

February 10, 2012

VIA FACSIMILE (540) 868-4977

David M. Hardy

Chief, Record/Information Dissemination Section, Records Management Division

170 Marcel Drive

Winchester, VA 22602-4843

(540) 868-4500 (Telephone)

(540) 868-4997 (Fax)

Re: Freedom of Information Act Request and Request for Expedited Processing

Dear Mr. Hardy:

This letter constitutes a request under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center (“EPIC”). As detailed below, EPIC seeks agency records concerning cell site simulator and other cell phone tracking technologies deployed by the Federal Bureau of Investigation (“FBI”) to covertly locate, target, and track targets of interest.

Factual Background

On July 23, 2008 Daniel David Rigmaiden was indicted on various counts of conspiracy, wire fraud, and identity theft by U.S. Attorneys in Phoenix, Arizona.¹ Rigmaiden was located after “federal agents used a stingray to track a mobile device to an apartment building.”² A StingRay is a device that can triangulate the source of a cellular signal by acting “like a fake cell phone tower” and measuring the signal strength of an identified device from several locations.³

Defendant Rigmaiden has submitted various discovery motions seeking information about the investigatory techniques used to locate him.⁴ In opposition to one such motion, the Department of Justice submitted a memorandum, dated October 27, 2011, by the FBI’s Supervisory Special agent who stated that all data from stingray-type devices are deleted because the devices may tend to pick up information “from all

¹ *United States v. Rigmaiden*, CR 08-814-PHX-DGC, 2010 WL 3463723 (D. Ariz. Aug. 27, 2010).

² Jennifer Valentino-Devries, *Feds Shift Tracking Defense*, THE WALL STREET JOURNAL, Nov. 3, 2011, available at <http://online.wsj.com/article/SB10001424052970204621904577014363024341028.html>.

³ *Department of Justice Neuters Fourth Amendment with StingRay Ruling*, TECHANDFILM, Nov. 6, 2011, available at <http://techandfilm.wordpress.com/2011/11/06/department-of-justice-neuters-fourth-amendment-with-stingray-ruling/>.

⁴ *Id.*

wireless devices in the immediate area of the FBI device that subscribe to a particular provider ... including those of innocent, non-target devices.”⁵

In support of its October 27, 2011 memorandum, the U.S. Attorneys submitted the affidavit of supervisory special agent Bradley S. Morrison.⁶ Agent Morrison is the Unit Chief of the Tracking Technology Unit (TTU), Traditional Technology Section, Operational Technology Division in Quantico, Virginia.⁷ As such, Agent Morrison is responsible for the “development, procurement and deployment of technical assets and capabilities to covertly locate, tag and track targets of interest in support of all FBI investigative, intelligence collection and operational programs.”⁸ Agent Morrison’s affidavit stated that:

FBI policy requires that at the conclusion of a location operation, FBI technical personnel are to purge all data stored in the [tracking device]. During a local operation, the electronic serial numbers (ESNs) (or their equivalent) from all wireless devices in the immediate area of the FBI device that subscribe to a particular provider may be incidentally recorded, including those of innocent, non-target devices.⁹

As the court documents submitted by the Government in *US v. Rigmaiden* make clear, the FBI currently uses “cell site simulator” technologies such as StingRay to “locate, tag and track.”¹⁰ These devices were procured from third party vendors, which would require contracts and/or statements of work. The devices presumably have related technical documents and descriptions of operational requirements. Given the potential impact on “innocent, non-target devices,” and the requirements of the E-Government Act of 2002, the agency is obligated to conduct a Privacy Impact Assessment (“PIA”) before using these devices . As the Department of Justice PIA Official Guidance book describes:

Section 208 of the E-Government Act of 2002 requires all federal agencies to conduct a PIA before developing or procuring information technology that collects, maintains, or disseminates information that is in identifiable form or before initiating a new collection of information that will be collected, maintained, or disseminated using information technology and that includes any information in identifiable form in certain circumstances involving the public.¹¹

⁵ Affidavit of Supervisory Special Agent Bradley S. Morrison, *US v. Rigmaiden*, No. 08-cr—00814 at *3 (D. Ariz. Oct. 27, 2011).

⁶ *Id.* at *1.

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.* (“As the Unit Chief of the TTU, I am responsible for the development, procurement and deployment of technical assets and capabilities to covertly *locate, tag, and track* targets of interest in support of all FBI investigative, intelligence collection and operational programs.”).

¹¹ OFFICE OF PRIVACY AND CIVIL LIBERTIES, UNITED STATES DEPARTMENT OF JUSTICE, PRIVACY IMPACT ASSESSMENTS – OFFICIAL GUIDANCE (Revised August 2010), *available at* http://www.justice.gov/opcl/pia_manual.pdf.

Because the “[Government’s] position continues to be that, as a factual matter, the [aircard tracking] operation did not involve a search or seizure under the Fourth Amendment,”¹² and because Special Agent Morrison insists that the equipment qualifies as “a pen register/trap and trace device, as defined in 18 U.S.C. §§ 3127(3) and (4),”¹³ it is likely that the FBI or another office has issued a legal basis memorandum regarding the use of cell site simulator technology.

Documents Requested

EPIC requests copies of the following agency records in possession of the ___:

1. All documents concerning technical specifications of the StingRay device or other cell site simulator technologies.
2. All documents concerning procedural requirements or guidelines for the use of StingRay device or other cell site simulator technologies (e.g. configuration, data retention, data deletion).
3. All contracts and statements of work that relate to StingRay device or other cell site simulator technologies.
4. All memoranda regarding the legal basis for the use of StingRay device or other cell site simulator technologies.
5. All Privacy Impact Assessments or Reports concerning the use or capabilities of StingRay device or other cell site simulator technologies.

Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information . . .” and it pertains to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity.” 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).

EPIC is “primarily engaged in disseminating information.” *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

There is a particular urgency for the public to obtain information about location tracking technology, given the heated debate surrounding the recent US Supreme Court decision, *US v. Jones*, holding unanimously that the use of a GPS Tracking Device was a Fourth Amendment search requiring a warrant. *United States v. Jones*, 565 U.S. ____ (2012). The public’s interest in and desire for information about the Government’s

¹² Government Memorandum re Motion for Discovery, *US v. Rigmaiden*, No. 08-cr—00814 at *1 n.1 (D.Ariz Oct. 27, 2011).

¹³ Affidavit of Supervisory Special Agent Bradley S. Morrison, *US v. Rigmaiden*, No. 08-cr—00814 at *3 (D. Ariz. Oct. 27, 2011).

tracking activities is reflected in the sheer volume of news coverage that *Jones* and related cases have received in the last six months. For examples, see EPIC: US v. Jones.¹⁴

Request for “News Media” Fee Status

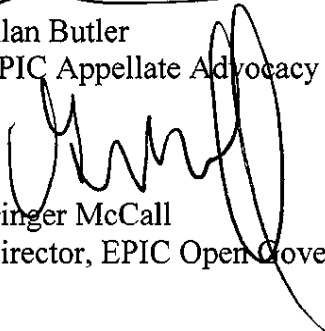
EPIC is a “representative of the news media” for fee waiver purposes. *EPIC v. Department of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on our status as a “news media” requester, we are entitled to receive the requested record with only duplication fees assessed. Further, because disclosure of this information will “contribute significantly to public understanding of the operations or activities of the government,” any duplication fees should be waived.

Thank you for your consideration of this request. As provided in 6 C.F.R. § 5.5(d)(4), I will anticipate your determination on our request for expedited processing within ten (10) calendar days.

Respectfully Submitted,



Alan Butler
EPIC Appellate Advocacy Fellow



Ginger McCall
Director, EPIC Open Government Project

¹⁴ Available at <http://epic.org/amicus/jones/>.

Exhibit 1

1 ANN BIRMINGHAM SCHEEL
United States Attorney
District of Arizona

2
3 FREDERICK A. BATTISTA
Maryland State Bar Member
PETER S. SEXTON
Arizona State Bar No. 011089
4 JAMES R. KNAPP
Arizona State Bar No. 021166
5 Assistant U.S. Attorneys
Two Renaissance Square
40 North First Avenue, Suite 1200
6 Phoenix, Arizona 85004
Telephone: (602) 514-7500
7 Fred.Battista@usdoj.gov
Peter.Sexton@usdoj.gov
James.Knapp2@usdoj.gov

8 UNITED STATES DISTRICT COURT
9 DISTRICT OF ARIZONA

10 United States of America,
11
12 Plaintiff,
13
14 v.
15 Daniel David Rigmaiden, et al.,
16 Defendant.

No. CR-08-0814-PHX-DGC

**GOVERNMENT'S MEMORANDUM
RE MOTION FOR DISCOVERY**

16 The United States, through undersigned counsel, submits this Memorandum in an attempt
17 to clarify and narrow some issues for the upcoming October 28, 2011, hearing regarding
18 Defendant's Motion for Discovery.

19 First, the United States proposes that the Court assume, arguendo, for Defendant's Motion
20 for Discovery and any forthcoming motion to suppress, that the aircard tracking operation was
21 a Fourth Amendment search and seizure. ^{1/}

22
23 ^{1/} The United States' position continues to be that, as a factual matter, the operation did
24 not involve a search or seizure under the Fourth Amendment. The United States explained in
25 its March 11, 2011, Memorandum Regarding Law Enforcement Privilege that Defendant does
26 not have a reasonable expectation of privacy in his general location or in the cell site records he
27 transmitted wirelessly to Verizon. (CR 465 at 13-17.) Therefore, the use of the cell site
28 simulator is not a search under the Fourth Amendment. See, e.g., Smith v. Maryland, 442 U.S.
735, 740 (1979) ("application of the Fourth Amendment depends on whether the person
invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of
privacy' that has been invaded by government action"). Nevertheless, in an attempt to simplify
the analysis and to avoid unnecessary disclosure of privileged information, the United States will

(continued...)

1 Second, the United States agrees to rely solely on the Rule 41 tracking warrant,
2 application, and affidavit, No. CR08-90330-MISC, to authorize the use of equipment to
3 communicate directly with Defendant's aircard and determine its location. ^{2/}

4 Third, the United States will agree to allow the Court to factually assume, that, at the
5 conclusion of the July 16, 2008, aircard tracking operation, the FBI located the aircard within
6 Unit 1122 of the Domocilio Apartments. ^{3/}

7 Fourth, with respect to whether the equipment used to locate the aircard was operated in
8 a "man in the middle" manner or caused a brief "disruption of service," the United States will
9 agree that the Court can assume, arguendo, that it did. ^{4/}

10 Fifth, for the purpose of defendant's pending motion(s) to compel discovery and his
11 prospective motion to suppress, the United States does not expect to present facts in any in
12 camera proceeding that it would then request the Court to consider for the purpose of rebutting
13 any of defendant's claims without disclosing those facts to the defendant.

14
15 _____
16 ^{1/} (...continued)
17 no longer argue in this case only that the aircard tracking operation was not a search or seizure
18 under the Fourth Amendment, and will instead rely on its authority under the hybrid order and
19 tracking warrant, Defendant's lack of standing, and, if necessary, the agents' good faith reliance
20 on these court orders.

21 ^{2/} Again, the United States' position is that the hybrid order confers sufficient authority
22 to use a cell site simulator and that a tracking warrant is unnecessary. Nevertheless, the United
23 States will rely solely on the Rule 41 warrant application, affidavit and order in this case to
24 authorize its use of a cell site simulator. The hybrid order, No. CR08-90331-MISC, will be used
25 to justify obtaining cell site and other non-content information from Verizon Wireless.

26 ^{3/} This is not, in fact, accurate. As explained previously, the FBI was only able to
27 narrow the aircard down to three or four apartments. But to avoid disclosure of privileged
28 information and simplify the Fourth Amendment analysis, the United States will concede, for
purposes of any forthcoming motion to suppress, that the FBI located the aircard within Unit
1122 of the Domocilio Apartments.

^{4/} The United States indicated at the September 22, 2011, hearing that it believed "the
simulator in this case was taking the message it received from the aircard and sending it on to
a Verizon tower." (RT 9/22/2011 (CR 637) at 61:5-8.) As FBI Agent Bradley Morrison
clarifies in the attached affidavit, however, the equipment did not capture any content and it did
not act as a "man in the middle," collecting data and passing it along to Verizon Wireless.
(Morrison Aff. 2-3 ¶ 4.)

1 Finally, the United States is submitting a sworn affidavit from Bradley Morrison, the Unit
2 Chief of the FBI Tracking Technology Unit, to describe facts regarding the aircard tracking
3 operation and clarify some remaining factual issues. The United States will make Agent
4 Morrison available ex parte and in camera to answer questions the Court may have about the
5 tracking operation and the equipment used. In addition, the United States will make this
6 individual available for testimony at any future suppression hearing, so long as the United States
7 has an opportunity to file a motion in limine in order to seek to limit cross-examination regarding
8 privileged law enforcement sensitive material. In order to proceed in this fashion, the United
9 States requests an opportunity to explain, in camera, the basis for its claims of privilege.

10 Respectfully submitted this 27th day of October, 2011.

11 ANN BIRMINGHAM SCHEEL
12 Acting United States Attorney
13 District of Arizona

14 S/Frederick A. Battista

15 FREDERICK A. BATTISTA
16 PETER S. SEXTON
17 JAMES R. KNAPP
18 Assistant U.S. Attorneys
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I hereby certify that on October 27, 2011, I caused the attached document to be electronically transmitted to the Clerk's Office using the ECF system for filing and transmittal of a Notice of Electronic Filing to the following ECF registrants:

Philip Seplow
Shadow Counsel for Defendant Daniel David Rigmaiden

Taylor Fox
Counsel for Defendant Ransom Carter

A copy of the attached document was also mailed to:

Daniel David Rigmaiden
Agency No. 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132

S/James Knapp

Exhibit 2

AFFIDAVIT OF SUPERVISORY SPECIAL AGENT
BRADLEY S. MORRISON

1. I, Bradley S. Morrison, am a Supervisory Special Agent with the Federal Bureau of Investigation. I am assigned as the Unit Chief of the Tracking Technology Unit (TTU), Traditional Technology Section, Operational Technology Division in Quantico, Virginia. I have been an FBI Special Agent since 1996. As the Unit Chief of the TTU, I am responsible for the development, procurement and deployment of technical assets and capabilities to covertly locate, tag and track targets of interest in support of all FBI investigative, intelligence collection and operational programs. As part of these duties, I am responsible for overseeing deployment and monitoring policy compliance governing the FBI's use of equipment to locate cellular devices.

2. On July 16, 2008, 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. The actual make and model of the equipment used in any particular operation by the FBI is law enforcement sensitive, and pursuant to FBI policy, cannot be released to the general public.

3. As a pen register/trap and trace device, as defined in 18 U.S.C. §§ 3127(3) and (4), the equipment used in this case can only record, decode or capture electronic impulses which identify the originating number of a source of electronic communications, or other

dialing, routing, signaling and addressing information utilized in the processing and transmitting of electronic communications. To comply with the legal definition of a pen register/trap and trace device, the equipment used in this case is unable to upload, encode or write any information to a target device. If the equipment were capable of these functions, it would no longer be in compliance with the statutory definition of a pen register/trap and trace device. Therefore, the equipment used in this case is technologically unable to take any action to reprogram the hardware or software in the aircard or the defendant's laptop.

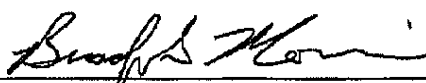
4. Further, 18 U.S.C. §§ 3127(3) and (4) specifically prohibit pen register or trap and trace devices from recording, decoding or capturing the substantive content of any communication. Were the equipment to do this, by statute, it would no longer be a pen register/trap and trace device. Instead, it would be an electronic intercept device regulated by Title III. To ensure that the content of communications is not intercepted, in accordance with 18 U.S.C. §3121(c), all pen register/trap and trace devices used by government agencies must be restricted from recording or decoding any data or impulses not strictly related to the dialing, routing, signaling or addressing information utilized in the processing or transmitting of wire or electronic communications. The equipment used in this case was in compliance with the requirements of the statutes cited above. Therefore, the pen register/trap and trace 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.

5. FBI policy requires that at the conclusion of a location operation, FBI technical personnel are to purge all data stored in the pen register/trap and trace equipment. During a location operation, the electronic serial numbers (ESNs) (or their equivalent) from all wireless devices in the immediate area of the FBI device that subscribe to a particular provider may be incidentally recorded, including those of innocent, non-target devices. Purging is done by the FBI as an additional, internal procedural safeguard to ensure (1) that the privacy rights of those innocent third parties are maintained, (2) that the FBI does not store or maintain pen register/trap and trace data beyond the scope of its legal authorization, or (3) that the FBI does not collect information about individuals who are not the subject of criminal or national security investigations.

6. I declare under penalty of perjury that the foregoing facts are true and correct.

10/27/11
Date


Bradley S. Morrison
Supervisory Special Agent
FBI

