of the FBI data and information obtained from the monitoring of transmissions related to the location of the [aircard]... while the agents are stationed in a public location...” Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (order, p. 2-3) (Dkt. #470-1).

1397. See Argument, Section V(F)(1)(f), supra (explaining how all authorized actions, which were directed solely at Verizon Wireless, were supported by a finding of “specific and articulable facts”).

1398. See Procedural History, Section III(E), supra (explaining procedural aspects of the N.D.Cal. 08-90330MISC-RS order).

1399. See id.

1400. See General Facts, Section IV(B)(18), supra.

1401. See id., supra.
order, and the circumstances surrounding the execution of the order all support a finding that the relevant searches and seizures were conducted outside the scope of the issued order.

b. The N.D.Cal. 08-90330MISC-RS order does not authorize the installation, use, or monitoring of a “mobile tracking device”—whatever that device may be.

The government cannot even arguably justify its searches and seizures by relying upon the “mobile tracking device” wording of the N.D.Cal. 08-90330MISC-RS order because the issuing magistrate never authorized use of a “mobile tracking device”—whatever that device may be.[1402] The operative section of the order merely commands that “Verizon Wireless... provide to agents of the FBI data and information obtained from the monitoring of transmissions related to the location of the [[aircard]],”[1403] and that “Verizon Wireless... provide said agents immediately on request with all information, facilities, and technical assistance needed to ascertain the physical location of the [[aircard]].”[1404] The only mention of “mobile tracking device” is in a separate findings sections of the order which is insufficient to authorize the FBI's use of any type of equipment or to conduct any type of action that may be categorized as a “mobile tracking device.”

The N.D.Cal 08-90330MISC-RS order suffers the same fatal flaw suffered by the warrant discussed in United States v. Robinson, 358 F.Supp.2d 975 (D.Mont. 2005). In Robinson, law enforcement relied upon a warrant to search a residence while “the operative portion of the warrant, that which commands the search, d[id] not include a reference to the residence...” Id. at 977. The Robinson court found that a warrant is invalid if it “omits the residence from the command section[]” even if the warrant contains “an explicit finding of probable cause to search the residence.” Id. at 979.[1405] Although the Robinson court

1402. As explained in Argument, Section V(F)(1)(d), infra, the N.D.Cal. 08-90330MISC-RS order fails for particularity because the broad “mobile tracking device” term contained in the N.D.Cal. 08-90330MISC-RS order is neither defined nor explained.

1403. Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (order, p. 2) (Dkt. #470-1).

1404. Id. (order, p. 3) (Dkt. #470-1).

1405. The Robinson Court rejected the government's “cut and paste” error argument and found that “[t]he Fourth Amendment's warrant requirement has no exception for a mistake in cutting and pasting, nor does it authorize a reviewing court to divine what seems obvious but
addressed a search of a residence—as apposed to installation, use, and monitoring of a
“mobile tracking device”—it's reasoning is still applicable to the present case. Courts that
issue proper warrants for “mobile tracking devices” take care to command that the
government execute the warrant and begin using the device. For example, In The Matter Of
An Application For An Order Authorizing The Installation, Use, Monitoring, Repair,
Replacement And Removal Of A Tracking Device, Judge Carter issued a warrant
commanding agents to “execute th[e] warrant and begin using the object or installing the
tracking device...” See id., 11-MC-031-ALC, Doc. #001-2, p. 1 [Tracking Warrant]
(E.D.N.Y. 2011).1406 In the present case, even if the the FBI technical agents used a
“mobile tracking device,” their actions are not even arguably authorized by the N.D.Cal. 08-
90330MISC-RS order because it neither commanded nor authorized the installation, use, or
monitoring of such a device.

c. Even if a “mobile tracking device” was authorized by the
N.D.Cal. 08-90330MISC-RS order, the aircard locating
mission did not involve use of one.

Even if the Court is convinced that the N.D.Cal. 08-90330MISC-RS order authorized
the FBI to install, use, and monitor a “mobile tracking device,” the government cannot even
arguably rely on the order because the aircard locating mission did not involve a mobile
tracking device. The prosecution submitted a declaration by FBI Agent Morrison claiming
that “FBI technical personnel used equipment to locate an aircard believed to be used by the
defendant in this matter, and that equipment falls within the statutory definition of a pen
register/trap and trace device”—i.e., not a mobile tracking device. Although the
defendant asserts that the wireless device locators used to locate the aircard are something
other than Pen/Trap devices, both parties are still in agreement that the devices are absolutely

is clearly outside the scope of the application and warrant authorizing the search.” Id. at 976.
1406. See also EXHIBIT 115 of 2nd Consolidated Exhibits (Dkt. #821-6) (copies of Doc.
#005, p. 1-4 (Tracking Warrant and Return) and Doc. #001, p. 22-25 (Tracking Order) in 11-
MC-031-ALC (E.D.N.Y. 2011)).
1407. Government's Memorandum Re Motion For Discovery, “Affidavit Of Supervisory
Special Agent Bradley S. Morrison,” ¶ 2, p. 1 (Dkt. #674-1, p. 1).
Additionally, the defendant has submitted extensive evidence distinguishing mobile tracking devices from the wireless device locators used by the FBI technical agents to locate the aircard.

d. In any event, the “mobile tracking device” term contained in the N.D.Cal. 08-90330MISC-RS order fails for lack of particularity.

Without regard to what actually occurred, Hotal, 143 F.3d at 1227, the “mobile tracking device” term used in the N.D.Cal. 08-90330MISC-RS order fails for lack of particularity. Because the order lacks particularity, the searches and seizures conducted by the FBI technical agents were done in violation of the defendant's Fourth Amendment rights.

The order does not define or even remotely explain what “mobile tracking device” is intended to mean. The order only references 18 U.S.C. § 3117, which defines “tracking device” as “an electronic or mechanical device which permits the tracking of the movement of a person or object.” 18 U.S.C. § 3117(b). This definition has been described as “striking for its breadth.” Smith (mj) 2005 Opinion, 396 F.Supp.2d at 753. Such a broad term cannot provide authority to use a cell site emulator—let alone the authority needed to conduct a search and seizure. The Ninth Circuit, as well as all other courts, have repeatedly noted that the description in a warrant “must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized.” United States v. Mann, 389 F.3d 869, 877 (9th Cir. 2004). The only expansion of the “tracking device” term contained in

1408. The Court has repeatedly referred to the wireless device locators used to locate the aircard as “mobile tracking devices.” See, e.g., January 4, 2012 Court Order (Dkt. #723). The defendant insists that the Court correct its error considering (1) both parties are in agreement that the wireless device locators used to locate the aircard are not “mobile tracking devices,” and (2) evidence cited in this memorandum distinguishes mobile tracking devices from the actual equipment used to locate the aircard.

1409. Incidentally, the prosecution also agreed to not rely upon the N.D.Cal. 08-90331MISC-RS order (authorizing use of a Pen/Trap device) to justify the FBI locating the aircard using what FBI Agent Morrison labeled as a “pen register/trap and trace device.” See Government’s Memorandum RE Motion For Discovery (Dkt. #674, p. 2) (“[T]he United States agrees to rely solely on the Rule 41 tracking warrant, application, and affidavit, No. CR08-90330-MISC, to authorize the use of equipment to communicate directly with Defendant’s aircard and determine its location.” (footnote omitted)).

1410. Compare Technical Explanations, Section II(F), supra (explaining mobile tracking devices) with Technical Explanations, Section II(G)(1), supra (explaining wireless device locators).
the N.D.Cal. 08-90330MISC-RS order was done by placing the word “mobile” immediately before “tracking” to make “mobile tracking device.”[1411] In the *Technical Explanations*, Section II(F), *supra*, it was explained how mobile tracking devices are GPS devices attached to a package or vehicle sought to be tracked. A search on the web also reveals that “mobile tracking device” products are of a type explained in the *Technical Explanations*.¹⁴¹² Even the government’s own *Electronic Surveillance Manual* has “mobile tracking devices” listed in a section completely separate from the cell site emulator capable wireless device locators used to locate the aircard.[¹⁴¹³] If the addition of the word “mobile” particularizes “tracking device” in any way then it only does so to mean GPS mobile tracking devices as the term is generally understood by society.

Additionally, in various past investigations, searches and seizures of a type similar to those used to locate the aircard were conducted only after the government obtained judicial authorization particularly describing the place or item to be searched and things or information to be seized. For example, in *United States v. Ahrndt*, the government obtained a probable cause warrant to search “[a] signal emanating from a wireless device, such as a wireless router[,]... emanating in the general vicinity of Southwest 184ᵗʰ Avenue and Southwest 183ʳᵈ Terrace in Aloha, Oregon...”¹⁴¹⁴ and to seize “[t]he router and connected computer Internet protocol (IP) address broadcasting the SSID ‘BELKIN54G’...”¹⁴¹⁵

---

¹⁴¹¹. See Procedural History, Section III(E), *supra* (discussing procedural aspects of N.D.Cal. 08-90330MISC-RS order).

¹⁴¹². See EXHIBIT 036 of 2ᵈ Consolidated Exhibits (Dkt. #821-2) (collection of various web pages from http://www.alibaba.com advertising GPS based mobile tracking devices).

¹⁴¹³. See U.S. Dep’t of Justice, *Electronic Surveillance Manual*, p. iii (having Section XVI titled “MOBILE TRACKING DEVICES” and Section XIV titled “CELL SITE SIMULATORS/DIGITAL ANALYZERS/TRIGGERFISH”). See also EXHIBIT 052 of 2ᵈ Consolidated Exhibits (Dkt. #821-3) (section on cell site emulators, etc., p. 40-41 and 44-45); EXHIBIT 053 of 2ᵈ Consolidated Exhibits (Dkt. #821-3) (section on mobile tracking devices, etc., p. 48).


¹⁴¹⁵. See id., p. 2; see also EXHIBIT 114 of 2ᵈ Consolidated Exhibits (Dkt. #821-6) (relevant sections of Doc. #025 attached).
Similarly, In The Matter Of An Application Of The United States Of America For An Order Authorizing The Disclosure Of Latitude And Longitude Data..., the government obtained an order to seize “specific latitude and longitude of [] the SUBJECT TELEPHONES...”[1416] by having Sprint/Nextel “initiate a signal to determine the location of the subject's mobile device on Sprint/Nextel's network...”[1417] In addition to the “initiate a signal” order, the government also obtained a companion probable cause warrant to remotely search the premises of “A WIRELESS TELEPHONE ISSUED BY SPRINT-NEXTEL WITH IMSI...”[1418] for the purpose of remotely seizing “a telephone issued by Sprint-Nextel with IMSI...”[1419] In the above cases, rather than issue orders merely stating “use and monitor a mobile tracking device,” the magistrates issued documents particularly describing the place or item to be searched and the thing or information to be seized. Likewise, the searches and seizures authorized by the above cited documents were all supported by findings of probable cause specific to the planned government actions. When examined in light of the above quoted warrants and order, the N.D.Cal. 08-90330MISC-RS order suffers a fatal particularity flaw with its broad “use and monitor a mobile tracking device” wording.

e. Even if the N.D.Cal. 08-90330MISC-RS order authorized a place to be searched, the description of the place fails for lack of particularity.

In Section V(F)(1)(a), supra, the defendant explained how “private residences” is not listed in the N.D.Cal. 08-90330MISC-RS order as a place to be searched, which resulted in a scope violation. The order merely states that Verizon Wireless “shall provide to agents of the FBI data and information obtained from the monitoring of transmissions related to the location of the [][aircard]... including the monitoring of the [][aircard] while... the [][aircard] is (a) inside private residences, garages and/or other locations not open to the public or visual

1416. Id., 11-MC-00393-SMG, order, p. 2 (E.D.N.Y. 2010) (Doc #001, p. 17); see also EXHIBIT 112 of 2nd Consolidated Exhibits (Dkt. #821-6) (relevant sections of Doc. #001 attached).

1417. Id., order, p. 3 (Doc #001, p. 18) (emphasis added); see also EXHIBIT 112 of 2nd Consolidated Exhibits (Dkt. #821-6) (relevant sections of Doc. #001 attached).

1418. Id., warrant (Doc #001, p. 20); see also EXHIBIT 112 of 2nd Consolidated Exhibits (Dkt. #821-6) (relevant sections of Doc. #001 attached).

1419. Id.
surveillance; and (b) anywhere else the [aircard] may be present within the United
States...”[1420] If the Court rejects the defendant's scope violation argument and is convinced
that the above quoted wording authorizes an actual search of private residences (via
transmitted interrogation signals and triangulation)[1421] then, as further explained below, the
description of the “place” to be searched fails for lack of particularity. Because the order
lacks particularity, the searches and seizures conducted by the FBI technical agents were
done in violation of the defendant's Fourth Amendment rights.

A warrant will fail if “the government was able to describe the items more particularly
in light of the information available to it at the time the warrant was issued.” Millender v.
County of Los Angeles, 620 F.3d 1016, 1024 (9th Cir. 2009) (citation omitted). Although the
Millender reasoning was provided in the context of the things to be seized, it applies equally
well to the place to be searched. At the time the N.D.Cal. 08-90330MISC-RS order issued,
the government knew that the aircard was in a stationary location[1422] within the
geographical area covered by the overlapping cell site sectors shown on the cell tower range
chart/map.[1423] The government could have very easily particularized the place to be
searched as being within Santa Clara, CA where the South-East sector of Verizon Wireless
cell site No. 139 overlaps the South-West sector of Verizon Wireless cell site No. 268.
Because the government failed to further particularize the relevant place, the N.D.Cal. 08-
90330MISC-RS order fails for lack of particularity.

1420. Submission Of Materials Related To Applications And Court Orders Numbered 08-
90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District
Of California, On July 11, 2008 (order, p. 2) (Dkt. #470-1).
1421. See General Facts, Section IV(B)(9)(e) and (g), supra.
1422. See id., Section IV(B)(2), supra.
1423. See id.; see also EXHIBIT 21 of 1st Consolidated Exhibits (Dkt. #587-2) (cell tower
range chart/map showing a 6,412,224 ft² triangulated location signature estimate (marked
with black pen lines) covering the location of apartment No. 1122); EXHIBIT 22 of 1st
Consolidated Exhibits (Dkt. #587-2) (cell tower range chart/map with government's
6,412,224 ft² triangulated location signature estimate marked in red and apartment No. 1122
marked with a yellow star).
f. None of the actions authorized by the N.D.Cal. 08-90330MISC-RS order were supported by an applicable finding of probable cause.

Because all of the actions authorized by the N.D.Cal. 08-90330MISC-RS order were based on a finding of “specific and articulable facts,” the operative section of the order lacks supportive probable cause findings. Considering the Fourth Amendment requires “probable cause,” U.S. Const. Amend. IV, and not the lesser standard of “specific and articulable facts,” any search and/or seizure conducted by Verizon Wireless (an agent for the government) was done in violation of the defendant's Fourth Amendment rights. The only actions authorized by the N.D.Cal. 08-90330MISC-RS order applied to Verizon Wireless, i.e., to provide the government with all data, information, facilities, and technical assistance needed to locate the aircard.\[1424\] Prior to the operative section of the order, the issuing magistrate makes two separate findings: (1) “there is probable cause to believe that the use and monitoring of a mobile tracking device for the [][aircard], will lead to evidence of violations of [the alleged offenses],”\[1425\] and (2) “specific and articulable facts establish that there are reasonable grounds to believe that the requested information pertaining to the location of the [][aircard] is relevant and material to an ongoing criminal investigation.”\[1426\] Considering Verizon Wireless was required to “provide said agents immediately on request with all information, facilities, and technical assistance needed to ascertain the physical location of the [][aircard],”\[1427\] it is clear that only the “specific and articulable facts” finding applied to that authorization. The separate probable cause finding applied to the use and monitoring of a “mobile tracking device,”\[1428\] which is apart from the section of the order directed at

---

\[1424\] See Procedural History, Section III(E), supra (discussing procedural aspects of N.D.Cal. 08-90330MISC-RS order).

\[1425\] Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (order, p. 2) (Dkt. #470-1).

\[1426\] Id. (order (emphasis added)) (Dkt. #470-1).

\[1427\] Id. (order, p. 3 (emphasis added)) (Dkt. #470-1).

\[1428\] As previously explained, the N.D.Cal. 08-90330MISC-RS order fails to authorize or command either the government or Verizon Wireless to use a “mobile tracking device,” see Argument, Section V(F)(1)(b), supra, and, in any event, the order fails to particularize the term “mobile tracking device,” see id., Section V(F)(1)(d), supra.
Verizon Wireless.

The above interpretation of the order follows common sense and also acts to give meaning to both of the magistrate's findings. See United States v. Cannon, 264 F.3d 875, 880 (9th Cir. 2001) (“A search warrant must be read in a common sense and realistic fashion.”); Cree v. Waterbury, 78 F.3d 1400, 1405 (9th Cir. 1996) (Explaining “the rule of contract construction that a court must give effect to every word or term employed by the parties and reject none as meaningless or surplusage in arriving at the intention of the contracting parties.” (internal citation and quotation marks omitted)). The magistrate’s “specific and articulable facts” finding contained in the N.D.Cal. 08-90330MISC-RS order was perceivably made pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act (SCA). Considering probable cause trumps the SCA’s “specific and articulable facts” standard, the issuing magistrate would have no reason to include that less-than-probable-cause finding unless he intended some actions to be supported by only “specific and articulable facts.” A different interpretation would act to read out the “specific and articulable facts” finding contained in the order.

g. The “all data, information, facilities, and technical assistance” term contained in the N.D.Cal. 08-90330MISC-RS order fails for lack of particularity.

Because the operative section of the N.D.Cal. 08-90330MISC-RS order lacks particularity, it is insufficient to justify Verizon Wireless' involvement in the aircard locating mission. The operative section of the N.D.Cal. 08-90330MISC-RS order commands that “Verizon Wireless... provide to agents of the FBI data and information obtained from the monitoring of transmissions related to the location of the [aircard],” and that “Verizon Wireless...
Wireless... provide said agents immediately on request with all information, facilities, and technical assistance needed to ascertain the physical location of the [aircard].” The term “data and information” encompasses numerous categories of data that may be collected from the “monitoring of transmissions” relating to location. Such a broad term in no way meets the particularity requirement of the Fourth Amendment. See, e.g., United States v. Feldman, 366 F. Supp. 356, 363 (D.Haw. 1973) (“The term 'documents and instrumentalities relating to the shipment and ownership of the marihuana' is too broad to particularly describe the things to be seized.”). Likewise, the term “all facilities, and technical assistance” also lacks particularity because it encompasses any number of Verizon Wireless activities the FBI could have exploit to locate the aircard. For example, the FBI could have relied upon the order to (1) assemble an army of Bay Area Verizon Wireless Store retail clerks, (2) force the clerks to accompany them to the Domicilio apartment complex, (3) arm each of the clerks with a KingFish, and (4) demand that the clerks assist them by kicking down the doors of Domicilio residents in order to enter homes and search for the aircard. Although the government probably exercised discretion and did not do this, “the Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised.” United States v. United States District Court, 407 U.S. 297, 317 (1972) (footnote omitted). Additionally, it is the view of the Ninth Circuit that “[i]f a warrant fails for lack of particularity or specificity, it is simply unconstitutional – without regard to what actually occurred.” Hotal, 143 F.3d at 1227.

Of California, On July 11, 2008 (order, p. 2) (Dkt. #470-1).

1432. Id. (order, p. 3) (Dkt. #470-1).

1433. The defendant has no way of knowing all of the ways Verizon Wireless assisted the FBI technical agents in locating the aircard because all discoverable evidence is being withheld by the government based on a claim of privilege. See January 4, 2012 Court Order (Dkt. #723).

1434. See also Hotal, 143 F.3d at 1223 (“Particularized descriptions serve the purpose of, first, ensuring that the discretion of the officer's executing the warrant is limited[.]” (internal quotation marks and citation omitted)).
h. The N.D.Cal. 08-90330MISC-RS order fails for facial unreasonableness.

   i. The N.D.Cal. 08-90330MISC-RS order is *facially* unreasonable because it is not a warrant.

   The N.D.Cal. 08-90330MISC-RS order is facially unreasonable under the Fourth Amendment because it is not a warrant by judicial process nor was it accompanied by an actual warrant. *See United States v. Mejia*, 69 F.3d 309, 320 (9th Cir. 1995) (“We are neither free nor willing to read the warrant requirement out of the Constitution.”); *see also* *Schnecklah v. Bustamonte*, 412 U.S. 218, 219 (1973) (A warrantless search is “*per se* unreasonable... subject only to a few specifically established and well-delineated exceptions.” (internal quotation marks and citations omitted)). In contrast to the N.D.Cal. 08-90330MISC-RS order, the mobile tracking device authority approved in 11-MC-031-ALC (E.D.N.Y. 2011) came with an actual warrant according to standard judicial process as enumerated in Rule 41, Fed. R. Crim. P.[1435]

   ii. The N.D.Cal. 08-90330MISC-RS order is *facially* unreasonable because it expressly omits compliance with Rule 41 inventory and return requirements.


---

1435. *See also EXHIBIT 115 of 2nd Consolidated Exhibits* (Dkt. #821-6) (copies of Doc. #005, p. 1-4 (Tracking Warrant and Return) and Doc. #001, p. 22-25 (Tracking Order) in 11-MC-031-ALC (E.D.N.Y. 2011)).

1436. *Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008* (order, p. 3) (Dkt. #470-1).
warrants,[1437] “within 10 calendar days after the use of the tracking device has ended, the
officer executing the warrant must return it to the judge designated in the warrant.” Fed. R.
Crim. P. 41(f)(2)(B) (2008) (tracking-device warrant). For both a conventional warrant and
tracking-device warrant, the warrant “must... designate the magistrate judge to whom it must
be returned,... [and] [t]he warrant must command the officer to: [...] return the warrant to the
judge designated in the warrant.” Fed. R. Crim. P. 41(e)(2)(B) and (iii) (2008) (tracking-
device warrant); Fed. R. Crim. P. 41(e)(2)(A) and (iii) (2008) (conventional warrant). There
is no justification contained in the order as to why Rule 41 return and inventory requirements
were to be ignored.

iii. The N.D.Cal. 08-90330MISC-RS order is facially unreasonable because it expressly omits compliance with Rule 41 receipt and service requirements.

The N.D.Cal. 08-90330MISC-RS order is facially unreasonable under the Fourth
Amendment because it states that agents are “not required to serve a copy of this Order on
any owner of the [][aircard]...”[1438] Whether a tracking-device warrant or conventional
warrant, federal rules require that law enforcement serve a copy of the warrant on the
individual of whom the warrant pertains:

Service. Within 10 days after the use of the tracking device has ended, the
officer executing a tracking-device warrant must serve a copy of the warrant on
the person who was tracked or whose property was tracked. Service may be
accomplished by delivering a copy to the person who, or whose property, was
tracked; or by leaving a copy at the person's residence or usual place of abode
with an individual of suitable age and discretion who resides at that location
and by mailing a copy to the person's last known address. Upon request of the
government, the judge may delay notice as provided in Rule 41(f)(3).


Receipt. The officer executing the warrant must give a copy of the warrant and
a receipt for the property taken to the person from whom, or from whose
premises, the property was taken or leave a copy of the warrant and receipt at
the place where the officer took the property.

1437. The defendant does not suggest that the FBI's actions involved used of a “tracking
device” or “mobile tracking device,” however, the government still violated Rule 41
inventory and return requirements from all possible angles.
1438. Submission Of Materials Related To Applications And Court Orders Numbered 08-
90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District
Of California, On July 11, 2008 (order, p. 3) (Dkt. #470-1).

There is no justification contained in the order as to why Rule 41 receipt and service requirements were not to be followed. Likewise, there is no authorization for delayed service pursuant to Rule 41(f)(3), let alone no service at all. See United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986) (Freitas I) (Finding that a “warrant was constitutionally defective in failing to provide for notice within a reasonable, but short, time subsequent to the [[search]].”).

iv. The N.D.Cal. 08-90330MISC-RS order is *facially* unreasonable because it commanded destruction of evidence obtained via the order.

The N.D.Cal. 08-90330MISC-RS order is facially unreasonable under the Fourth Amendment because it states that “at the conclusion of the tracking mission, the investigating agency shall expunge all of the data obtained by this Court Order[.]”[1439] The “destroy the evidence” provision of the order deliberately disregards rules announced and reiterated in numerous longstanding cases such as *Brady*,[1440] *Gamez-Orduno*,[1441] and *Barton*. The Supreme Court decided *Brady* more than 45 years prior to the N.D.Cal. 08-90330MISC-RS order being issued. The Ninth Circuit decided *Gamez-Orduno* more than 7 years prior to the N.D.Cal. 08-90330MISC-RS order being issued and *Barton* more than 15 years prior. There is also no justification contained in the order as to why all evidence was to be destroyed.

---

1439. Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (order, p. 3) (Dkt. #470-1).

1440. See *Brady v. Maryland*, 373 U.S. 83, 87 (1963) (Withholding evidence “violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.”).

1441. See *United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) (“The suppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different.” (internal citations omitted)).

1442. See *United States v. Barton*, 995 F.3d 931, 935 (9th Cir. 1993) (After applying concepts from *Franks, Brady*, and *Youngblood*, the Ninth Circuit required that the government preserve evidence having the potential to impeach allegations in an affidavit for a search warrant.).
v. The N.D.Cal. 08-90330MISC-RS order is **facially unreasonable** because it authorized the government to serve redacted versions of the order.

The N.D.Cal. 08-90330MISC-RS order is facially unreasonable under the Fourth Amendment because it states that “copies of the Court's Order in... redacted form may be served on [[][law enforcement] and the service providers...”[1443] Allowing the government discretion to serve and execute redacted versions of a court order grants the executive branch a blank check to violate constitutional rights. *See Trupino v. United States*, 334 U.S. 699, 705 (1948) (Noting “the desirability of having magistrates rather than police officers determine when searches and seizures are permissible and what limitations should be placed upon such activities.”). Contrary to the reasoning noted in *Trupino*, the N.D.Cal. 08-90330MISC-RS order allowed the government free will to black out sections of the order meant to provide limitations upon the government's authority as originally contemplated by the issuing magistrate.

i. Additional reasons as to why the N.D.Cal. 08-90330MISC-RS order was **executed** in an unreasonable manner.

i. The N.D.Cal. 08-90330MISC-RS order was unreasonably executed because agents violated the limitation to “monitoring.”

The N.D.Cal 08-90330MISC-RS order was executed unreasonably under the Fourth Amendment because the government violated the order's limitation to only monitoring aircard transmissions. The order commanded Verizon Wireless to “provide to agents of the FBI data and information obtained from the **monitoring** of transmissions”[1444] relating to the aircard with nothing in the order authorizing obtaining data and information from the **sending** of transmissions to the aircard. In order to locate the aircard, the FBI technical agents used the StingRay and KingFish to transmit interrogation signals to the aircard while

---

1443. *Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008* (order, p. 3) (Dkt. #470-1).

1444. *Id.* (order, p. 2) (Dkt. #470-1).
it was located inside the defendant's home—a violation of the order's limitation to ‘monitoring.’ In addition to general unreasonableness, the violation of the order's limitation to monitoring was a but-for, unattenuated cause of obtaining geolocation data relating to the aircard. Had the FBI technical agents not been transmitting interrogation signals, they would have not been able to collect the aircard's location finding response signals used to triangulate the location of the aircard and the defendant inside apartment No. 1122.[1446]

ii. The N.D.Cal. 08-90330MISC-RS order was unreasonably executed because agents failed to comply with receipt and service requirements.

The N.D.Cal 08-90330MISC-RS order was executed unreasonably under the Fourth Amendment because agents did not serve the defendant with a copy of the order or with a receipt of what was seized after the order had been executed.[1447] Instead, the defendant had to wait nine months until the prosecution finally provided the defendant's attorney with a copy of the order.[1448] Additionally, the defendant is yet to be provided with a receipt listing what was seized and will likely never receive one because the FBI technical agents destroyed all evidence relating to the aircard locating mission.[1449] In addition to general unreasonableness, the notice/receipt violation was a but-for, unattenuated cause of obtaining later physical evidence and the arrest of the defendant. 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.[1450] In other

1445. See General Facts, Section IV(B)(9)(e), supra.
1446. See id., et seq., supra (explaining how interrogation was an integral part of the aircard locating mission).
1447. See Procedural History, Section III(F), supra, (discussing procedural aspects of the N.D.Cal. 08-90330MISC-RS order).
1448. See General Facts, Section IV(B)(18), supra.
1449. See id., Section IV(B)(15), supra.
1450. See defendant's declaration accompanying this memorandum RE: Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050, ¶ 14, p. 4.
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.

iii. The N.D.Cal. 08-90330MISC-RS order was
unreasonably executed because agents failed to comply
with inventory and return requirements.

The N.D.Cal 08-90330MISC-RS order was executed unreasonably under the Fourth
Amendment because agents neither created nor returned an inventory of seized evidence to
the issuing magistrate.[1451] In Berger, the Supreme Court noted that when an “officer [][is]
required to and did make a return on [][an] order showing how it was executed and what was
seized[]... the danger of an unlawful search and seizure [][is] minimized.” Berger v. New
York, 388 U.S. 41, 57 (1967). In addition to general unreasonableness, the inventory and
return violation was a but-for, unattenuated cause of obtaining geolocation data relating to
the aircard. Had the FBI technical agents made a return listing all of the items and
information seized, the issuing magistrate would have recognized that the government used
the order as a general warrant and the resulting evidence would have been immediately
suppressed. “A search warrant authorizing inspection will not be a general warrant if such
standards reasonably guide the officers in avoiding seizure of protected property, and if upon
return of the warrant the magistrate may review the search to determine whether the
instructions were followed and legitimate property and privacy interests were protected.”
United States v. Hillyard, 677 F.2d 1336, 1340 (9th Cir. 1986) (emphasis added).

iv. The N.D.Cal. 08-90330MISC-RS order was
unreasonably executed because agents destroyed all
evidence seized during execution of the order.

The N.D.Cal 08-90330MISC-RS order was executed unreasonably under the Fourth
Amendment because agents did not preserve the evidence seized during execution of the
order. Instead, FBI technical agents willingly destroyed or failed to preserve evidence in bad
faith. See accompanying Memorandum RE: Destruction Of Evidence (explaining the

[1451] See Procedural History, Section III(F), supra, (discussing procedural aspects of the
N.D.Cal. 08-90330MISC-RS order).
government's bad faith destruction of evidence). The government's destruction of evidence resulted in the defendant suffering prejudice under the Fourth Amendment considering he is now unable to determine (1) whether Verizon Wireless' actions in obtaining aircard geolocation data (see Argument, Section V(E)(1)(g), supra) was a trespass-to-obtain-information search via a photon based entry into the defendant's aircard, home computer, and residence, (2) whether Verizon Wireless obtained communications content along with geolocation data for the aircard, and (3) whether Verizon Wireless violated the limitation to monitoring contained in the N.D.Cal. 08-90330MISC-RS order (see Argument, Section V(F)(1)(i)(i), supra).

j. Neither the N.D.Cal. 08-90330MISC-RS order application nor supporting affidavit act to cure defects in the issued order.

The government is unable to meet the requirements to have the underlying N.D.Cal. 08-90330MISC-RS order application and affidavit act to cure defects in the issued order. “We consider an affidavit to be part of a warrant, and therefore potentially curative of any defects, only if (1) the warrant expressly incorporated the affidavit by reference and (2) the affidavit either is attached physically to the warrant or at least accompanies the warrant while agents execute the search.” United States v. SDI Future Health, Inc., 553 F.3d 1246, 1258 (9th Cir. 2009) (citation and internal quotation marks omitted).[1452] First, the N.D.Cal. 08-90330MISC-RS order does not contain suitable words of reference incorporating the underlying application and affidavit. Although the Ninth Circuit has “not defined precisely what verbiage is suitable for this purpose,” id. at 699-700 (citation omitted), in Towne, the Ninth Circuit held that the wording of, “See Attachment B,” created “no question that Attachment B was incorporated by reference in the search warrant.” United States v. Towne, 997 F.2d 537, 539 and 548-49 (9th Cir. 1993). In the present case, nowhere in the N.D.Cal. 08-90330MISC-RS order does the magistrate include any verbiage that resembles “See

1452. See also United States v. McGrew, 122 F.3d 847, 850 (9th Cir. 1997) (“If the 'incorporated' affidavit does not accompany the warrant, agents cannot claim good faith reliance on the affidavit's contents.”).
affidavit,” “See application,” or similar.[1453]

Second, even if the N.D.Cal. 08-90330MISC-RS order can somehow be construed to contain suitable words of reference, the government is yet to offer any evidence indicating that the undisclosed FBI technical agents, and/or Verizon Wireless, had the actual order with them while locating the aircard, let alone the application and affidavit. Because the prosecution refuses to identify and produce the FBI technical agents as witnesses,[1454] the government effectively concedes the issue addressed in this subsection.[1455] The application and affidavit were also sealed while the order was executed and this casts further doubt upon any claim that the documents accompanied the issued order. While the N.D.Cal. 08-90330MISC-RS order specifically permits agents to be served with copies of the sealed order, there is no authorization to serve agents with copies of the sealed application and affidavit.[1456] See Groh v. Ramirez, 540 U.S. 551, 558 (2004) (“But in this case the warrant

1453. There is no mention of either the application or affidavit using verbiage that amounts to an express incorporation into the N.D.Cal. 08-90330MISC-RS order. First, the application is mentioned in an introductory paragraph that merely reiterates AUSA Yen's request to have the order only authorize actions conducted by Verizon Wireless and not by the government. See Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (order, p. 1) (“This matter is before the Court pursuant to an Application... by Assistant United States Attorney Shawna Yen,... which Application requests an Order directing Verizon Wireless to assist agents... 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...”) (Dkt. #470-1). Second, the application and affidavit are mentioned in the operative section of the order requiring that both documents be sealed. See id., p. 3. Neither of the noted sections contain verbiage expressly incorporating either document into the underlying order in a curative fashion.

1454. See January 4, 2012 Court Order (Dkt. #723, p. 12) (The Court denied the defendant's motion for disclosure (Dkt. #592) and concluded that “[d]isclosures 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.”).

1455. There is also evidence that FBI agents typically do not keep on hand the order, let alone the application/affidavit, while conducting locating/tracking missions. For example, in one FBI email produced as a result of a FOIA request, an agent recounted his frustrations in dealing with a wireless carrier who told him the data he was after “was not specifically mentioned in the Court Order[].” The frustrated FBI agent then candidly noted that “it would have been helpful for me to have a copy of the order to refer to...” See FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 43 of 67 (emphasis added); see also EXHIBIT 038 of 2nd Consolidated Exhibits (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

1456. See Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (order, p. 3) (“The Court further ORDERS that the
did not incorporate other documents by reference, nor did either the affidavit or the application (which had been placed under seal) accompany the warrant. Hence, we need not further explore the matter of incorporation.” (emphasis added)). Finally, there is nothing even contained in the underlying documents that act to cure any of the violations being challenged by the defendant.

2. The N.D.Cal. 08-90331MISC-RS (Pen/Trap) order do not render any of the applicable searches and seizures reasonable.

The places, items, etc. searched by the government while executing the N.D.Cal. 08-90331MISC-RS order[1457] are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Searched place, item, etc.:</th>
<th>Explanation of relevant searches conducted by the government:</th>
<th>Sections addressing searches:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A private residence (i.e., Apartment No. 1122);</td>
<td>(1) forcing generation of real-time aircard cell site location information using surreptitious phone calls placed to the aircard (calls were never answered); (2) obtaining real-time aircard cell site location information from Verizon Wireless IAPs using the SF-Martinez DCS-3000 Pen/Trap device;</td>
<td>1. Section V(E)(1)(f) 2. Section V(E)(1)(f)</td>
</tr>
<tr>
<td>2</td>
<td>Aircard (i.e., UTStarcom PC5740 broadband access card);</td>
<td>(1) forcing generation of real-time aircard cell site location information using surreptitious phone calls placed to the aircard (calls were never answered);</td>
<td>1. Section V(E)(1)(f)</td>
</tr>
<tr>
<td>3</td>
<td>Host laptop computer (i.e., Lenovo IBM ThinkPad S/N #LV-C4398);</td>
<td>(1) forcing generation of real-time aircard cell site location information using surreptitious phone calls placed to the aircard (calls were never answered);</td>
<td>1. Section V(E)(1)(f)</td>
</tr>
</tbody>
</table>

The effects, information, etc. seized by the government while executing the N.D.Cal. 08-90331MISC-RS order are as follows:

government's Application, the attached Affidavit, and the Court's Order be filed under seal, except that copies of the Court's Order in full or redacted form may be served on [][law enforcement] and the service providers as necessary to effectuate the Court's Order.”) (Dkt. #470-1).

1457. The government previous indicated that “[t]he hybrid order, No. CR08-90331-MISC, will be used to justify obtaining cell site and other non-content information from Verizon Wireless.” Government's Memorandum RE Motion For Discovery (Dkt. #674, p. 2 fn. 2).
<table>
<thead>
<tr>
<th>#</th>
<th>Seized effect, information, etc.:</th>
<th>Explanation of relevant seizures (or preceding searches) conducted by the government:</th>
<th>Sections addressing seizures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Aircard (i.e., UTStarcom PC5740 broadband access card);</td>
<td>(1) denying the defendant access to the Internet for six hours (i.e., denial-of-service attack) using surreptitious phone calls;</td>
<td>1. Section V(E)(1)(h)</td>
</tr>
<tr>
<td>2</td>
<td>Host laptop computer (i.e., Lenovo IBM ThinkPad S/N #LV-C4398);</td>
<td>(1) denying the defendant access to the Internet for six hours (i.e., denial-of-service attack) using surreptitious phone calls;</td>
<td>1. Section V(E)(1)(h)</td>
</tr>
<tr>
<td>3</td>
<td>Real-time cell site location information relating to the aircard while inside private residences and <strong>not engaged in a call</strong>;</td>
<td>(1) obtaining real-time aircard cell site location information from Verizon Wireless IAPs using the SF-Martinez DCS-3000 Pen/Trap device;</td>
<td>1. Section V(E)(1)(f)</td>
</tr>
<tr>
<td>4</td>
<td>Location of the aircard and the defendant inside apartment No. 1122;</td>
<td>(1) obtaining real-time aircard cell site location information from Verizon Wireless IAPs using the SF-Martinez DCS-3000 Pen/Trap device;</td>
<td>1. Section V(E)(1)(f)</td>
</tr>
<tr>
<td>5</td>
<td>Aircard Internet access service;</td>
<td>(1) denying the defendant access to the Internet for six hours (i.e., denial-of-service attack) using surreptitious phone calls;</td>
<td>1. Section V(E)(1)(h)</td>
</tr>
</tbody>
</table>

The places, items, etc. searched by the government (via its agent, **Verizon Wireless**) while executing the N.D.Cal. 08-90331MISC-RS order are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Searched place, item, etc.:</th>
<th>Explanation of relevant searches conducted by Verizon Wireless as an agent for government:</th>
<th>Sections addressing searches:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A private residence (i.e., Apartment No. 1122);</td>
<td>(1) transmitting signals from a cell site to the aircard (in response to FBI's surreptitious phone calls) causing it to generate real-time cell site sector location information;</td>
<td>1. Section V(E)(1)(f)</td>
</tr>
<tr>
<td>2</td>
<td>Aircard (i.e., UTStarcom PC5740 broadband access card);</td>
<td>(1) transmitting signals from a cell site to the aircard (in response to FBI's surreptitious phone calls) causing it to generate real-time cell site sector location information;</td>
<td>1. Section V(E)(1)(f)</td>
</tr>
<tr>
<td>3</td>
<td>Host laptop computer (i.e., Lenovo IBM ThinkPad S/N #LV-C4398);</td>
<td>(1) transmitting signals from a cell site to the aircard (in response to FBI's surreptitious phone calls) causing it to generate real-time cell site sector location information;</td>
<td>1. Section V(E)(1)(f)</td>
</tr>
</tbody>
</table>

The effects, information, etc. seized by the government (via its agent, **Verizon**)
While executing the N.D. Cal. 08-90331MISC-RS order are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Seized effect, information, etc.:</th>
<th>Explanation of relevant seizures conducted by Verizon Wireless as an agent for government:</th>
<th>Sections addressing seizures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Real-time cell site location information relating to the aircard while inside private residences and <strong>not engaged in a call</strong>;</td>
<td>(1) logging and sending real-time aircard cell site location information from Verizon Wireless IAPs to the SF-Martinez DCS-3000 Pen/Trap device;</td>
<td>1. Section V(E)(1)(f)</td>
</tr>
<tr>
<td>2</td>
<td>Location of the aircard and the defendant inside apartment No. 1122;</td>
<td>(1) logging and sending real-time aircard cell site location information from Verizon Wireless IAPs to the SF-Martinez DCS-3000 Pen/Trap device;</td>
<td>1. Section V(E)(1)(f)</td>
</tr>
</tbody>
</table>

**a. The searches and seizures conducted during execution of the N.D. Cal. 08-90331MISC-RS order were not backed by anything resembling a probable cause warrant.**

Considering the N.D. Cal. 08-90331MISC-RS order was not issued based on a finding of probable cause, all relevant searches and seizures were conducted in violation of the defendant's Fourth Amendment rights. The government conceded that “the aircard tracking operation was a Fourth Amendment search and seizure.”[1458] The government's concession covers the actions taken by the FBI technical agents and Verizon Wireless while executing the N.D. Cal. 08-90331MISC-RS order. Additionally, the defendant identified and categorized the specific searches and seizures that occurred during execution of the order (see Argument, Section V(E)(1)(f) and (h), supra), which are summarized in the table immediately above (see Argument, Section V(F)(2), supra). Because, and as the government concedes, the relevant actions were Fourth Amendment searches and seizures, the N.D. Cal. 08-90331MISC-RS order **must** contain a probable cause finding in support of the various searches and seizures conducted in relation to the order. See, e.g., United States v. Winsor, 846 F.2d 1569, 1575 (9th Cir. 1987) (A search of a residence will never “constitute such a limited intrusion on Fourth Amendment interests that it may be justified by a degree of

---

1458. See Government's Memorandum Re Motion For Discovery (Dkt. #674, p. 1), (footnote omitted); see also January 4, 2012 Court Order (Dkt. #723, p. 14-15) (“[F]or purposes of Defendant’s motion to suppress, the government agrees that the Court may assume that the aircard tracking operation was a Fourth Amendment search and seizure.”).
suspicions less than probable cause.”); United States v. Reilly, 224 F.3d 986, 995 (9th Cir. 2000) ( Suppressing evidence and refusing “to excuse the failure to obtain a search warrant where the police had probable cause but simply did not attempt to obtain a warrant.”)

(quoted Mejia, 69 F.3d at 320)); Payton v. New York, 445 U.S. 573, 585 (1980) (“Unreasonable searches or seizures conducted without any warrant at all are condemned by the plain language of the first clause of the [Fourth] Amendment.”). The magistrate who issued the N.D.Cal. 08-90331MISC-RS order merely found that AUSA Yen “certified that the information likely to be obtained... is relevant to an ongoing criminal investigation” and that there are “specific and articulable facts showing that there are reasonable grounds to believe that... cell site information regarding the [aircard is]... relevant and material to an ongoing criminal investigation.”

Considering the Fourth Amendment requires “probable cause,” U.S. Const. Amend. IV, and not the lesser standard of “specific and articulable facts,” the government finds no support in the N.D.Cal. 08-90331MISC-RS order to justify its searches and seizures.

b. The FBI's searches and seizures conducted during execution of the N.D.Cal. 08-90331MISC-RS order exceeded the scope of the issued order.

All searches and seizures conducted under the N.D.Cal 08-90331MISC-RS order were in further violation of the defendant's Fourth Amendment rights based on scope violations. Specifically, the FBI technical agents and Verizon Wireless violated the particularity clause of the Fourth Amendment through various scope violations. As explained in Section V(F)(1)(a), supra, analyzing scope violations requires application of the Hitchcock test: “Whether a search exceeds the scope of a search warrant is an issue we determine through an objective assessment of the circumstances surrounding the issuance of the warrant, the contents of the search warrant, and the circumstances of the search.” Hurd, 499 F.3d at 966 (citation omitted). Below, the Hitchcock test is applied to the government's Fourth Amendment searches and seizures conducted during execution of the N.D.Cal 08-
Applying the first part of the *Hitchcock* test, the government failed to seek a warrant to locate the aircard and instead submitted an application for a court order that did not seek authorization to conduct the searches and seizures occurring during the order’s execution. The government failed to seek proper judicial authorization even while FBI agents have been using DCS-3000 Pen/Trap devices since the mid to late 1990s and are fully aware of the searches and seizures involved in their use to locate wireless devices.

Applying the second part of the *Hitchcock* test, the order itself does not list the aircard, host laptop computer, or private residences as places to be searched. For the items to be seized, the order does not list (1) the aircard, (2) the host laptop computer, (3) real-time cell site sector location information relating to the aircard while inside private residences and not engaged in a call, (4) the location of the aircard while inside a private residence, or (5) the aircard Internet access service. Although the operative section of the order does authorize obtaining some real-time cell site location information, it does not authorize obtaining “any cell site information that might be available when the [aircard] is turned ‘on’ but a call is not in progress[.]” With respect to seizing real-time cell site information,
the government cannot rely upon the order because the aircard is not a telephone and is simply **incapable** of placing or answering calls.\[1467\] As the prosecution agrees,\[1468\] the FBI's surreptitious phone calls placed to the aircard were never answered and therefore no call was ever “in progress” or “off the hook,” as required for the resulting cell site information to fall within the scope of the order. Applying the third and final part of the *Hitchcock* test, the circumstances surrounding the execution of the various searches and seizures also point towards a scope violation. While conducting the various unauthorized searches and seizures, the FBI technical agents made no return to the issuing magistrate\[1469\] and did not serve the defendant with a copy of the order or a receipt of what was seized.\[1470\]

The circumstances surrounding the issuance of the order, the contents of the order, and the circumstances surrounding the execution of the order all support a finding that the relevant searches and seizures were conducted outside the scope of the issued order.

c. **Additional reasons as to why the N.D.Cal. 08-90331MISC-RS order was executed in an unreasonable manner.**

i. The N.D.Cal. 08-90331MISC-RS order was unreasonably executed because agents violated the limitation to “recording.”

   The N.D.Cal 08-90331MISC-RS order was executed unreasonably under the Fourth Amendment because the government violated the order's limitation to only recording outgoing and incoming aircard transmissions. The order authorized the government to

---

1467. *See General Facts*, Section IV(A)(1), *supra* (explaining how the aircard hardware is incapable of ringing or alerting to an incoming call and how it does not allow for placing or receiving telephone calls); *id.*, Section IV(B)(6), *supra* (citing supporting evidence).

1468. *See EXHIBIT 069 of 2nd Consolidated Exhibits* (Dkt. #821-3) (June 7, 2011 letter from AUSA Battista to the defendant, p. 1: “The forwarded numbers arose after the operators of the equipment used to locate the aircard called a telephone number associated with the aircard…. Because the aircard device was not a conventional telephone, incoming calls to the device could not be connected to it as a normal call. The incoming calls in question were forwarded by the Verizon Wireless network to the various numbers which belong to, and are used by, Verizon Wireless for processing incoming calls that cannot be connected/terminated to the original called number - *i.e.*, the targeted number.” (emphasis added)).

1469. *See Procedural History*, Section III(F), *supra* (explaining procedural aspects of the N.D.Cal. 08-90331MISC-RS order).

1470. *See General Facts*, Section IV(B)(18), *supra*.
"install, or cause to be installed, and use a pen register to record or decode dialing, routing, addressing, or signaling information transmitted from the [aircard]" and to "install, or cause to be installed, and use a trap and trace device on the [aircard] to capture and record the incoming electronic or other impulses..."[1471] with no provisions authorizing the sending of transmissions to the aircard. During the aircard locating mission, the FBI technical agents forced the aircard to generate real-time cell site sector location information by transmitting signals to the aircard via surreptitious phone calls[1472]—a violation of the order's limitation to "recording." In addition to general unreasonableness, the violation of the order's limitation to recording was a but-for, unattenuated cause of obtaining geolocation data relating to the aircard. Had the FBI technical agents not been using surreptitious phone calls to transmit signals, they would not have been able to collect the aircard's real-time cell site sector location information to narrow the geographic area of where to search for the aircard and the defendant using the StingRay.[1473]

ii. The N.D.Cal. 08-90331MISC-RS order was unreasonably executed because agents violated the "after receipt and storage" provision of the order.

The N.D.Cal 08-90331MISC-RS order was executed unreasonably under the Fourth Amendment because the government violated the order's requirement that Verizon Wireless first record real-time cell site information prior to providing it to the FBI. Through the "after receipt and storage" provision, the order required that all cell site information be "first captured and recorded by the provider before being sent to the Investigative Agency."[1474] As explained in Section IV(B)(6), supra, the data indicating the cell site sector being accessed by the aircard in real-time was not recorded by Verizon Wireless, but simply

1471. See Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (order, p. 2-3) (Dkt. #470-2)

1472. See General Facts, Section IV(B)(6), supra.

1473. See id., supra (explaining how real-time cell site sector location information was an integral part of the aircard locating mission).

1474. See Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (order, p. 4 and fn. 6) (Dkt. #470-2).
buffered for few seconds and then forwarded on to the FBI's SF-Martinez DCS-3000 Pen/Trap device[1475][1476]—a violation of the order's strict requirement that the data be first recorded/stored by Verizon Wireless. In addition to general unreasonableness, the violation of the order's “after receipt and storage” provision was a but-for, unattenuated cause of obtaining geolocation data relating to the aircard. It would have been impossible for Verizon Wireless to comply with the “after receipt and storage” provision of the order considering its Intercept Access Points (IAPs) do not store Pen/Trap data but simply forward the data to law enforcement in real-time. Had Verizon Wireless sought to comply with the order, the FBI would have never been able to obtain the aircard's real-time cell site sector location information.[1477]

d. Neither the N.D.Cal. 08-90331MISC-RS order application nor supporting affidavit act to cure defects in the issued order.

The government is unable to meet the requirements to have the underlying N.D.Cal. 08-90331MISC-RS order application and affidavit act to cure defects in the issued order. The reasons as to why the underlying documents fail to cure defects in the N.D.Cal. 08-90331MISC-RS order are nearly identical to the reasons explained in Section V(F)(1)(j), supra[1478]—applicable to the 08-9033MISC-RS order and its underlying documents failing to cure defects. See Argument, Section V(F)(1)(j), supra (containing supporting legal analysis and citations). Similar to what was explained in Section V(F)(1)(j), supra, the N.D.Cal. 08-90331MISC-RS order does not contain suitable words of reference

1475. See General Facts, Section IV(B)(6), supra (citing supporting evidence).

1476. See also EXHIBIT 067 of 2nd Consolidated Exhibits (Dkt. #821-3) (January 28, 2011 letter from AUSA Battista to the defendant, p. 4: “Any information transmitted to the FBI pursuant to any disclosed court Order was received by Verizon Wireless, buffered by Verizon Wireless and then transmitted to the FBI. The time period from receipt by Verizon Wireless, buffering and then transmission to the FBI is extremely short.”).

1477. See also In The Matter Of An Application Of The United States For An Order (1) Authorizing The Use Of A Pen Register And A Trap And Trace Device And (2) Authorizing Release Of Subscriber Information And/Or Cell Site Information, 396 F.Supp.2d 294, 314 (E.D.N.Y. 2005) (“Orenstein (mj) 2005 Opinion”) (“Of greater concern is the absence of any indication of how the government would, as a practical matter, obtain 'disclosure' of cell site information from the provider after the fact – however quickly – rather than intercept the information by means of its pen register.”).

1478. Argument, V(F)(1)(j), supra, is hereby incorporated into this section by reference.
incorporating the underlying application and affidavit. Additionally, even if the N.D.Cal. 08-90331MISC-RS order can somehow be construed to contain suitable words of reference, the government is yet to offer any evidence indicating that the undisclosed FBI technical agents, and/or Verizon Wireless, had the actual order with them while locating the aircard, let alone the application and affidavit. Finally, there is nothing even contained in the underlying documents that act to cure any of the violations being challenged by the defendant.

3. The D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders do not render any of the applicable searches and seizures reasonable.

The places, items, etc. searched by the government while executing the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Searched place, item, etc.:</th>
<th>Explanation of relevant searches conducted by the government:</th>
<th>Sections addressing searches:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A private residence (i.e., Apartment No. 1122);</td>
<td>(1) the FBI obtaining from Verizon Wireless historical cell site location information relating to the location of the aircard while it was inside apartment No. 1122; (2) the FBI using triangulation and location signature techniques on aircard historical cell site location information;</td>
<td>1. Section V(E)(1)(b) 2. Section V(E)(1)(c)</td>
</tr>
<tr>
<td>2</td>
<td>Aircard (i.e., UTStarcom PC5740 broadband access card);</td>
<td>(1) the FBI obtaining from Verizon Wireless historical cell site location information relating to the location of the aircard while it was inside apartment No. 1122; (2) the FBI using triangulation and location signature techniques on aircard historical cell site location information;</td>
<td>1. Section V(E)(1)(b) 2. Section V(E)(1)(c)</td>
</tr>
</tbody>
</table>

1479. There is absolutely no mention of the affidavit and any mention of the application fails to use verbiage that amounts to an express incorporation into the N.D.Cal. 08-90331MISC-RS order. First, the application is mentioned in an introductory paragraph that merely states that less-than-probable-cause findings were made after review of the application. See Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (order, p. 1) (“Upon review of the Application, the Court hereby FINDS that: [there is less-than-probable-cause to obtain cell site information”]) (Dkt. #470-2). Second, the application is mentioned in the closing section of the order requiring that the document be sealed. See id., p. 6. Neither of the noted sections contain verbiage expressly incorporating either document into the underlying order in a curative fashion.
The effects, information, *etc.* seized by the government while executing the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Seized effect, information, <em>etc.</em>:</th>
<th>Explanation of relevant seizures (or preceding searches) conducted by the government:</th>
<th>Sections addressing seizures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Historical cell site location information relating to aircard while inside a private residence;</td>
<td><em>(1)</em> the FBI obtaining from Verizon Wireless historical cell site location information relating to the location of the aircard while it was inside apartment No. 1122;</td>
<td>1. Section V(E)(1)(b)</td>
</tr>
<tr>
<td>2</td>
<td>Location of the aircard and the defendant inside apartment No. 1122;</td>
<td><em>(1)</em> the FBI obtaining from Verizon Wireless historical cell site location information relating to the location of the aircard while it was inside apartment No. 1122; <em>(2)</em> the FBI using triangulation and location signature techniques on aircard historical cell site location information;</td>
<td>1. Section V(E)(1)(b) 2. Section V(E)(1)(c)</td>
</tr>
</tbody>
</table>

The places, items, *etc.* searched by the government (via its agent, Verizon Wireless) while executing the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Searched place, item, <em>etc.</em>:</th>
<th>Explanation of relevant searches conducted by Verizon Wireless as an agent for government:</th>
<th>Sections addressing searches:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A private residence <em>(i.e., Apartment No. 1122)</em>;</td>
<td><em>(1)</em> Verizon Wireless providing the FBI historical cell site location information relating to the location of the aircard while it was inside apartment No. 1122;</td>
<td>1. Section V(E)(1)(b)</td>
</tr>
<tr>
<td>2</td>
<td>Aircard <em>(i.e., UTStarcom PC5740 broadband access card)</em>;</td>
<td><em>(1)</em> Verizon Wireless providing the FBI historical cell site location information relating to the location of the aircard while it was inside apartment No. 1122;</td>
<td>1. Section V(E)(1)(b)</td>
</tr>
</tbody>
</table>

The effects, information, *etc.* seized by the government (via its agent, Verizon Wireless) while executing the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Seized effect, information, <em>etc.</em>:</th>
<th>Explanation of relevant seizures conducted by Verizon Wireless as an agent for government:</th>
<th>Sections addressing seizures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Historical cell site location information relating to aircard while inside a private residence;</td>
<td><em>(1)</em> Verizon Wireless providing the FBI historical cell site location information relating to the location of the aircard while it was inside apartment No. 1122;</td>
<td>1. Section V(E)(1)(b)</td>
</tr>
</tbody>
</table>
Location of the aircard and the defendant inside apartment No. 1122;  

| 1480. See Government’s Memorandum Re Motion For Discovery (Dkt. #674, p. 1), (footnote omitted); see also January 4, 2012 Court Order (Dkt. #723, p. 14-15) (“[F]or purposes of Defendant’s motion to suppress, the government agrees that the Court may assume that the aircard tracking operation was a Fourth Amendment search and seizure.”). |
| 1481. See also Argument, Section V(F)(2)(a), supra (quoting/paraphrasing Winsor, Reilly, and Payton) |
| 1482. Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard (order, p. 1) (Dkt. #576-4, p. 2); id. (order, p. 1) (Dkt. #576-6, p. 2). |
Amendment requires “probable cause,” U.S. Const. Amend. IV, and not the lesser standard of “specific and articulable facts,” the government finds no support in the orders to justify its searches and seizures.

b. The FBI's searches and seizures conducted during execution of the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders exceeded the scope of the issued orders.

All searches and seizures conducted under the D.Ariz cell site information orders were in further violation of the defendant's Fourth Amendment rights based on scope violations. Specifically, the FBI technical agents and Verizon Wireless violated the particularity clause of the Fourth Amendment through various scope violations. As explained in Section V(F)(1)(a), supra, analyzing scope violations requires application of the Hitchcock test: “Whether a search exceeds the scope of a search warrant is an issue we determine through an objective assessment of the circumstances surrounding the issuance of the warrant, the contents of the search warrant, and the circumstances of the search.” Hurd, 499 F.3d at 966 (citation omitted). Below, the Hitchcock test is applied to the government's Fourth Amendment searches and seizures conducted during execution of the D.Ariz. cell site information orders.

Applying the first part of the Hitchcock test, the government failed to seek a warrant to locate the aircard[1483] and instead submitted applications for court orders that did not seek authorization to conduct the searches and seizures occurring during the orders' execution.[1484] The government failed to even include the word “location” in the proposed orders and the applications do not contain the word “location” in any relevant context. None of the documents presented to the magistrates contain any indication that the government sought to locate the aircard and the defendant in any fashion whatsoever.[1485] Applying the

1483. See Argument, Section V(F)(3)(a), supra (explaining how the government failed to obtain a warrant and probable cause finding in support of its searches and seizures).

1484. Compare Argument, Section V(F)(3), supra (listing searches and seizures conducted by the government and Verizon Wireless) with Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard (Dkt. #576-3 and #576-5) (applications failing to seek authority to conduct the listed searches and seizures).

1485. See id.
second part of the Hitchcock test, the issued orders themselves list neither the aircard nor 
private residences as places to be searched.\[1486]\[1487] For the items to be seized, the orders 
list neither historical cell site location information nor the location of the aircard while inside 
a private residence.\[1488] The D.Ariz. cell site information orders list (1) cell site 
information, (2) sector information, and (3) distance information—all particularized for the 
sole purpose of determining “the cellular/data network’s registration of the assigned 
broadband access card(s)...”\[1489]\[1490] Because the aircard never conducted “registration” 
with the Verizon Wireless network—a process that is simply void in the context of 1xEV-DO 
Rel. 0 Access Terminals connecting to Access Networks\[1491]—all historical cell site 
location information obtained by the government was plainly beyond what the orders 

1486. See id.; see also Procedural History, Section III(C) and (D), supra (explaining 
procedural aspects of the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders).

1487. Although it would have been impossible to list the precise address of apartment No. 
1122, the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders still could have listed 
“private residences” as places to be searched.

1488. See id.

1489. Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB- 
LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard 
(order, ATTACHMENT A) (Dkt. #576-4, p. 4); id. (order, ATTACHMENT A) (Dkt. #576-5, 
p. 4).

1490. As explained in the Technical Explanations, Section II(D)(1), supra, the term “cell 
site information” is an ambiguous catch-all phrase and it therefore fails to meet the 
particularity requirement of the Fourth Amendment. However, a catch-all phrase does not 
invalidate an otherwise valid warrant if it is accompanied by a more particularized 
description of what is to be seized. See Andersen v. Maryland, 427 U.S. 463, 479 (1979). 
The D.Ariz. cell site information orders further particularize the catch-all phrase of “cell site 
information” as data that will allow the government “to determine” the network’s 
“registration” of the aircard. The remaining listed data, i.e., “sector/distance information,” is 
irrelevant considering it does not describe any of the historical cell site location information 
obtained by the government under the orders. See General Facts, Section IV(B)(2), supra 
discussing the data seized by the government under the D.Ariz. cell site information orders).

1491. See Technical Explanations, Section II(B) et seq., supra (explaining the 1xEV-DO 
cellular communications system deployed by Verizon Wireless).
authorized. As apposed to “registration,”[1492] the aircard established sessions[1493] with the Verizon Wireless network following each initial power-on and route update.[1494] Therefore, all of the historical geolocation data obtained by the government was determinate of the aircard's session establishments / route updates—as apposed to falling within the scope of the issued orders, i.e., data determinate of the aircard's “registration.” Applying the third and final part of the Hitchcock test, the circumstances surrounding the execution of the various searches and seizures also point towards a scope violation. While conducting the various unauthorized searches and seizures, the FBI technical agents made no returns to the issuing magistrates[1495] and did not serve the defendant with copies of the orders or a receipts of what was seized.[1496] The circumstances surrounding the issuance of the order,s the contents of the orders, and the circumstances surrounding the execution of the orders all support a finding that the relevant searches and seizures were conducted outside the scope of the issued orders.

4. The D.Ariz. 07-03-609 and 07-03-615 Grand Jury subpoenas and/or 08-3286MB-LOA order do not render any of the applicable searches and seizures reasonable.

The places, items, etc. searched by the government while executing the D.Ariz. 07-03-609 and 07-03-615 Grand Jury subpoenas and the D.Ariz. 08-3286MB-LOA order are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Searched place, Explanation of relevant searches</th>
<th>Sections addressing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1492.</td>
<td>As previously explained, “registration” in 1xEV-DO Rel. 0 occurs between the Packet Control Function (PCF) and Packet Data Serving Node (PDSN)—a process not involving the Access Terminal (e.g., aircard) and unrelated to cell site location. See id., Section II(B)(3)(c)(vi), supra; see also EXHIBIT 055 of 2\textsuperscript{nd} Consolidated Exhibits (Dkt. #821-3) (diagram from ANSI/TIA-878-2 (Addenda to TIA-878) showing 1xEV-DO registration process occurring between PCF and PDSN over the A11 interface, i.e., not between the Access Terminal and Access Network).</td>
<td></td>
</tr>
<tr>
<td>1493.</td>
<td>See Technical Explanations, Section II(B)(3)(c)(iii), supra (explaining 1xEV-DO Rel. 0 session establishment).</td>
<td></td>
</tr>
<tr>
<td>1494.</td>
<td>See id., Section II(B)(3)(d) et seq., supra (explaining the different types of handoffs dictated by the Default Route Update Protocol).</td>
<td></td>
</tr>
<tr>
<td>1495.</td>
<td>See Procedural History, Section III(C) and (D), supra (explaining procedural aspects of the D.Ariz. 08-3298MB-LOA and 08-7273MB-ECV orders).</td>
<td></td>
</tr>
<tr>
<td>1496.</td>
<td>See General Facts, Section IV(B)(18), supra.</td>
<td></td>
</tr>
</tbody>
</table>
The effects, information, etc. seized by the government while executing the D.Ariz. 07-03-609 and 07-03-615 Grand Jury subpoenas and the D.Ariz. 08-3286MB-LOA order are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Seized effect, information, etc.:</th>
<th>Explanation of relevant seizures (or preceding searches) conducted by the government:</th>
<th>Sections addressing seizures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The defendant's 1.8 million destination IP addresses relating to use of the aircard;</td>
<td>(1) Verizon Wireless providing the FBI with the defendant's 1.8 million destination IP addresses relating to his use of the aircard to access the Internet;</td>
<td>1. Section V(E)(1)(a)</td>
</tr>
<tr>
<td>2</td>
<td>Communications content and other private information derived from destination IP addresses;</td>
<td>(1) Verizon Wireless providing the FBI with the defendant's 1.8 million destination IP addresses relating to his use of the aircard to access the Internet;</td>
<td>1. Section V(E)(1)(a)</td>
</tr>
</tbody>
</table>

The effects, information, etc. seized by the government (via its agent, Verizon Wireless) while executing the D.Ariz. 07-03-609 and 07-03-615 Grand Jury subpoenas and the D.Ariz. 08-3286MB-LOA order are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Seized effect, information, etc.:</th>
<th>Explanation of relevant seizures conducted by Verizon Wireless as an agent for government:</th>
<th>Sections addressing seizures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The defendant's 1.8 million destination IP addresses relating to use of the aircard;</td>
<td>(1) Verizon Wireless providing the FBI with the defendant's 1.8 million destination IP addresses relating to his use of the aircard to access the Internet;</td>
<td>1. Section V(E)(1)(a)</td>
</tr>
</tbody>
</table>

a. The searches and seizures conducted during execution of the D.Ariz. 07-03-609 and 07-03-615 Grand Jury subpoenas and 08-3286MB-LOA order were not backed by anything resembling a probable cause warrant.

Considering the D.Ariz. 07-03-609 and 07-03-615 Grand Jury subpoenas and the D.Ariz. 08-3286MB-LOA order (hereafter sometimes referred to as “destination IP address subpoenas and order”) were not issued based on findings of probable cause, all relevant
searches and seizures were conducted in violation of the defendant's Fourth Amendment rights. The government conceded that “the aircard tracking operation was a Fourth Amendment search and seizure.”[1497] The government's concession covers the actions taken by the government directly and by Verizon Wireless while executing the D.Ariz. destination IP address subpoenas and order. Additionally, the defendant identified and categorized the specific searches and seizures that occurred during execution of the subpoenas and order (see Argument, Section V(E)(1)(a), supra), which are summarized in the table immediately above (see Argument, Section V(F)(4), supra). Because, and as the government concedes, the relevant actions were Fourth Amendment searches and seizures, the D.Ariz. destination IP address subpoenas and order must contain probable cause findings in support of the various searches and seizures conducted in relation to those documents.

See, e.g., Winsor, 846 F.2d at 1575; Reilly, 224 F.3d at 995; Payton, 445 U.S. at 585.[1498]

First, the destination IP address subpoenas contain no probable cause findings and were not reviewed by a magistrate prior to being issued.[1499] “When the right of privacy must reasonably yield to the right of a search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.” United States v. Johnson, 333 U.S. 10, 14 (1948); see also United States v. Dionisio, 410 U.S. 1, 11 (1973) (a grand jury subpoena is not a “talisman that dissolves all constitutional protections.”). Second, the magistrate who issued the destination IP address order merely found that AUSA Battista “offered 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.”[1500]

Considering the Fourth Amendment requires “probable cause,” U.S. 1497. See Government's Memorandum Re Motion For Discovery (Dkt. #674, p. 1), (footnote omitted); see also January 4, 2012 Court Order (Dkt. #723, p. 14-15) (“[F]or purposes of Defendant’s motion to suppress, the government agrees that the Court may assume that the aircard tracking operation was a Fourth Amendment search and seizure.”).

1498. See also Argument, Section V(F)(2)(a), supra (quoting/paraphrasing Winsor, Reilly, and Payton)

1499. See Submission Of Documents Related To District Of Arizona Grand Jury Subpoenas 07-03-609 And 07-03-615 Obtained To Facilitate Locating The Aircard (Dkt. #565-1 and #565-2).

1500. Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-
Const. Amend. IV, and not the lesser standard of a mere subpoena or “specific and articulable facts,” the government finds no support in the D.Ariz. destination IP address subpoenas and order to justify its searches and seizures.

b. The description of “destination IP addresses” contained in the D.Ariz. 07-03-609 and 07-03-615 Grand Jury subpoenas and 08-3286MB-LOA order fails for lack of particularity.

Because the destination IP address subpoenas and order lack particularity, the government obtaining 1.8 million of the defendant's destination IP addresses was a violation of his Fourth Amendment rights. The subpoenas requested that Verizon Wireless provide the government with all of the destination IP addresses accessed by the defendant between March 1, 2008 and June 16, 2008. Similarly, the subsequent “retroactive” order requested the same data already received via the subpoenas as well as further destination IP addresses accessed by the defendant through July 9, 2008. In the subpoenas and order, the government made no attempt to narrow its requests to destination IP addresses it had identified as being linked to alleged criminal activity. In McLaughlin, the Ninth Circuit found a particularity violation because “information available from a prior investigation would have permitted more specific descriptions.” United States v. McLaughlin, 851 F.2d 283, 285 (9th Cir. 1988). McLaughlin is directly on point with the present case because, for example, “the IRS Fraud Detection Center... identified approximately 1,272 returns[,] [and] 175 IP addresses...” corresponding to “electronically filed returns for the 2007 tax year.”

The government could have very easily provided Verizon Wireless with a list of the 175 relevant destination IP addresses and requested that they conduct a “keyword search” for all matching IP addresses accessed by the aircard. In fact, after the Fourth Amendment

1501. See Procedural History, Section III(A), supra (discussing procedural aspects of D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615).
1502. See Procedural History, Section III(B), supra (discussing procedural aspects of D.Ariz. 08-3286MB-LOA court order).
1503. Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122 (affidavit, p. 3) (#566-1, p. 5).
violation had already occurred, IRS-CI Agent Daun was able to conduct a search precisely of this nature by using the overly broad 1.8 million destination IP addresses seized from Verizon Wireless.\[1504\] Considering the government “was able to describe the items more particularly in light of information available to it at the time[,]” the subpoenas and order fail for lack of particularity. United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986).

5. The D. Ariz. 07-03-709 Grand Jury subpoena does not render any of the applicable searches and seizures reasonable.

The places, items, etc. searched by the government while executing the D. Ariz. 07-03-709 Grand Jury subpoena are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Searched place, item, etc.:</th>
<th>Explanation of relevant searches conducted by the government:</th>
<th>Sections addressing searches:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A private residence (i.e., Apartment No. 1122);</td>
<td>(1) obtaining and using the defendant's historical geolocation information via his Domicilio electronic gate key access records;</td>
<td>1. Section V(E)(1)(r)</td>
</tr>
</tbody>
</table>

The effects, information, etc. seized by the government while executing the D. Ariz. 07-03-709 Grand Jury subpoena are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Seized effect, information, etc.:</th>
<th>Explanation of relevant seizures (or preceding searches) conducted by the government:</th>
<th>Sections addressing seizures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Historical geolocation information via Domicilio electronic gate key access records;</td>
<td>(1) obtaining and using the defendant's historical geolocation information via his Domicilio electronic gate key access records;</td>
<td>1. Section V(E)(1)(r)</td>
</tr>
<tr>
<td>2</td>
<td>Location of the defendant inside apartment No. 1122;</td>
<td>(1) obtaining and using the defendant's historical geolocation information via his Domicilio electronic gate key access records;</td>
<td>1. Section V(E)(1)(r)</td>
</tr>
</tbody>
</table>

1504. See General Facts, Section IV(B)(1), supra; EXHIBIT 078 of 2\textsuperscript{nd} Consolidated Exhibits (Dkt. #821-4) (June 25, 2008 email from IRS-CI Agent Daun to FBI Agent Murray et al.: “based on the pattern following along for just all of the Ips that I found to match - I really think this is the person filing the returns...”). See also EXHIBIT 14 of 1\textsuperscript{st} Consolidated Exhibits (Dkt. #587-1) (July 1, 2008 email from IRS-CI Agent Daun to Nathan A. Watt: “We have correlated returns being filed from specific Proxy Ips, that this guy was also connected to at the same time.”); EXHIBIT 15 of 1\textsuperscript{st} Consolidated Exhibits (Dkt. #587-1) (July 7, 2008 email from IRS-CI Agent Medrano to Constance M. Davis: “We strongly believe we have identified the [[[suspect]]...”).
The places, items, etc. searched by the government (via its agent, Quality Alarm Service) while executing the D.Ariz. 07-03-709 Grand Jury subpoena are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Searched place, item, etc.:</th>
<th>Explanation of relevant searches conducted by Quality Alarm Service as an agent for government:</th>
<th>Sections addressing searches:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A private residence (i.e., Apartment No. 1122);</td>
<td>(1) obtaining and using the defendant's historical geolocation information via his Domicilio electronic gate key access records;</td>
<td>1. Section V(E)(1)(r)</td>
</tr>
</tbody>
</table>

The effects, information, etc. seized by the government (via its agent, Quality Alarm Service) while executing the D.Ariz. 07-03-709 Grand Jury subpoena are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Seized effect, information, etc.:</th>
<th>Explanation of relevant seizures conducted by Quality Alarm Service as an agent for government:</th>
<th>Sections addressing seizures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Historical geolocation information via Domicilio electronic gate key access records;</td>
<td>(1) obtaining and using the defendant's historical geolocation information via his Domicilio electronic gate key access records;</td>
<td>1. Section V(E)(1)(r)</td>
</tr>
<tr>
<td>2</td>
<td>Location of the defendant inside apartment No. 1122;</td>
<td>(1) obtaining and using the defendant's historical geolocation information via his Domicilio electronic gate key access records;</td>
<td>1. Section V(E)(1)(r)</td>
</tr>
</tbody>
</table>

a. The searches and seizures conducted during execution of the D.Ariz. 07-03-709 Grand Jury subpoena were not backed by anything resembling a probable cause warrant.

Considering the D.Ariz. 07-03-709 Grand Jury subpoena was not issued based on a finding of probable cause, all relevant searches and seizures were conducted in violation of the defendant's Fourth Amendment rights. The government conceded that “the aircard tracking operation was a Fourth Amendment search and seizure.”[1506] The government's

1505. Where a private party acts as an instrument or agent of the government in effecting a search or seizure, fourth amendment interests are implicated” See Walther, 652 F.2d at 791. Through the D.Ariz. 07-03-709 Grand Jury subpoena, the government was “exercising such coercive power” over Quality Alarm Service “that it is responsible for the specific private conduct” carried out by Quality Alarm Service employees. Fidelity Financial Corp., 792 F.2d at 1435.

1506. See Government's Memorandum Re Motion For Discovery (Dkt. #674, p. 1), (footnote omitted); see also January 4, 2012 Court Order (Dkt. #723, p. 14-15) (“[F]or purposes of Defendant’s motion to suppress, the government agrees that the Court may assume that the aircard tracking operation was a Fourth Amendment search and seizure.”).
concession covers the actions taken by the government directly and by Quality Alarm Service while executing the D.Ariz. 07-03-709 Grand Jury subpoena. Additionally, the defendant identified and categorized the specific searches and seizures that occurred during execution of the subpoena (see Argument, Section V(E)(1)(r), supra), which are summarized in the table immediately above (see Argument, Section V(F)(5), supra). Because, and as the government concedes, the relevant actions were Fourth Amendment searches and seizures, the D.Ariz. 07-03-709 Grand Jury subpoena must contain a probable cause finding in support of the various searches and seizures conducted in relation to the subpoena. See, e.g., Winsor, 846 F.2d at 1575; Reilly, 224 F.3d at 995; Payton, 445 U.S. at 585.[1507] The D.Ariz. 07-03-709 Grand Jury subpoena contains no probable cause finding and was not reviewed by a magistrate prior to being issued.[1508] “When the right of privacy must reasonably yield to the right of a search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.” Johnson, 333 U.S. at 14; see also Dionisio, 410 U.S. at 11 (a grand jury subpoena is not a “talisman that dissolves all constitutional protections.”). Considering the Fourth Amendment requires “probable cause,” U.S. Const. Amend. IV, and not the lesser standard of a mere subpoena, the government finds no support in the D.Ariz. 07-03-709 Grand Jury subpoena to justify its searches and seizures.

G. The good-faith exception to the exclusionary rule does not apply to the government's various illegal Fourth Amendment searches and seizures.

The Supreme Court has identified a number of circumstances of which a “good-faith exception” to the exclusionary rule acts to erase government perpetrated Fourth Amendment violations resulting in otherwise illegally obtained evidence being admissible at trial. The Supreme Court's good faith exceptions apply under the following circumstances: (1) government actors violate the Fourth Amendment while relying on a warrant later held invalid due to a magistrate's erroneous determination that the warrant application established

1507. See also Argument, Section V(F)(2)(a), supra (quoting/paraphrasing Winsor, Reilly, and Payton)

1508. See Submission Of Documents Related To District Of Arizona Grand Jury Subpoena 07-03-709 Obtained To Facilitate Locating The Aircard (Dkt. #805-1 and #805-2).
probable cause,\footnote{1509} (2) government actors violate the Fourth Amendment while relying on a warrant later held invalid due to a magistrate's clerical error,\footnote{1510} (3) government actors violate the Fourth Amendment while relying on a statute later held unconstitutional,\footnote{1511} (4) government actors violate the Fourth Amendment while relying on mistaken arrest warrant information contained in a court database,\footnote{1512} (5) government actors violate the Fourth Amendment while relying on mistaken arrest warrant information contained in a law enforcement database,\footnote{1513} and (6) government actors violate the Fourth Amendment while relying on binding appellate court precedent.\footnote{1514} Regardless of the circumstance, the “good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that a search was illegal in light of all of the circumstances.” \cite{Herring} 129 S.Ct. at 703 (internal quotation marks and citation omitted). In the present case, none of the government's illegal Fourth Amendment searches and seizures occurred under any of the circumstances enumerated above. To the contrary, and as the proceeding subsections will explain, the government's flagrant misconduct in the present case occurred under circumstances where various courts have found that the good-faith exception to the exclusionary rule plainly does not apply.\footnote{1515}

1. Consolidated “no good-faith” argument RE: lack of probable cause findings; \textit{[applicable to all orders and subpoenas].}

The orders and subpoenas that lack applicable probable cause findings—causing them to be inadequate avenues for government claims of good-faith—are as follows:

\footnote{1514} See United States v. Davis, 131 S.Ct. 2419 (2011).
\footnote{1515} The proceeding subsections do not set out to explain all of the reasons why the good-faith exception to the exclusionary rule should not apply to the government's illegal Fourth Amendment searches and seizures involved in the present case. See, \textit{e.g.}, United States v. Michaelian, 803 F.2d 1042, 1048 (9th Cir. 1986) (“The government, not the defendant, bears the burden of proving that its agents' reliance upon the warrant was objectively reasonable.”).
<table>
<thead>
<tr>
<th>#</th>
<th>Relevant order or subpoena:</th>
<th>Description of violation/circumstance precluding government claim of good-faith:</th>
<th>Sections addressing violation/circumstance:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N.D.Cal. 08-90330MISC-RS “mobile tracking device” order;</td>
<td>(1) authorized actions were supported by a less-than-probable-cause “specific and articulable facts” finding;</td>
<td>1. Section V(F)(1)(f)</td>
</tr>
<tr>
<td>2</td>
<td>N.D.Cal. 08-90331MISC-RS “Pen/Trap real-time cell site sector information” order;</td>
<td>(1) authorized actions were supported by a less-than-probable-cause “relevancy” and “specific and articulable facts” finding;</td>
<td>1. Section V(F)(2)(a)</td>
</tr>
<tr>
<td>3</td>
<td>D.Ariz. 08-3298MB-LOA “cell site information” order;</td>
<td>(1) authorized actions were supported by a less-than-probable-cause “specific and articulable facts” finding;</td>
<td>1. Section V(F)(3)(a)</td>
</tr>
<tr>
<td>4</td>
<td>D.Ariz. 08-7273MB-ECV “cell site information” order;</td>
<td>(1) authorized actions were supported by a less-than-probable-cause “specific and articulable facts” finding;</td>
<td>1. Section V(F)(3)(a)</td>
</tr>
<tr>
<td>5</td>
<td>D.Ariz. 07-03-609 “destination IP address” Grand Jury subpoena;</td>
<td>(1) authorized actions were supported by no findings at all;</td>
<td>1. Section V(F)(4)(a)</td>
</tr>
<tr>
<td>6</td>
<td>D.Ariz. 07-03-615 “destination IP address” Grand Jury subpoena;</td>
<td>(1) authorized actions were supported by no findings at all;</td>
<td>1. Section V(F)(4)(a)</td>
</tr>
<tr>
<td>7</td>
<td>D.Ariz. 08-3286MB-LOA “destination IP address” order;</td>
<td>(1) authorized actions were supported by less-than-probable-cause “specific and articulable facts” finding;</td>
<td>1. Section V(F)(4)(a)</td>
</tr>
<tr>
<td>8</td>
<td>D.Ariz. 07-03-709 “electronic gate geolocation information” Grand Jury subpoena;</td>
<td>(1) authorized actions were supported by no findings at all;</td>
<td>1. Section V(F)(5)(a)</td>
</tr>
</tbody>
</table>

The government cannot claim a good-faith reliance on any of the above listed orders or subpoenas because they are not warrants supported by probable cause findings specific to the Fourth Amendment searches and seizures conducted by the government. In *Leon*, the Supreme Court made clear that they were “leav[ing] untouched the probable-cause standard and the various requirements for a valid warrant.” *Leon*, 468 U.S. at 923. Therefore, because the prosecution conceded that the agents' actions were Fourth Amendment searches...
and seizures, the government simply cannot claim a good-faith reliance on documents that contain either no probable cause findings at all or a probable cause finding irrelevant to what the document authorized. Additionally, the government cannot now claim that at the time of the searches and seizures, the agents' subjective states of mind were that their actions were something less than Fourth Amendment searches and seizures. “[E]venhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state of mind of the officer.” United States v. Ewain, 88 F.3d 689, 694 (9th Cir. 1996) (addressing government claim of good-faith). In other words, the prosecution's concession that the agents' actions were Fourth Amendment searches and seizures applies just as much at the time when the searches and seizures actually occurred as it applies now. Because, from an objective standpoint, the agents were conducting Fourth Amendment searches and seizures without probable cause findings, the government is now precluded from claiming a good-faith reliance on any order or subpoena in any manner whatsoever.

2. Consolidated “no good-faith” argument RE: scope violations; [applicable to various orders].

The orders corresponding to various scope violations,—causing them to be inadequate avenues for government claims of good-faith—are as follows:

1516. See Government’s Memorandum Re Motion For Discovery (Dkt. #674, p. 1), (footnote omitted); see also January 4, 2012 Court Order (Dkt. #723, p. 14-15) (“[F]or purposes of Defendant’s motion to suppress, the government agrees that the Court may assume that the aircard tracking operation was a Fourth Amendment search and seizure.”). In Section V(E) et seq., supra, the defendant identified and categorized all of the government's Fourth Amendment searches and seizures covered by the prosecutions blanket concession.

1517. The documents that contain no probable cause findings at all are as follows: D.Ariz. Grand Jury subpoena No. 07-03-609, D.Ariz. Grand Jury subpoena No. 07-03-615, D.Ariz. 08-3286MB-LOA order, D.Ariz. 08-3298MB-LOA order, D.Ariz. 08-7273MB-LOA order, N.D.Cal. 08-90331MISC-RS order, and D.Ariz. Grand Jury subpoena No. 07-03-709.

1519. The document that contains a probable cause finding irrelevant to what the document authorized is as follows: N.D.Cal. 08-90330MISC-RS order. See, e.g., Greenstreet v. County of San Bernardino, 41 F.3d 1306, 1309 (9th Cir. 1994) (“A search warrant designating more than one person or place to be searched must contain sufficient probable cause to justify its issuance as to each person or place named therein.”) (citation omitted)).
The government cannot claim a good-faith reliance on any of the above listed orders because agents conducted various searches and seizures beyond the scope of each order's terms. In *Leon*, the Supreme Court made clear that the good-faith exception "assumes, of course, that officers properly executed the warrant and searched only those places and for those objects that it was reasonable to believe were covered by the warrant." *Leon*, 468 U.S. at 918 fn. 19. See also *Robinson*, 358 F.Supp.2d at 980 ("Because the search of the residence exceeded the scope of the warrant, the evidence must be suppressed... [and] the good faith exception has no application in this case."); *Hitchcock*, 286 F.3d at 1072 ("The good faith exception has no application here, where... the issue is whether the search was conducted within the scope of a warrant..."). Because the government exceeded the scope of what the relevant orders authorized, it is precluded from claiming a good-faith reliance on the issued orders.

3. Consolidated “no good-faith” argument RE: particularity violations; [applicable to various orders and subpoenas].

The orders and subpoenas that fail for lack of particularity—causing them to be

---

1520. See also, id. at 920 (Explaining that the good-faith exception only applies if government actors “obtained a search warrant from a judge or magistrate and acted within its scope.” (footnote omitted)).
inadequate avenues for government claims of good-faith—are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Relevant order or subpoena:</th>
<th>Description of violation/circumstance precluding government claim of good-faith:</th>
<th>Sections addressing violation/circumstance:</th>
</tr>
</thead>
</table>
| 1  | N.D.Cal. 08-90330MISC-RS “mobile tracking device” order;       | (1) if even applicable, the “mobile tracking device” term fails for lack of particularity; (2) if even described at all, the place to be searched fails for lack of particularity; (3) the “all data, information, facilities, and technical assistance” term fails for lack of particularity; | 1. Section V(F)(1)(d)  
    2. Section V(F)(1)(e)  
    3. Section V(F)(1)(g) |
| 2  | D.Ariz. 07-03-609 “destination IP address” Grand Jury subpoena; | (1) the “destination IP address” description fails for lack of particularity;                                                             | 1. Section V(F)(4)(b)                                    |
| 3  | D.Ariz. 07-03-615 “destination IP address” Grand Jury subpoena; | (1) the “destination IP address” description fails for lack of particularity;                                                             | 1. Section V(F)(4)(b)                                    |
| 4  | D.Ariz. 08-3286MB-LOA “destination IP address” order;          | (1) the “destination IP address” description fails for lack of particularity;                                                             | 1. Section V(F)(4)(b)                                    |

The government cannot claim a good-faith reliance on the above listed orders or subpoenas because each fails for lack of particularity. In *Leon*, the Supreme Court made clear that the good-faith exception to the exclusionary rule does not apply when a warrant fails to “particularize the place to be searched or the things to be seized...” *Leon*, 468 U.S. at 923. “Given that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid.” *Groh*, 540 U.S. at 563. Specific to the N.D.Cal. 08-90330MISC-RS order, because the government “prepared the invalid [] [order],” it may not argue that it “reasonably relied on the Magistrate's assurance” that the order was valid. *Groh*, 540 U.S. at 564. The prosecution confirmed that the N.D.Cal. 08-90330MISC-RS proposed order was signed “as is.”

[1521] The present case is unlike *Sheppard* where a judge made clerical corrections to a poorly drafted warrant and assured the applicant that the warrant was valid. See *Sheppard*, 468 U.S. at 989. “We have held that absent specific assurances from an...
impartial judge or magistrate that the defective warrant is valid despite its overbreadth, a reasonable reliance argument fails.” Marks v. Clarke, 102 F.3d 1012, 1028 (9th Cir. 1996) (internal quotation marks and citation omitted). Because the Fourth Amendment searches and seizures relevant to the above listed orders and subpoenas were based on descriptions that lack particularity, the government is precluded from claiming a good-faith reliance on the issued documents.

4. Consolidated “no good-faith” argument RE: violating terms and limitations contained in orders; [applicable to various orders].

The orders of which agents violated express terms and limitations—causing them to be inadequate avenues for government claims of good-faith—are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Relevant order or subpoena:</th>
<th>Description of violation/circumstance precluding government claim of good-faith:</th>
<th>Sections addressing violation/circumstance:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N.D.Cal. 08-90330MISC-RS “mobile tracking device” order;</td>
<td>(1) the government violated the limitation to “monitoring”;</td>
<td>1. Section V(F)(1)(i)(i)</td>
</tr>
<tr>
<td>2</td>
<td>N.D.Cal. 08-90331MISC-RS “Pen/Trap real-time cell site sector information” order;</td>
<td>(1) the government violated the limitation to “recording”; (2) the government failed to comply with the “after receipt and storage” provision;</td>
<td>1. Section V(F)(2)(c)(i) 2. Section V(F)(2)(c)(ii)</td>
</tr>
</tbody>
</table>

The government cannot claim a good-faith reliance on the above listed orders because agents violated terms and limitations placed in the orders as to the precise manner in which they were to be executed. In Dalia, the Supreme Court held that “[n]othing in the language of the Constitution or in this Court's decisions interpreting that language suggests that... search warrants [] must include a specification of the precise manner in which they are to be executed.” Dalia, 441 U.S. at 257. However, the Dalia court did not speak to situations where the magistrate does, in fact, expressly include terms and limitations as to precise manner in which an order must be executed and the government thereafter fails to comply with those specifications. In Comprehensive Drug Testing Inc. (“CDTI”), the Ninth Circuit addressed such a situation, albeit in the context of a motion for return of property, and
reasoned that “[w]hen, as here, the government comes into possession of evidence by
circumventing or willfully disregarding limitations in a search warrant, it must not be
allowed to benefit from its own wrongdoing by retaining the wrongfully obtained evidence
or any fruits thereof.” *United States v. Comprehensive Drug Testing Inc.* 621 F.3d 1162,
1174 (9th Cir. 2010) (addressing violations of a computer search protocol). The reasoning of
*CDTI* applies to the good-faith analysis at issue in the present case. Because agents willfully
disregarded the magistrate's terms and limitations placed into the relevant orders, the
government is precluded from claiming a good-faith reliance on the issued orders.

5. **Consolidated “no good-faith” argument RE: Rule 41 violations; [applicable to all orders and subpoenas].**

The orders and subpoenas executed by the government that deliberately disregard
provisions of Rule 41, *Fed. R. Crim. P.*—causing them to be inadequate avenues for
government claims of good-faith—are as follows:[1522]

<table>
<thead>
<tr>
<th>#</th>
<th>Relevant order or subpoena:</th>
<th>Description of violation/circumstance precluding government claim of good-faith:</th>
<th>Sections addressing violation/circumstance:</th>
</tr>
</thead>
</table>
| 1  | N.D.Cal. 08-90330MISC-RS “mobile tracking device” order; | (1) deliberately disregarded Rule 41 inventory and return requirements; (2) deliberately disregarded Rule 41 receipt and service requirements; (3) agents violated Rule 41 receipt and service requirements; (4) agents violated Rule 41 inventory and return requirements; | 1. Section V(F)(1)(h)(ii)  
2. Section V(F)(1)(h)(iii)  
3. Section V(F)(1)(i)(ii)  
4. Section V(F)(1)(i)(iii) |
| 2  | N.D.Cal. 08-90331MISC-RS “Pen/Trap real-time cell site sector information” order; | (1) failed to comply with all provisions of Rule 41, *Fed. R. Crim. P.*; | 1. N/A – see footnote No. 1522, *supra*; |
| 3  | D.Ariz. 08-3298MB- | (1) failed to comply with all provisions of Rule | 1. N/A – see footnote |

[1522] For orders/subpoenas having a “section column” value of “N/A,” the corresponding Rule 41 violations occurring during/after execution of the relevant orders/subpoenas are not addressed in this memorandum in detail. However, for those documents, the government violated every provision of Rule 41 while conducting the related Fourth Amendment searches and seizures addressed in Section V(E) and (F), *supra*. Considering the government used all orders and subpoenas as if they were warrants, Rule 41 violations are relevant to the good-faith analysis. For the orders/subpoenas addressed in this footnote, no good-faith is cognizable considering the subpoenas were not reviewed/issued by a magistrate and the underlying applications for the orders did not inform the issuing magistrates of the planned searches and seizures falling under provisions of Rule 41.
The government cannot claim a good-faith reliance on any of the above listed orders or subpoenas considering agents violated various provisions of Rule 41, Fed. R. Crim. P., and/or destroyed seized evidence. If a provision of Rule 41 is, at the time, generally understood to be a requirement, “deliberate disregard of this rule will indicate to reviewing courts that the warrant should have never been issued, and will render inapplicable the good faith exception.” United States v. Johns, 948 F.2d 599, 606 (9th Cir. 1991). For the N.D.Cal. 08-90330MISC-RS order, the issuing magistrate included terms that “erased” numerous provisions of Rule 41.[1523] However, even with those implicit assurances, the government cannot claim a good-faith reliance considering the magistrate had no business issuing an order permitting the government to ignore relevant provisions of Rule 41. See Sheppard, 468 U.S. at 990 fn. 7 (The good-faith exception does not apply when “a magistrate or judge had no business issuing a warrant.”).

1523. See Procedural History, Section III(E), supra, (discussing procedural aspects of the N.D.Cal. 08-90330MISC-RS order).
6. Consolidated “no good-faith” argument RE: lack of candor in order applications; [applicable to various orders].

The orders executed by the government having underlying order applications exhibiting a lack of candor—causing the orders to be inadequate avenues for government claims of good-faith—are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Relevant order or subpoena:</th>
<th>Description of violation/circumstance precluding government claim of good-faith:</th>
<th>Sections addressing violation/circumstance:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N.D.Cal. 08-90330MISC-RS “mobile tracking device” order;</td>
<td>(1) government did not notify issuing magistrate that it planned to locate the aircard using its own equipment consisting of cell site emulators; (2) government failed to notify the issuing magistrate of the existence of prior orders seeking related information;</td>
<td>1. Section V(G)(6)(a) 2. Section V(G)(6)(c)</td>
</tr>
<tr>
<td>2</td>
<td>N.D.Cal. 08-90331MISC-RS “Pen/Trap real-time cell site sector information” order;</td>
<td>(1) government was misleading with its “general geographical location” claim; (2) government failed to notify issuing magistrate of the existence of prior orders seeking related information;</td>
<td>1. Section V(G)(6)(b) 2. Section V(G)(6)(c)</td>
</tr>
<tr>
<td>3</td>
<td>D.Ariz. 08-3286MB-LOA “destination IP address” order;</td>
<td>(1) government failed to advise issuing magistrate of extensive use of illegally obtained destination IP addresses;</td>
<td>1. Section V(G)(6)(d)</td>
</tr>
</tbody>
</table>

The government cannot claim a good-faith reliance on any of the above listed orders because prosecutors and agents who applied for the orders exhibited a lack of candor in the underlying order applications. In *CDTI*, Justice Kozinski reasoned that “[a] lack of candor in [] any [] aspect of [][a] warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data.” *Comprehensive Drug Testing Inc.*, 621 F.3d at 1178 (Kozinski, J., concurring). In *Marks*, the Ninth Circuit denied the government qualified immunity for a Fourth Amendment violation in part because “it appear[ed] that the magistrate may have been misled by the terms of the request set forth in the affidavit...” *Marks v. Clarke*, 102 F.3d 1012, 1028 (9th Cir. 1996). In the present case, the government exhibited a lack of candor in the underlying order applications applicable to the above listed orders. The proceeding subsections identify and explain the government's lack of candor relevant to each order application.
a. Lack of candor in the N.D.Cal. 08-90330MISC-RS order application relating to the government's true intentions.

In the N.D.Cal. 08-90330MISC-RS order application, the government did not inform the issuing magistrate that it planned to locate the aircard through use of cell site emulators and related equipment. The government also failed to inform the magistrate that it would use its own equipment, as opposed to Verizon Wireless using its network, to (1) hijack the aircard connection, (2) download data from the aircard, (3) deactivate aircard encryption, (4) conduct interrogation upon the aircard, (5) collect transmitted aircard signals, (6) triangulate aircard signals, (7) forced the aircard to transmit at a higher power, and (8) deny the aircard access to the Internet. The Court has already expressed concern over the government being able to obtain the N.D.Cal. 08-90330MISC-RS order without explaining the technology to the issuing magistrate. See February 10, 2011 Status Conference, Partial Transcript of Proceedings, p. 26, 16:17:47 – 16:18:23 [THE COURT] (“So what is the judge -- I mean, the reason I'm asking this is a search warrant, as you know, is very specific. It says you can search during daylight hours at this location and these are pertinent buildings for the following items. How did this order authorize the use of this equipment without saying specifically what it was?”).

b. Lack of candor in the N.D.Cal. 08-90331MISC-RS order application relating to “general geographical location” claim.

In the N.D.Cal. 08-90331MISC-RS order application, the government did not inform the issuing magistrate that it intended to obtain the precise location of the aircard within a private residence. The applicant, AUSA Yen, instead indicated that the “the general geographical location of the [aircard] derived from [real-time] cell site information... can [be] compare[d] to] observations of the user of the [aircard]... in order to verify the identification and approximate location of the user of the [aircard].”[1524] Nothing in the order application properly advised the issuing magistrate of the government's true intentions to precisely locate the aircard and its user.

1524. Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (application, p. 8 (emphasis added)) (Dkt. #470-2).
c. Lack of candor in the N.D.Cal. 08-90330MISC-RS and 08-90331MISC-RS order applications relating to failure to advise of prior orders seeking related information.

In the N.D.Cal. 08-90330MISC-RS and 08-90331MISC-RS order applications, the government did not inform the issuing magistrate that prior orders seeking related information had been applied for and issued in the District of Arizona. The applicant, AUSA Yen, did not mention in either of the Northern District of California order applications that orders from the District of Arizona (i.e., 08-3298MB-LOA and 08-7273MB-ECV) had been previously used to obtain the defendant's historical cell site location information relating to his use of the aircard. Similar to the misconduct addressed in CDTI, the government was misleading and manipulative with “its strategy of moving from district to district and judicial officer to judicial officer in pursuit of the same [or related] information, and without fully disclosing its effects elsewhere.” Comprehensive Drug Testing Inc., 621 F.3d at 1175.

“[W]hile the government is free to pursue warrants, subpoenas and other investigatory tools, and may do so in whichever judicial district is appropriate in light of the location of the information sought, it must fully disclose to each judicial officer prior efforts in other judicial fora to obtain the same or related information, and what those efforts have achieved.” Id.

d. Lack of candor in the D.Ariz. 08-3286MB-LOA order application relating to failure to advise of extensive use of illegally obtained destination IP addresses.

In the D.Ariz. 08-3286MB-LOA order application, the government did not inform the issuing magistrate that the illegally obtained destination IP addresses (sought to be obtained “retroactively”) were heavily relied upon by the government to advance its investigation.

1525. See Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008 (Dkt. #470-1 and #470-2)

1526. Had AUSA Yen informed the magistrate that historical cell site location information had already been sought and obtained in the District of Arizona, further inquiries would have likely been made regarding the exact activities the government planned to conduct while executing the Northern District of California orders. Had the magistrate been inclined to make such inquiries, and had the government responded by informing the magistrate of its plan to conduct the applicable searches and seizures, the magistrate would have seen through the government's charade and would have never issued the orders in the form that they were requested by the government.
against the defendant during the prior 26 days.[1527] The applicant, AUSA Battista, instead indicated that his supervisor “required that all of the information received by Verizon Wireless concerning destination IP addresses and information relating to the volume of the data transferred be sealed and not used in any manner in furtherance of the investigation.”[1528] Nothing in the order application properly advised the issuing magistrate of the government's extensive use of the illegally obtained destination IP addresses.

7. Consolidated “no good-faith” argument RE: mistaken understanding of the law; [applicable to all orders and subpoenas].

The orders and subpoenas that were obtained/executed by the government based on mistaken understandings of the law—causing them to be inadequate avenues for government claims of good-faith—are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Relevant order or subpoena:</th>
<th>Description of violation/circumstance precluding government claim of good-faith:</th>
<th>Sections addressing violation/circumstance:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>D.Ariz. 08-3298MB-LOA “cell site information” order;</td>
<td>(1) misunderstood and misapplied the relevant cited and/or relied upon statutes;</td>
<td>1. Section V(F)(7)(a)</td>
</tr>
<tr>
<td>4</td>
<td>D.Ariz. 08-7273MB-ECV “cell site information” order;</td>
<td>(1) misunderstood and misapplied the relevant cited and/or relied upon statutes;</td>
<td>1. Section V(F)(7)(a)</td>
</tr>
<tr>
<td>5</td>
<td>D.Ariz. 07-03-609 “destination IP address” Grand Jury subpoena;</td>
<td>(1) misunderstood and misapplied the relevant cited and/or relied upon statutes;</td>
<td>1. Section V(F)(7)(a)</td>
</tr>
<tr>
<td>6</td>
<td>D.Ariz. 07-03-615 “destination IP address” Grand Jury subpoena;</td>
<td>(1) misunderstood and misapplied the relevant cited and/or relied upon statutes;</td>
<td>1. Section V(F)(7)(a)</td>
</tr>
<tr>
<td>7</td>
<td>D.Ariz. 08-3286MB-LOA “destination IP address” order;</td>
<td>(1) misunderstood and misapplied the relevant cited and/or relied upon statutes; (2) use of “retroactive order” is not supported by applicable law;</td>
<td>1. Section V(F)(7)(a) 2. Section V(F)(7)(b)</td>
</tr>
<tr>
<td>8</td>
<td>D.Ariz. 07-03-709</td>
<td>(1) misunderstood and misapplied the relevant</td>
<td>1. Section V(F)(7)(a)</td>
</tr>
</tbody>
</table>

1527. See General Facts, Section IV(B)(1), supra (discussing factual aspects of the illegally obtained destination IP addresses).

1528. Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard (application, p. 14-15 (emphasis added)) (Dkt. #576-1, p. 15-16).
“electronic gate geolocation information” Grand Jury subpoena;
cited and/or relied upon statutes;

N.D.Cal. 08-90330MISC-RS “mobile tracking device” order;
(1) misunderstood and misapplied the relevant cited and/or relied upon statutes;
1. Section V(F)(7)(c)

N.D.Cal. 08-90331MISC-RS “Pen/Trap real-time cell site sector information” order;
(1) misunderstood and misapplied the relevant cited and/or relied upon statutes;
1. Section V(F)(7)(d)

The government cannot claim a good-faith reliance on any of the above listed orders or subpoenas considering they either cite to or rely upon statutes that are inapplicable to the related Fourth Amendment searches and seizures. In 
K
rull, the Supreme Court extended the good-faith exception to the exclusionary rule for when law enforcement seize evidence while acting in objectively reasonable reliance on a statute later found to be unconstitutional. 
K
rull, 480 U.S. 340. However, the Supreme Court expressly declined to decide whether the good-faith exception applied to “an officer who erroneously, but in good faith, believes he is acting within the scope of a statute.” Id. at 360 fn. 17. The 
K
rull court then added that extending the exception to situations where an officer violates the statute upon which he was relying “does not follow inexorably from today's decision” because “[i]n that context, the relevant actors are not legislatures or magistrates, but police officers.” Id. Additionally, the Ninth Circuit has held that an officer does not act “objectively reasonable” if “his belief [in the law] was wrong” and there “is no good-faith exception to the exclusionary rule for police who do not act in accordance with governing law.” United States v. 
T
willey, 222 F.3d 1092, 1094 (9th Cir. 2000).\[1529\] Similarly, in Warshack, 631 F.3d 266, the Sixth Circuit found that “it seems evident that an officer's failure to adhere to the boundaries of a given statute should preclude him from relying upon it in the face of a constitutional challenge[.]” id. at 289, unless “the mistakes at issue had no bearing on the constitutional violations.” Id. at 290.
See also United States v. Whiting, 781 F.2d 692, 698 (9th Cir. 1986) (Refusing to apply the

\[1529\] See also United States v. Song Ja Cha, 597 F.3d 995, 1005 (9th Cir. 2009) (same).
Leon good faith exception to an illegal search conducted by a government employee who mistakenly believed that export regulations authorized his search.). The proceeding subsections explain why the government cannot rely upon the above listed orders and subpoenas for claims of good-faith considering government actors misunderstood and misapplied each of the relevant statutes.

a. Mistaken understanding of the law relating to 18 U.S.C. § 2703 et seq. (i.e., the Stored Communications Act) as cited and/or relied upon by various orders and subpoenas.

The government cannot maintain a good-faith reliance upon the D.Ariz. 08-3286MB-LOA, 08-7273MB-ECV, and 08-3286MB-LOA orders, or upon the D.Ariz. 07-03-609, 07-03-615, and 07-03-709 Grand Jury subpoenas because they cite to and/or rely upon provisions of the Stored Communications Act (SCA), 18 U.S.C. § 2703 et seq., that are inapplicable to the Fourth Amendment searches and seizures conducted during execution of the relevant documents. The government misunderstood the SCA when it sought and obtained less-than-probable-cause orders and subpoenas, instead of probable cause warrants, as authority to conduct the Fourth Amendment searches and seizures discussed in Sections V(F)(3), (4), and (5), supra. The government obtained the three D.Ariz. orders based on 18 U.S.C. § 2703(d) and the three D.Ariz. Grand Jury subpoenas based on 18 U.S.C. § 2703(c)(2). As further explained below, the government misunderstood/misapplied 18 U.S.C. § 2703(d) and (c)(2) as authority to support the related Fourth Amendment searches and seizures and the government's misunderstanding of the law precludes application of the good-faith exception.

The SCA makes available various options for use by 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 to or customer of such service.” 18

1530. The government conceded that “the aircard tracking operation was a Fourth Amendment search and seizure.” See Government's Memorandum Re Motion For Discovery (Dkt. #674, p. 1), (footnote omitted). Additionally, the defendant identified and categorized the specific searches and seizures that occurred during execution of the orders and subpoenas relevant to this section, which are summarized in tables contained in Sections V(F)(3), (4) and (5), supra.
U.S.C. § 2703(c)(1). One available option is a mere subpoena for basic account information (see 18 U.S.C. § 2703(c)(1)(E) and (c)(2)) while another available option is an *ex parte* order for additional information based on the “specific and articulable facts” standard (see 18 U.S.C. § 2703(c)(1)(B) and (d)). However, the SCA also provides the option to obtain a Rule 41 warrant based on the probable cause standard (see 18 U.S.C. § 2703(c)(1)(A)). The warrant option contained in the SCA permits the government to obtain a record or other information under the statute even while the probable cause standard is implicated. Because the government's Fourth Amendment searches and seizures conducted during execution of the D.Ariz. orders and subpoenas implicated the probable cause standard,[1531] the government should have obtained warrants under 18 U.S.C. § 2703(c)(1)(A), as opposed to the orders and subpoenas that were obtained under 18 U.S.C. § 2703(d) and (c)(2).[1532]

Additionally, for the two D.Ariz subpoenas used to obtain the defendant's destination IP addresses (*i.e.*, 07-03-609 and 07-03-615), the relied upon 18 U.S.C. § 2703(c)(2) is plainly inapplicable. *See Procedural History, Section III(B), supra* (the government agrees that the destination IP addresses were obtained in violation of the SCA).

**b. Mistaken understanding of the law relating to the retroactive nature of the D.Ariz. 08-3286MB-LOA “retroactive order.”**

The government cannot maintain a good-faith reliance upon the D.Ariz. 08-3286MB-LOA order because the SCA provides no support for issuing “retroactive orders” intended to undo prior violations of the statute. The government obtained the D.Ariz. 08-3286MB-LOA order to unseal the destination IP addresses that were previously obtained illegally. *See Procedural History, Section III(B), supra; Argument, Section G(7)(a), supra.* However, even while attempting to correct its prior mistake, the government once again misunderstood the SCA considering it has no provision authorizing “retroactive orders”:

---

1531. *See also, Argument, Section V(G)(1), supra* (explaining how, from an objective standpoint, the agents were conducting Fourth Amendment searches and seizures without probable cause findings).

1532. For the three D.Ariz. orders, the issuing magistrates were not responsible for the errors, as the government failed to mention anywhere in the order applications that agents planned to conduct Fourth Amendment searches and seizures.
The application in this case seeks what the United States Attorney refers to as a *nunc pro tunc* order which would somehow validate retroactively the disclosure of the records to the government. The question is whether the court has the power to issue such an order. For starters, it is quite clear that the statute provides no such power. The statute is quite clear—the government can "require" a provider to "disclose" these records when the government "obtains a court order for such disclosure." 18 U.S.C. 2703(c)(1)(B). The obtaining of the court order is to preclude the disclosure of the records... There is nothing to indicate that the court has any power to issue retroactive authorizations...


The D.Ariz. 08-3286MB-LOA “retroactive order” misapplied the SCA and the government's misunderstanding of the law precludes application of the good-faith exception.

c. **Mistaken understanding of the law relating to the hybrid use of the Pen/Trap statutes and the SCA in support of the N.D.Cal. 08-90331MISC-RS order.**

The government cannot maintain a good-faith reliance upon the N.D.Cal. 08-90331MISC-RS order because it cites to provisions of the SCA that simply do not apply to the searches and seizures conducted during execution of the order. The N.D.Cal. 08-90331MISC-RS order required Verizon Wireless to provide the government with real-time cell site location information pursuant to the Pen/Trap statutes (18 U.S.C. §§ 31122 and 3123) and the SCA (18 U.S.C. §§ 2703(c)(1)(B), (c)(2) and (d)). In obtaining the order, the government did not rely solely upon the Pen/Trap statutes because the Communications Assistance For Law Enforcement Act requires that, “with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices..., such call-identifying information shall not include any information that may disclose the physical location of the subscriber...” 47 U.S.C. § 1002(a)(2) and (a)(2)(B) (emphasis added).

However, rather than supplement the Pen/Trap statutes with the required Rule 41 warrant based on probable cause, the government erroneously relied upon the SCA, 18 U.S.C. § 2703(d), and obtained a finding of “specific and articulable facts.” Because “the SCA does 1533. Combining the Pen/Trap statutes with the SCA to obtain real-time cell site location information is known as the “hybrid” or “dual” theory for cell site surveillance. See Smith (mj) 2005 Opinion, 396 F.Supp.2d at 761 (Coining the term “hybrid theory,” and noting the government's faulty argument that “cell site data enjoys a unique status under electronic surveillance law – a new form of electronic surveillance combining the advantages of the pen/trap law and the SCA [] without the respective limitations.”).

- 347 -
not seem to contemplate allowing the government to access any cell site information that
does not exist at the time the order is entered\[^{1534}\]\[1534\] the N.D.Cal. 08-90331MISC-RS order
misapplied the SCA and the government's misunderstanding of the law precludes application
of the good-faith exception.\[^{1535}\]\[1535\]

d. Mistaken understanding of the law relating to 18 U.S.C. §§
2703 and 3117, and 28 U.S.C. § 1651 as cited by the N.D.Cal.
08-90330MISC-RS order.

In the effect that the N.D.Cal. 08-90330MISC-RS order cites Rule 41(b), Fed. R.
Crim. P., it was previously explained how the order fails from numerous angles if analyzed
as a warrant.\[^{1536}\]\[1536\] The government also cannot maintain a good-faith reliance upon the other
cited statutes, i.e., 18 U.S.C. §§ 2703 and 3117, and 28 U.S.C. § 1651, considering they
conjure no replacement authority for a warrant and otherwise have contradicting provisions.
First, the All Writs Act, 28 U.S.C. § 1651, cannot be used as a replacement for a probable
cause warrant. “The government simply cannot use the All Writs Act to circumvent the
requirements of the Fourth Amendment and other statutes that already occupy the
space.”\[^{1537}\]\[1537\] Under the same reasoning, the SCA, 18 U.S.C. § 2703, and the tracking device

1534. In The Matter Of The Application Of The United States Of America For An Order
Authorizing The Installation And Use Of A Pen Register And A Caller Identification System
On Telephone Numbers [Sealed] And [Sealed] And The Production Of Real Time Cell Site
Information, 402 F.Supp.2d 597, 604 fn. 11 (D.Md. 2005); see also In The Matter Of The
Application Of United States Of America For An Order Authorizing (1) Installation And Use
Of A Pen Register And Trap And Trace Device Or Process, (2) Access To Customer Records,
And (3) Cell Phone Tracking, 441 F.Supp.2d 816, 837 (S.D.Tex. 2006) (“The constitutional
difficulties of the dual theory for cell site surveillance are inherent.”); In The Matter Of The
Application Of The United States Of America For An Order Authorizing The Installation
And Use Of A Pen Register Device, A Trap And Trace Device, And For Geographic Location
Information, 497 F.Supp.2d 301, 312 (P.R. 2007) (“Congress has not authorize disclosure of
cell site information in the statutes proffered by the government – namely the Pen Register
Statute combined with the SCA.”).

1535. Seemingly realizing the limitations of the SCA, the government also sought and
obtained the “after receipt and storage” directive contained in the order. Such a directive has
been rejected by prior courts. See, e.g., Orenstein (mj) 2005 Opinion, 396 F.Supp.2d at 314.
Nevertheless, the government failed to comply with the “after receipt and storage” directive
during execution of the order. See Argument, Section V(F)(2)(c)(ii), supra.

1536. See Argument, Section V(F)(1) et seq., supra.

1537. In The Matter Of An Application Of The United States Of America For An Order
Authorizing Disclosure Of Location Information Of A Specified Wireless Telephone, No. 10-
the All Writs Act and Fourth Amendment in detail).
statute, 18 U.S.C. § 3117, cannot be used as a replacement for Fourth Amendment requirements. Second, the statutes cited in the order, 18 U.S.C. § 2703 and 18 U.S.C. § 3117, do not at all complement one another. Such a combination of statutes is entirely nonsensical considering, the SCA, 18 U.S.C. § 2703 et seq., defines “electronic communications” to expressly exclude “any communication from a tracking device (as defined in section 3117 of this title).”[1538] Because the statutes cited in the N.D.Cal. 08-90331MISC-RS order are not replacements for a probable cause warrant, and because 18 U.S.C. § 2703 and 18 U.S.C. § 3117 otherwise cannot be used together, the statutes were misapplied and the government's misunderstanding of the law precludes application of the good-faith exception.

VI. [Conclusion:] Exclusion is an appropriate remedy for the various Fourth Amendment violations and all illegally obtained evidence and derivative evidence must be suppressed.

In support of his request for suppression, the defendant identified and explained numerous Fourth Amendment violations including scope violations, particularity violations, lack of probable cause findings, failure to obtain warrants, Rule 41 violations,[1539] general


1539. There are three circumstances upon which evidence obtained in violation of Rule 41, Fed. R. Crim. P., requires suppression:

1) the violation rises to a “constitutional magnitude;” 2) the defendant was prejudiced, in the sense that the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule; or 3) officers acted in “intentional and deliberate disregard” of a provision in the Rule.

United States v. Williamson, 439 F.3d 1125, 1132 (9th Cir. 2006) (citation omitted).

However, shortly after Williamson, the Hudson case was decided wherein the Supreme Court refused to exclude evidence to remedy a violation of judicially created policy, i.e., the knock-and-announce rule, because the “violation was not the un attenuated but-for cause of obtaining the evidence.” United States v. Hector, 474 F.3d 1150, 1154 (9th Cir. 2007) (paraphrasing Hudson v. Michigan, 547 U.S. 586 (2006)). If extended to Rule 41 violations, Hudson eliminated Williamson circumstance Nos. 1 and 3, and now requires that circumstance No. 2 absolutely be met in order for suppression to remain an adequate remedy under Williamson post Hudson. However, Hudson did not specifically address violations of Rule 41, “which reflects the Fourth Amendment’s policy [(as opposed to judicially created policy)] against unreasonable searches and seizures[].” Zurcher, 436 U.S. at 558 (emphasis added) (internal quotation marks, brackets, and citation omitted); see also United States v.
unreasonableness, and many others. All Fourth Amendment violations addressed in this memorandum are unattenuated but-for causes of obtaining the evidence sought to be suppressed. The defendant also explained how the good-faith exception to the exclusionary rule is plainly inapplicable to the circumstances upon which the government's flagrant misconduct violated the defendant’s Fourth Amendment rights. As an adequate remedy, the defendant requests that all illegally obtained evidence be suppressed including (1) wholesale destination IP addresses, (2) communications content and other private information derived from destination IP addresses, (3) historical cell site location information, (4) real-time cell site location information, (5) real-time geolocation data obtained from Verizon Wireless, (6) aircard signals collected by the FBI over the air interface, (7) aircard geolocation data obtained by the FBI directly, (8) historical electronic gate location information, (9) the location of the aircard and the defendant as information

Butts, 357 Fed. Appx. 850 (9th Cir. 2009) (analyzing Rule 41 violation without any mention of Hudson). Nevertheless, regardless of how the Court wishes to apply Hudson, the defendant explained how all Rule 41 violations occurred under all three Williamson circumstances. See Argument, Section V(G)(5), supra (table listing sections where Rule 41 violations are analyzed supra).

1540. See Hudson, 547 U.S. at 592-93 (suppression merited when violation is unattenuated but-for causation of obtaining evidence sought to be suppressed). For scope, particularity, lack of probable cause, warrantless searches/seizures, and similar fundamental constitutional violations, unattenuated but-for causality is inherent. Other violations explained throughout this memorandum, e.g., Rule 41 violations and failure to adhere to terms and limitations contained in issued orders, are supplemented with additional analyses in support of “unattenuated but-for causality” in the Argument, Section V(F) et seq., supra.

1541. The defendant is not only requesting that the destination IP addresses revealing of his home web browsing be suppressed, he is also requesting suppression of destination IP addresses later matched to those allegedly used to e-file fraudulent tax returns. The doctrine of severance is applied by “follow[ing] the rule that where invalid portions of a warrant may be stricken and the remaining portions held valid, seizures pursuant to the valid portions will be sustained. That doctrine requires, however, that identifiable portions of the warrant be sufficiently specific and particular to support severance.” Spilotro, 800 F.2d at 967. In the present case, the destination IP address subpoenas and order do not meet the requirements for severance. The subpoenas and order do not list the specific destination IP addresses associated with the allegedly fraudulent e-filed tax returns. See Argument, Section V(F)(4)(b), supra. The government had a list of specific destination IP addresses related to alleged criminal activity prior to obtaining the subpoenas and order but made no effort to narrow the scope of the records sought. See id. Just like the entirely invalid warrant in Cardwell, the subpoenas and order in the present case “do[ ] not refer to specific records, either in terms of the their character or date[, t]herefore, [severance does not apply and] all materials seized under the defective warrant should be suppressed.” United States v. Cardwell, 680 F.2d 75, 79 (9th Cir. 1982).
obtained by the government, (10) ESN data downloaded from the aircard by the FBI, and
(11) all other information and physical evidence obtained as a result of the illegal searches
and seizures conducted by the government.\[^{1542}\] The remainder of this section provides
reasons as to why the “deterrence benefits [of suppression] outweigh its 'substantial social
costs[.]’” Hudson, 547 U.S. at 591 (internal citation omitted).

During oral arguments before the Supreme Court in United States v. Jones\[^{1543}\]—a
recent case addressing warrantless GPS tracking of vehicles on public streets—Justice Scalia
abruptly interrupted the government's ramblings to ask a very important question: “Don't we
have any legislatures out there that could stop this stuff?”\[^{1544}\] Unfortunately, the answer to
that question is as much “no” for the geolocation surveillance at issue in the present case as
it is for the GPS surveillance at issue in Jones. Although Congress has introduced three
separate bills addressing locational privacy,\[^{1545}\] nothing has been passed into law that
would prevent the types of government abuses addressed in this memorandum. In fact,

\[^{1542}\] The geolocation information obtained by the government ultimately led to the in-
person search of apartment No. 1122 via the N.D.Cal. 08-70460-HRL/PVT warrant, which in
turn led to all subsequent searches and seizures based on the additional warrants
listed/referenced in row No. 13 within the “evidence table” at the end of this section. The
geolocation information also ultimately led the government to other evidence based on
investigations not involving warrants, as referenced in row No. 14 within the “evidence
table” at the end of this section.


\[^{1544}\] United States v. Jones, Supreme Court of the United States, No. 10-1259 (Nov. 8,
2011), Transcripts of Oral Argument [JUSTICE SCALIA], p. 25, ln. 22-23, available at
http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf (last
accessed: Jan. 5, 2012); see also

\[^{1545}\] “In particular, Senator Ron Wyden and Representative Jason Chaffetz introduced
identical legislation, S. 1212 and H.R. 2168, the Geolocational Privacy and Surveillance Act
(GPS bill), which would make it unlawful for a service provider to disclose a person’s
location unless law enforcement obtained a warrant based upon probable cause or one of the
limited exceptions applies. Senator Al Franken has introduced the Location Privacy and
Protection Act of 2011 (S. 1223)—similar to the GPS bill, but which applies only to private,
not governmental, actors. Senator Patrick J. Leahy has introduced the Electronic
Communications Privacy Act Amendment Act of 2011 (S. 1011), which not only includes a
warrant requirement for geolocation information, but also overhauls and updates other
provisions of federal electronic surveillance law.” Thompson, Richard M., Congressional
Research Service, Government Tracking of Cell Phones and vehicles: The Confluence of
Congress has not done much of anything since the defendant's arrest in August of 2008.[1546] Certainly to no surprise, in January of 2012, an ABC News/Washington Post poll revealed that Congress had the lowest approval rating since 1974—a striking 13%.[1547] Equally unavailing is any expectation of positive change from our government's executive branch. During a hearing before the second session of the 111th Congress, Marc J. Zwillinger responded to a question on whether DOJ policy addressing locational privacy is binding upon federal agents and U.S. attorneys:

Mr. ZWILLINGER. Can I comment briefly on that? As someone who represents providers, I frequently get requests from and subpoenas and other legal process from U.S. attorneys’ offices around the country, and I am the one typically telling them that, you know, that what you have done is in violation of DOJ policy. And sometimes I hear back, “Oh, do you mean those folks in Washington?” To which I say, “Yes, and you should call them.” And they say, “Well, our boss is a U.S. attorney, and he has been confirmed by the Senate, and we will do things the way we do things.” So to rely on DOJ policy to prevent prosecutors from doing things that we would think that the law would prevent them from doing is somewhat dangerous, and it puts a lot of burden on ISPs and providers to make sure that government isn’t doing what it shouldn’t be doing.


Additionally, it was confirmed by the prosecution in the present case that the specific type of misconduct involved in the aircard locating mission is routine and widespread—a circumstance weighing towards suppression. See Herring, 129 S.Ct. at 704. When asked by the Court “how was it that the government was able to get [][the N.D.Cal. 08-90330MISC-}
RS] order... without disclosing the technology to the court?,” AUSA Battista responded that “it was a standard practice,... [t]his wasn't a unique scenario, [t]his particular style of order had been sought before, before the magistrates.” The government also continues to maintain that it can operate wireless device locators using mere Pen/Trap orders—a further circumstance weighing towards suppression. See Herring, 129 S.Ct. at 704 (suppression merited if government shows “reckless disregard of constitutional requirements...").

Neither the legislative branch nor executive branch provide much hope for implementing an adequate solution to protect locational privacy. Luckily, our Founding Fathers designed the United States government as a three branch system that operates on a series of checks and balances. In line with our Founding Fathers' vision of maintaining liberty, the Court must check both the legislative branch and executive branch for failing to protect the people's right to be free from abusive government intrusions involving locational privacy. At the very least, such Court action will deter the executive branch from engaging in similar abuses in the future—a goal squarely in line with the Supreme Court's application of the exclusionary rule. Therefore, the defendant respectfully requests that


1550. See Government's Memorandum Re Motion For Discovery (Dkt. #674, p. 1 fn. 1 and p. 2 fn. 2) (Although concessions were made in the present case in order to resolve discovery issues, it is still the general position of the government that “the use of the cell site simulator is not a search under the Fourth Amendment.... Again, the United States’ position is that the hybrid order [(i.e., combination order for Pen/Trap device and stored records under SCA)] confers sufficient authority to use a cell site simulator and that a tracking warrant is unnecessary.”).

1551. To be clear, in addition to standard exclusionary rule arguments, the defendant is also raising the novel argument that suppression is merited as a remedy for Congress' failure to act upon any of its proposed locational privacy bills that would otherwise prevent many of the Fourth Amendment violations at issue in the present case. By ordering evidence suppressed, the Court will ultimately achieve what Congress attempted to achieve but failed. Such a ruling will act as an interim solution until Congress can thoroughly address the issue by working together to pass relevant changes to the United States Code.

1552. Suppression is a “remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved.” Leon, 468 U.S. at 906 (citation omitted).
the Court suppress the following evidence obtained illegally in this case:

**Evidence Table**

<table>
<thead>
<tr>
<th>#</th>
<th>Evidence sought to be suppressed:</th>
<th>Relevant order or subpoena executed while evidence was seized:</th>
<th>Sections addressing evidence:</th>
</tr>
</thead>
</table>
| 1 | The defendant's 1.8 million destination IP addresses relating to use of the aircard; | (1) D.Ariz. 07-03-609 Grand Jury subpoena; (2) D.Ariz. 07-03-615 Grand Jury subpoena; (3) D.Ariz. 08-3286MB-LOA order; | 1. Section V(F)(4)  
2. Section V(F)(4)  
3. Section V(F)(4) |
| 2 | Communications content and other private information derived from destination IP addresses; | (1) D.Ariz. 07-03-609 Grand Jury subpoena; (2) D.Ariz. 07-03-615 Grand Jury subpoena; (3) D.Ariz. 08-3286MB-LOA order; | 1. Section V(F)(4)  
2. Section V(F)(4)  
3. Section V(F)(4) |
| 3 | Historical cell site location information relating to aircard; | (1) D.Ariz. 08-3298MB-LOA order; (2) D.Ariz. 08-7273MB-ECV order; | 1. Section V(F)(3)  
2. Section V(F)(3) |
<p>| 4 | Real-time cell site location information relating to the aircard; | (1) N.D.Cal. 08-90331MISC-RS order; | 1. Section V(F)(2) |
| 5 | Real-time aircard geolocation information (obtained by FBI from Verizon Wireless); | (1) N.D.Cal. 08-90330MISC-RS order; | 1. Section V(F)(1) |
| 6 | Location finding response signals transmitted by aircard (obtained by FBI directly); | (1) N.D.Cal. 08-90330MISC-RS order; | 1. Section V(F)(1) |
| 7 | Geolocation data showing the location of the aircard and the defendant inside apartment No. 1122 (obtained by FBI directly); | (1) N.D.Cal. 08-90330MISC-RS order; | 1. Section V(F)(1) |
| 8 | Historical geolocation information via Domicilio electronic gate key access records; | (1) D.Ariz. 07-03-709 Grand Jury subpoena; | 1. Section V(F)(5) |</p>
<table>
<thead>
<tr>
<th></th>
<th>Location of the aircard and the defendant inside apartment No. 1122 (as information obtained by the government);</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>(1) D.Ariz. 08-3298MB-LOA order; (2) D.Ariz. 08-7273MB-ECV order; (3) N.D.Cal. 08-90331MISC-ECV order; (4) N.D.Cal. 08-90330MISC-ECV order; (5) D.Ariz. 07-03-709 Grand Jury subpoena;</td>
<td>1. Section V(F)(3)</td>
<td>2. Section V(F)(3)</td>
</tr>
<tr>
<td></td>
<td>(1) D.Ariz. 08-3298MB-LOA order; (2) D.Ariz. 08-7273MB-ECV order; (3) N.D.Cal. 08-90331MISC-ECV order; (4) N.D.Cal. 08-90330MISC-ECV order; (5) D.Ariz. 07-03-709 Grand Jury subpoena;</td>
<td>3. Section V(F)(2)</td>
<td>4. Section V(F)(1)</td>
</tr>
<tr>
<td>10</td>
<td>ESN data stored on aircard's internal storage device (obtained by FBI directly);</td>
<td>(1) N.D.Cal. 08-90330MISC-ECV order;</td>
<td>5. Section V(F)(5)</td>
</tr>
<tr>
<td>11</td>
<td>All other evidence illegally obtained while executing challenged orders and subpoenas;</td>
<td>(1) D.Ariz. 08-3298MB-LOA order; (2) D.Ariz. 08-7273MB-ECV order; (3) N.D.Cal. 08-90331MISC-ECV order; (4) N.D.Cal. 08-90330MISC-ECV order; (5) D.Ariz. 07-03-709 Grand Jury subpoena; (6) D.Ariz. 07-03-609 Grand Jury subpoena; (7) D.Ariz. 07-03-615 Grand Jury subpoena; (8) D.Ariz. 08-3286MB-LOA order;</td>
<td>1. Section V(F)(3)</td>
</tr>
<tr>
<td>12</td>
<td>Information obtained as a result of the warrantless keyhole search of apartment No. 1122;</td>
<td>(1) N/A;</td>
<td>3. Section V(F)(2)</td>
</tr>
<tr>
<td>13</td>
<td>All derivative evidence, i.e., fruits-of-the-poisonous-tree, stemming from all other warrants;</td>
<td>(1) N.D.Cal. 08-70460-HRL warrant; (2) N.D.Cal. 08-70460-PVT warrant; (3) N.D.Cal. 08-70503-PVT warrant; (4) N.D.Cal. 08-70502-PVT warrant; (5) E.D.Cal. 08-SW-0586-EBD warrant; (6) D.Ariz. 08-3397MB-LOA warrant; (7) D.Ariz. 08-3399MB-LOA warrant; (8) D.Ariz. 08-3401MB-LOA; (9) D.Ariz. 08-3403MB-LOA warrant; (10) D.Ariz. 08-3402MB-LOA warrant; (11) D.Ariz. 08-3398MB-LOA warrant; (12) D.Ariz. 08-6038MB-DKD warrant; (13) D.Ariz. 09-7124MB-ECV warrant; (14) all other warrants stemming for the location of the aircard;</td>
<td>1-14. N/A – See footnote No. 1541, supra;</td>
</tr>
<tr>
<td>14</td>
<td>All derivative evidence, i.e., fruits-of-the-poisonous-tree, stemming from investigations not involving warrants;</td>
<td>(1) N/A;</td>
<td>1. N/A – See footnote No. 1541, supra;</td>
</tr>
</tbody>
</table>

* This memorandum was researched, prepared, and drafted by Daniel David Rigmaid, pro se. - June 1, 2012;