Daniel J. Pochoda (SBA 021979)
Kelly J. Flood (SBA 019772)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF ARIZONA
3707 N. 7th Street, Suite 235
Phoenix, AZ 85014
Telephone: (602) 650-1854
dpochoda@acluaz.org
kflood@acluaz.org

Linda Lye*
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm St., 2nd Floor
San Francisco, California 94111
Telephone (415) 621-2493
llye@aclunc.org

Hanni M. Fakhoury*
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x. 117
hanni@eff.org

**Application for admission pro hac vice pending*
Additional counsel listed on signature page

Attorneys for Proposed *Amici Curiae*

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>DANIEL RIGMAIDEN,<br><br>Defendant. | CASE NO.: 2:08-CR-00814-DGC<br><br>**[PROPOSED] BRIEF *AMICI CURIAE* IN SUPPORT OF DANIEL RIGMAIDEN'S MOTION TO SUPPRESS**<br><br>**ORAL ARGUMENT REQUESTED** |

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

### FEDERAL CASES

**STATE CASES**



**OTHER AUTHORITIES**

**STATUTES**

## I. INTRODUCTION AND SUMMARY OF ARGUMENT

This case will likely result in the first decision to address the constitutional implications of a so-called "stingray" device, which locates and identifies wireless devices in its vicinity and can be used for other forms of surveillance. The government concedes that the device located Mr. Rigmaiden within his home and its use constituted a search, but contends that he lacked a reasonable privacy expectation because he purchased his aircard under an alias, and the search was conducted pursuant to a proper warrant. *Amici* explain why these two arguments have dramatic constitutional implications and must be rejected. In addition, *amici* discuss several salient aspects of the surveillance technology used here. Finally, *Amici* explain why the government's separate location tracking effort through the collection of 38 days of cell site location information constituted a Fourth Amendment search.

Stingrays are highly intrusive and indiscriminate. To locate a suspect's cell phone, stingrays obtain information from *all* devices on the same network in a given area and send signals into the homes, bags, or pockets of the suspect and third parties alike. This type of device, even if not the one used here, can capture the content of communications, not merely the location of the device. Their use implicates the privacy interests of the suspect, as well as untold numbers of third parties as to whom there is no probable cause.

Yet the underlying Affidavit and supporting Application failed to disclose the government's intent to use a stingray and the device's indiscriminate intrusiveness into protected areas. The government cannot obtain judicial approval for a search using sophisticated, uniquely invasive technology that it never explained to the magistrate. To construe this Order as a valid "warrant" authorizing the use of the stingray would prevent magistrates from making informed determinations on warrant applications and encourage the government to keep magistrates in the dark.

The Fourth Amendment assigns judicial officers a critical role in ensuring that all aspects of a search are supported by probable cause and are not overly intrusive. *See United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986). The government's omission

of material information in a warrant application prevents the court from exercising this constitutional function. *United States v. Rettig*, 589 F.2d 418, 422-23 (9th Cir. 1979). Judicial supervision is particularly important with evolving technology, where there is a heightened risk of overly intrusive searches. *See United States v. Comprehensive Drug Testing, Inc.* (*CDT*), 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc).

As interpreted by the government, the Order authorized it to send signals into the home of and obtain information about the devices and whereabouts of Mr. Rigmaiden and third parties as to whom it lacked probable cause. Because the government withheld material information about stingray technology, the magistrate was not on notice of the need to limit and particularize the search, so as to mitigate the impact on third parties (if feasible) and prevent the Order from becoming a *de facto* "general warrant."

This case is a stark illustration of how Fourth Amendment privacy protections – for suspects and third parties alike will significantly be eroded if the government fails to apprise judicial officers about new surveillance technologies. The government seeks blanket authorization to conduct searches using invasive new technologies, without providing the issuing magistrate even rudimentary information about how the technology works. This Court should not countenance the government's effort to render meaningless the role of courts as an essential safeguard against unconstitutional searches and seizures.

In addition, the government wrongly asserts that Mr. Rigmaiden lacked a reasonable privacy expectation because he used an alias. Because the First Amendment protects the right to anonymous internet speech, his privacy interest was objectively reasonable.

Finally, the government engaged in a Fourth Amendment search when it obtained 38 days of cell site location information. Five justices agree that prolonged location tracking violates reasonable expectations of privacy. *See United States v. Jones,* 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

## II. STINGRAY TECHNOLOGY IS BOTH INVASIVE AND PRECISE

"Stingray" is the name for the Harris Corporation's line of "cell site simulator"

technology, also called "IMSI catchers" by technologists, in reference to the unique identifier – or international mobile subscriber identity of wireless devices.[1] Wireless carriers provide coverage through a network of base stations that connect wireless devices on the network to the regular telephone network. An IMSI catcher masquerades as a wireless carrier's base station; wireless devices then communicate with it as though it were actually the carrier's base station. One common feature of IMSI catchers is the ability to determine the location of mobile phones or wireless broadband data cards (or aircards).[2] *Amici* emphasize four points about the operation of these devices pertinent to the legal issues before the Court.[3]

First, stingrays impact third parties, not just the target of an investigation. In mimicking a wireless company's network equipment, the stingray sends signals to and triggers an automatic response from third parties' mobile devices.[4] The government concedes as much, and contends that its dragnet sweep of third-party information necessitated its destruction of evidence after the tracking mission. *See* Order, Doc. 723 at 18. The devices may also disrupt third parties' network connectivity.[5]

Second, the devices broadcast electronic signals that penetrate the walls of private locations not visible to the naked eye, including homes, offices, and other private

---

[1] Although "Stingray" refers to a specific line of Harris Corporation products, *see infra*, note 9, *amici* use the term "stingray" in this brief generically to refer to IMSI catchers.

[2] *See, e.g.,* HARRIS SOLE SOURCE VENDOR LETTER, http://egov.ci.miami.fl.us/Legistarweb/Attachments/48003.pdf at 6 (Harris Corporation "AmberJack" operates with other Harris products, "enabling tracking and location of targeted mobile phones").

[3] IMSI catchers vary, depending on among other things, whether the target phone operates on a "GSM" (e.g., AT&T) or "CDMA" (e.g., Verizon) network, and whether the IMSI catcher is "active" or "passive." This discussion focuses on commons features.

[4] *See, e.g.,* Hannes Federrath, "Protection in Mobile Communications," *in* Mulilateral Security in Communications, at 5 (Günter Müller et al. eds., 1999) ("possible to determine the IMSIs of all users of a radio cell"), *available at* http://epub.uni-regensburg.de/7382/1/Fede3_99Buch3Mobil.pdf; Daehyun Strobel, "IMSI Catcher," Seminararbeit, Ruhr-Universität, Bochum, Germany at 13 (July 13, 2007) ("An IMSI Catcher masquerades as a Base Station and causes every mobile phone of the simulated network operator within a defined radius to log in."), *available at* http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf.

[5] Juliam Dammann, "IMSI-Catcher and Man-in-the-Middle attacks," presentation at Seminar on Mobile Security, University of Bonn at 19 (February 9, 2011), *available at* http://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/10ws/10ws-sem-mobsec/talks/dammann.pdf.

locations of the target and third parties in the area.[6] Depending on the device's signal strength, the broadcast radius can reach up to "several kilometers."[7]

Third, the devices can pinpoint an individual with extraordinary precision, in some cases "within an accuracy of 2 m[eters]."[8] The government has conceded that the device located Mr. Rigmaiden precisely *within* his apartment. Order, Doc. 723 at 15, 19.

Fourth, although the specific device used by the FBI in this case may have been configured not to intercept content, materials from several surveillance vendors selling IMSI catchers show that these devices are certainly capable of doing so.[9]

## III. USE OF THE STINGRAY VIOLATED THE FOURTH AMENDMENT

The government's use of the stingray violated the Fourth Amendment

### A. N.D. Cal. 08-90330 Was Not A Valid Warrant Authorizing The Stingray Search

---

[6] The devices send signals like those emitted by a carrier's own base stations. *See, e.g.,* Harris Corp. product sheet at 1 ("Active interrogation capability emulates base stations"), *available at* http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/2600/Harris_StingRay.pdf. Those signals, of course, "penetrate walls" (necessarily, to provide connectivity indoors). *What You Need to Know About Your Network*, AT&T, http://www.att.com/gen/press-room?pid=14003; *see also* E.H. Walker, *Penetration of Radio Signals Into Buildings in the Cellular Radio Environment*, 62 THE BELL SYSTEMS TECHNICAL JOURNAL 2719 (1983), *available at* http://www.alcatel-lucent.com/bstj/vol62-1983/articles/bstj62-9-2719.pdf.

[7] Strobel, *supra*, note 4, at 13.

[8] *See, e.g.,* "GSM Cellular Monitoring Systems" brochure by PKI Electronic Intelligence GmbH at 12 (device can "locat[e]... a target mobile phone within an accuracy of 2 m[eters]"), *available at* http://www.docstoc.com/docs/99662489/GSM-CELLULAR-MONITORING-SYSTEMS---PKI-Electronic-#; Resp. to National Telecommunications Information Administration Notice of Inquiry (Doc. #100504212-0212-01) Requesting Information on Preventing Contraband Cell Phone Use in Prisons, submitted by Bahia 21 Corp. at 3 (June 11, 2010), *available at* http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/BAHIA21%20resposne%20to%20NTIA%20NOI.pdf (a US surveillance vendor offering fixed IMSI catchers to be installed in prisons to detect contraband cell phones, promising 10-15m accuracy of geolocation identification) .

[9] *See, e.g.,* Harris, Wireless Products Group Price List at 8 (September 2008) (StingRay line of products includes "Intercept Software Package" for GSM phones), *available at* https://info.publicintelligence.net/Harris-SurveillancePriceList.pdf; *Active GSM Interceptor,* ABILITY, http://www.interceptors.com/intercept-solutions/Active-GSM-Interceptor.html (describing IBIS II device: "The user can control the level of service to the target mobiles, selectively Jam specific mobiles, perform silent calls, call or SMS on behalf of target mobile, change SMS messages on the fly, detect change of SIM card or change of handset, and support Direction Finding system and many additional operational features."); *Cell Phone Intercept Apparatus*, VIEW SYSTEMS, http://www.viewsystems.com/pdf/CIA_11_20_06.pdf("Optional voice decode, record and forward; *see also* Dammann, *supra,* note 5, at 5 ("is able to eavesdrop").

The government concedes a Fourth Amendment search occurred, a concession compelled by Supreme Court precedent.[10] But the government cannot plausibly claim that N.D. Cal. 08-90330 was a warrant that authorized the government to use the stingray.[11]

**1. The Stingray Search Was Not Within The Scope Of 08-90330**

The government's stingray search did not fall within the scope of N.D. Cal. 08-90330. The Order directs *Verizon* to provide the government with information and assistance, but nowhere authorizes the *government* to search or seize anything.[12]

Nor could this defect be cured by the Application and Affidavit, which indicate only that the government sought Verizon's assistance in locating the aircard. *See, e.g.,* Application at 1 ("submits this Application in support of an Order *directing Verizon Wireless* to assist agents of the" FBI) (emphasis added). These documents nowhere use the term "stingray," and instead make fleeting references to a "mobile tracking device." But the only description of the device is buried at the end of an 18-page declaration:

> The cell sites provide a link between the Target Broadband Access Card/Cellular Telephone and Verizon Wireless facilities, where the [sic] *Verizon Wireless* [can] then determine the general location of the Target Broadband Access Card/Cellular Telephone. The mobile tracking equipment ultimately generate[s] a signal that

---

[10] First, the device pinpointed Mr. Rigmaiden's location *within* his residence. Like the beeper placed into a can of ether, in turn taken into a residence, in *United States v. Karo*, 468 U.S. 705 (1984), the "monitoring of [the] electronic device" here was a search because it "reveal[ed] a critical fact about the interior of the premises that the Government is extremely interested in knowing about and that it could not otherwise have obtained without a warrant." *Id.* at 715; *see also Kyllo v. United States,* 533 U.S. 27, 34 (2001) (thermal imaging to detect heat from home constituted search). Second, the device sent electronic signals to penetrate the walls of Mr. Rigmaiden's residence (and unsuspecting third parties). This "unauthorized physical penetration into the premises" constituted a search. *Silverman v. United States,* 365 U.S. 505, 509 (1961) (finding search where government used "spike mike," a microphone attached to spike inserted into walls of house); *see also Jones,* 132 S.Ct. at 949 (installation and monitoring of GPS on suspect's vehicle constituted search because of "physical intrusion" "for the purpose of obtaining information").

[11] N.D. Cal. 08-90330 and 08-90331 are lodged under seal at Doc. 470. This Court denied Defendant's motion to unseal those documents because at the time they remained subject to a seal order in the issuing Court, the Northern District of California. *See* Doc. 727. *Amicus* has since obtained an order in the Northern District unsealing the two Orders, and the underlying Applications and Affidavits. *See* Lye Decl., *filed herewith,* ¶¶4-9.

[12] *See* Order at 2 ("The Court therefore ORDERS … that Verizon Wireless … shall"); *id.*at 3 ("It is further ORDERED … that Verizon Wireless shall"). The orders, applications and affidavits in 08-90330 and 08-90331, the government's companion application for cell site information, are attached at Lye Decl., Exh. 2 & 3, respectively.

> fixes the geographic position of the Target Broadband Access Card/Cellular Telephone.

Affidavit at ¶42 (emphasis added). Particularly because the Application sought Verizon's assistance, these two sentences suggest that *Verizon* would determine the location of the aircard by monitoring some unspecified "mobile tracking equipment."

In evaluating whether a search falls outside the scope of a warrant, a court looks to "the circumstances surrounding the issuance of the warrant, the contents of the search warrant, and the circumstances of the search." *United States v. Hurd,* 499 F.3d 963, 966 (9th Cir. 2007) (internal quotation marks, citation omitted).

In this case, the "contents of the search warrant" do not authorize the government to perform any search or seizure. *Dalia v. United States,* 441 U.S. 238 (1979), on which the government relies, *see* Gov.'s Resp., Doc. 873 at 51, has no bearing on this case. The warrant there contained critical language not present here: "WHEREFORE, it is hereby ordered that: Special Agents of the Federal Bureau of Investigation … are authorized … to: …Intercept oral communications…." *Dalia*, 441 U.S. at 242 n.4. The government makes much of the finding of "probable cause" but that speaks only to whether the government complied with the Fourth Amendment in obtaining information and assistance from Verizon (to which the Order was directed), not whether the search the government conducted fell within the scope of this Order.[13]

**2. The Government Cannot Obtain Judicial Authorization To Engage In A Search Using Technology It Has Failed To Explain To The Issuing Magistrate**

If, however, the Order could be construed to authorize a search, which it cannot,

[13] Indeed, there is good reason to believe that the government fully understood that the stingray search was *not* within the scope of 08-90330. Emails written after the stingray search located Mr. Rigmaiden suggest that the government did not wish to disclose its use of the stingray to the court in its subsequent application for a warrant to search Mr. Rigmaiden's apartment. *See* E-mail from Denise Medrano, Special Agent, to Albert Childress (July 17, 2008) (Doc. 587-2, Exh. 34) (government sought "to develop independent probable cause of the search warrant…FBI does not want to disclose the [redacted]"); E-mail from Fred Battista, AUSA, to Shawna Yen (July 17, 2008) (Doc. 587-3, Exh. 38) ("The main effort now may be to tie the target to the case without emphasis on the [redacted]."). Why would the government labor to avoid disclosure of a search for which it had obtained a warrant? Its desire to avoid disclosure only makes sense if the government believed at the time what the face of the Order makes clear – that the stingray search was not within the scope of 08-90330.

the Order would be an unconstitutional "general warrant." By failing to apprise the magistrate that it intended to use a stingray, what the device is, and how it works, it prevented the judge from exercising his constitutional function of ensuring that warrants are not overly intrusive and all aspects of the search are supported by probable cause.

The Fourth Amendment was "the product of [the Framers'] revulsion against" "general warrants" that provided British "customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws." *Stanford v. Texas,* 379 U.S. 476, 481, 482 (1965). The particularity requirement serves two purposes. It "prevents general, exploratory searches and indiscriminate rummaging through a person's belongings." *Spilotro,* 800 F.2d at 963. "It also ensures that the magistrate issuing the warrant is fully apprised of the scope of the search and can thus accurately determine whether the entire search is supported by probable cause." *Id.*

The role of the magistrate is key. In *Rettig*, the Ninth Circuit required suppression where the government withheld material information about the intended scope of the search. 589 F.2d at 422-23. After applying unsuccessfully for a search warrant for cocaine-related evidence, the government went to a different magistrate, obtained a warrant for evidence of a marijuana offense, and then engaged in a broad search, seizing cocaine-related items. *Id.* at 420-21. The court found a Fourth Amendment violation: The magistrate may have granted the marijuana search warrant, but subject to "limitations" on the scope of the search and seizure "to prevent an overly intrusive search." *Id.* at 423. "A judicial officer cannot perform the function of issuing a warrant particularly describing the places to be searched and things to be seized," if "the agents withh[o]ld [material] information." *Id.* at 423.

The Ninth Circuit has emphasized the heightened need for judicial supervision in the context of evolving technology, where the danger of overly intrusive searches and seizures is acute. In *CDT*, the government searched and seized electronic records of hundreds of people, as part of its investigation of steroid use by ten baseball players. 621 F.3d at 1166. While law enforcement may "need … broad authorization to examine

electronic records" ("[t]here is no way to be sure exactly what an electronic file contains without somehow examining its contents"), that need "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id.* at 1176. The *en banc* court therefore discussed "the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information," to prevent such searches from becoming overly intrusive. *Id.* at 1166; *see also id*. at 1170-71, 1177.

Chief Judge Kozinski, in a concurring opinion joined by four other judges, emphasized "the government's duty of candor in presenting a warrant application." *See id.* at 1178 (Kozinski, C.J., concurring). While the government may explain theoretical risks of concealment and evidence destruction that would weigh in favor of a broad warrant, it "should also fairly disclose the *actual* degree of such risks…. A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data." *Id.* (emphasis in original); *see also id.* at 1180 (providing guidance for electronic searches, including protocols for segregation and redaction of third-party data).

The government here failed to provide then-Magistrate, now-Judge, Seeborg with essential information about the nature and scope of the search. The Application and Affidavit indicated only that the government sought to obtain information from Verizon, not that the government sought to engage in its own search of Mr. Rigmaiden's home. The Application provides no explanation of a stingray. The Affidavit states only "[t]he mobile tracking equipment ultimately generate[s] a signal that fixes the geographic position" of the aircard, but did not provide any explanation whatsoever of *what* the mobile tracking equipment was and *how* it "ultimately generate[s]" that signal. Affidavit at ¶42. It did not explain that the device broadcasts signals to all devices in the area, receives information about other devices in the possession of third parties, potentially disrupts the connections of third-party devices, and penetrates the walls of every private residence in the vicinity, not solely that of the target. *See supra* at Part II.

The Affidavit is particularly misleading because its sole, conclusory paragraph purporting to describe the stingray is *identical* to the paragraph of the Affidavit submitted in support of the government's companion Application in 08-90331 to install an entirely different device, a pen register/trap and trace. *Compare* Affidavit (08-90330) at ¶42, *with* Affidavit (08-90331) at ¶42. Thus, the government's submissions completely failed to convey to the judge that it was seeking to use the unique device at issue here, and not a more common form of location tracking technology.

The government's "lack of candor" (*CDT,* 621 F.3d at 1170 (Kozinski, C.J., concurring)), was highly consequential.

Had the government candidly told the judge that it intended to use a stingray, he may have denied the application without prejudice to a subsequent application providing further details about the technology. This is precisely what a federal magistrate did in one of the two other decisions of which *amici* are aware involving a stingray. *See In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device* (*In re Stingray*), _F.Supp.2d_, 2012 WL 2120492, *1 (S.D. Tex. June 2, 2012). [14] As the same magistrate explained in denying a statutory application for cell site records of *all* subscribers from several cell towers, an understanding of "the technology involved" is necessary to "appreciate the constitutional implications of" the warrant application, particularly where, as here, the technology entails "a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment." *In re Application for an Order Pursuant to 18 U.S.C. §2703(d)* (*In re Cell Tower Dump*), 2012 WL 4717778 *4 (S.D. Tex. Sept. 26, 2012).

But with more complete information, the judge may have denied the application on the ground that use of a stingray is too intrusive, for example, because of the impact on third parties. This is what a federal magistrate did in the other stingray decision, involving the government's statutory application to use the device. *See In re Application for an*

[14] That case involved an application to use the device under the pen register statute, not for a warrant. The court concluded, based on the scant information before it, that the device did not fall under the statutory definition of a pen register. *Id.* at *5.

*Order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F.Supp. 197, 201 (C.D. Cal. 1995) (denying statutory application to use stingray because, *inter alia,* "depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted"). That stingrays obtain information about third parties "creates a serious risk that every warrant for [a stingray] will become, in effect, a general warrant," to search persons as to whom there is no probable cause. *See CDT,* 621 F.3d at 1176.

Indeed, the record suggests that the judge may well have denied the application had he known how precisely it is able to locate a suspect. The government submitted a companion application for historical cell site information that relied on a substantially similar factual predicate. *Compare* Affidavit (08-90331), *with* Affidavit (08-90330). But in the Order on the companion application, the judge expressly stated that the government was "*not* authorized to obtain" cell site information that would allow it "to determine the precise location of the user of the Target Device." *See* N.D. Ca. Order 08-90331 at 3:6-10 (emphasis added). By withholding information about the stingray's capabilities, the government obtained an Order which it now claims authorized it do exactly what the judge prohibited it from doing in a companion Order – precisely locating the aircard.

Alternatively, had the judge been fully apprised about the technology and how it functions, he may ultimately have issued a warrant, but could have crafted "explicit limitations … to prevent an overly intrusive search." *Rettig,* 589 F.2d at 423.

Such limitations are especially necessary with stingray devices. First, the devices obtain third-party information. The government asserts that its data destruction after the tracking mission was intended to protect these third parties. Doc. 674-1 ¶5. But after the fact data destruction does not prevent third-party residential searches. Moreover, although the Order submitted by the government and signed by the judge provided for data destruction, the Application and Affidavit failed to contain any "discussion about … the privacy rights … of these innocent subscribers whose information will be compromised" by the search. *See In re Cell Tower Dump,* 2012 WL 471778, *4 (denying application for

cell phone information of suspect and third parties). Had the court been alerted to the existence of this issue, it might have developed a procedure other than wholesale data purging, such as "[s]egregation and redaction" of third-party information "by specialized personnel or an independent third party." *See CDT,* 621 F.3d at 1180 (Kozinski, C.J., concurring). It was for the magistrate, not the government, to determine how best to balance the government's need for information, third-party privacy, and the suspect's interest in future access to potentially exculpatory information.

Second, and relatedly, the government failed to inform the magistrate that stingrays operate by broadcasting signals to all devices within a given area and what area it sought to search here, facts that are highly material to the appropriate scope of the search, *viz.,* its impact on third parties as to whom there was no probable cause. The government's failure to include these facts prevented the judge from "exercis[ing] meaningful supervision over" the search, for example, by imposing a limitation on the broadcast radius of the stingray. *Rettig*, 589 F.2d at 422.

Third, some IMSI catchers are capable of capturing content. *See supra* at Part II. The government *now* asserts that the device used here was not capable of doing so. But information about the capability and limitations of the technology proposed to be used bears on whether a given search is overly intrusive, and should have been provided to the magistrate *at the time of the Application*.[15]

In short, the government's failure to inform the judge about the stingray prevented him from exercising his constitutional supervisory function. These material omissions prevented the magistrate from meaningfully evaluating the necessity of limitations on the search – for example, related to the size of the search area and protocols for handling third-party data. Such limitations would have prevented the government from expanding this Order into a general warrant to engage in a highly intrusive search, including of third

[15] If the government wishes to intercept content, it must comply with the heightened requirements for a wiretap. *See* 18 U.S.C. §2518; *United States v. Oliva,* 686 F.3d 1106, 1113 (9th Cir. 2012) (in wiretap application, "the government cannot obtain – nor may courts approve – electronic surveillance orders by using ambiguous terminology that can be misconstrued to authorize interception of communications beyond what is intended").

parties as to whom it lacked probable cause. Where the government engages in a search pursuant to a general warrant, "we must regard the search as 'warrantless'…" *Groh v. Ramirez,* 540 U.S. 551, 558 (2004).[16]

Given the heightened risk of intrusive searches posed by advances in technology, "the government's duty of candor in presenting a warrant application," *CDT,* 621 F.3d at 1178 (Kozinski, C.J., concurring), requires it to explain to magistrates the technology and "the process by which the technology will be used to engage in the electronic surveillance." *In re Stingray,* 2012 WL 2120492 at *1. In light of their impact on third parties and their potential to capture content, IMSI catchers are a potent illustration of the Ninth Circuit's concern in *CDT* that absent judicial supervision, warrants authorizing electronic searches risk becoming "general warrant[s], rendering the Fourth Amendment irrelevant." 621 F.3d at 1176.[17]

### B. Mr. Rigmaiden Has A Reasonable Expectation Of Privacy In An Aircard Registered Under An Alias Because The First Amendment Protects Anonymous Internet Speech

The government contends that Mr. Rigmaiden lacks standing to raise this Fourth Amendment challenge because his use of an alias rendered his privacy expectation objectively unreasonable. *See Rakas v. Illinois,* 439 U.S. 128, 143 n.12 (1978) (defendant must prove subjective and objective expectation of privacy).[18] This argument is meritless.

First, even if the analysis turned solely on the aircard, the privacy interest is not simply in using an alias to engage in an ordinary commercial transaction, but in an

---

[16] The government's reliance on *Karo* is misplaced. *See* Gov's. Resp., Doc. 873 at 52. The Court in *Karo* stated "it will still be possible to describe the object into which the beeper is to be placed" and suggested that such information (along with probable cause and the duration of the proposed surveillance) would suffice. 468 U.S. at 718. Even with a beeper, which has far less technological capacity for intrusion than a stingray, the Court expected the government to explain the basic methodology of the proposed electronic surveillance (that the government intended to install a beeper at all, and where it sought to do so). The government here withheld from the judge the pertinent analogous information.

[17] There is a serious question whether stingray technology – because of its inevitable impact on third parties – can ever be used consistent with the Fourth Amendment. But the Court can conclude that the stingray search in this case violated the Fourth Amendment on scope or particularity grounds.

[18] The government does not dispute that Mr. Rigmaiden manifested a subjective expectation of privacy.

inherently expressive activity, accessing the internet anonymously. Mr. Rigmaiden has a legitimate expectation of privacy in his aircard because the constitutional right to anonymous internet speech is surely "one that society is prepared to recognize as reasonable." *Katz v. United States,* 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

"The internet is a unique democratizing medium unlike anything that has come before….Through the internet, speakers can bypass mainstream media to speak directly to 'an audience larger and more diverse than any the framers could have imagined.'" *Doe v. Cahill,* 884 A.2d 451, 455-56 (Del. 2005) (citation omitted). "Under our constitution, anonymous [speech] … is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent." *McIntyre v. Ohio Elections Comm'n.,* 514 U.S. 334, 357 (1995). "As with other forms of expression, the ability to speak anonymously on the Internet promotes the robust exchange of ideas and allows individuals to express themselves freely without fear of economic or official retaliation or concern about social ostracism." *In re Anonymous Online Speakers*, 661 F.3d 1168, 1173 (9th Cir. 2011) (internal quotation marks, citation omitted).[19]

Mr. Rigmaiden used his internet connection to access political speech, such as materials related to the 2008 election. *See* Def's. Mot. to Supress, Doc. 824 at 201-02. The government, however, would force Mr. Rigmaiden and other speakers to forfeit their Fourth Amendment right to be free of warrantless searches simply by exercising their First Amendment right to engage in anonymous speech. *But cf. Lingle v. Chevron U.S.A. Inc.*, 544 U.S. 528, 547 (2005) (discussing unconstitutional conditions doctrine).

The government's cases simply do not support its far-reaching and speech-inhibiting theory. *Cf.* Gov.'s Resp., Doc. 873 at 58-59. None of them involve a defendant's interest in anonymous internet access, and indeed one succinctly *rejects* the

[19] Recognizing the constitutional status of anonymous internet speech, courts across the country apply demanding standards before those allegedly harmed by the speech can unmask an anonymous speaker. *See, e.g., Indep. Newspapers, Inc. v. Brodie,* 966 A.2d 432 (Md. 2009); *Krinsky v. Doe 6*, 72 Cal.Rptr.3d 231 (Cal. App. 2008); *Mobilisa, Inc. v. Doe,* 170 P.3d 712 (Ariz. App. 2007); *Cahill,* 884 A.2d at 460-61; *Dendrite Int'l, Inc. v. Doe No. 3,* 775 A.2d 756 (N.J. App. 2001).

proposition that use of an alias forecloses a reasonable privacy expectation. In *United States v. Pitts,* 322 F.3d 449 (7th Cir. 2003), the court upheld a search of a package mailed to a fictitious name, but on the very different ground that the defendants had abandoned the parcel. *Id.* at 455. The majority went on to criticize the concurrence cited by the government: The refusal of the concurrence in *Pitts* – and the government here – to recognize a legitimate privacy expectation because of the alias either means that "everyone with a legitimate reason to remain anonymous should lose their expectation of privacy in the post" simply "because some people employ an alias and use the mail illegally," or that "only people using an alias for legitimate reasons may retain an expectation of privacy in their mailings while those who employ an alias for illicit purposes may not." *Id.* at 458. This Court should not embrace a theory that "turn[s] the Fourth Amendment on its head." *Id.*

Most of the government's alias cases rest on the unremarkable proposition that one cannot assert a privacy expectation in the property of another, and as a result, reject the defendant's assertion of a reasonable privacy expectation "when an individual uses an alias or fictitious name *and there is no other evidence linking the defendant to the item or property." United States v. Suarez-Blanca,* 2008 WL 4200156, *6 (N.D. Ga. Apr. 21, 2008) (emphasis added); *see also id.* at n.6 ("no evidence linking the subscriber, 'Felix Baby,' to Rodriguez"). [20] Here, by contrast, the government's entire care is premised on the link between the aircard and Mr. Rigmaiden.[21]

[20] The government's other alias cases similarly do not support its position. *See also United States v. Daniel*, 982 F.2d 146, 149 (5th Cir. 1993) (upholding search of package where defendant disavowed connection to name on package); *United States v. Coverson*, 2011 WL 1044632 *5 (D. Ala. Mar. 22, 2011) ("The alias Jay Jenkins was not an alias adopted and regularly used by Coverson."). *United States v. Davis,* 2011 WL 2036463 *3 (D. Or. May 24, 2011), similarly found an insufficient connection between the defendant and the account at issue ("not the registered owner or subscriber of the phone," "not registered as a permissible user"), but suggests that the Court would have found a legitimate privacy expectation had the Defendant presented "evidence that," like Mr. Rigmaiden, "he had used an alias to obtain the phone." *Id.* at *3.

[21] The government's remaining cases involve the opinion of a single judge, *see United States v. Lozano,* 623 F.3d 1055, 1060-61 (9th Cir. 2010) (majority upholding search of package because postal worker had reasonable suspicion to detain the package, and a subsequent dog sniff indicated the presence of drugs; alias played no role in decision), *or*

Second, the government's focus on the aircard is misplaced. Mr. Rigmaiden has standing because he has an undisputed privacy expectation in the *place* that was searched, his residence. In *Karo,* in which the Court found use of a beeper to monitor suspects indoors to be a search, the Court expressly addressed standing; its analysis turned not on the privacy interest in the beeper or the can of ether in which it was placed, but in the places electronically monitored. *See* 468 U.S. at 719-20. The government concedes the stingray identified Mr. Rigmaiden while inside his apartment. "At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." *Id*. at 714.[22]

The gravamen of the government's argument is that Mr. Rigmaiden has no legitimate expectation of privacy because he is "a thief and fugitive." Gov.'s Opp., Doc. 873 at 61. "We may not justify the search after the fact, once we know illegal activity was afoot; the legitimate expectation of privacy does not depend on the nature of the defendant's activities, whether innocent or criminal." *Pitt*, 322 F.3d at 458.

## IV. THE GOVERNMENT VIOLATED THE FOURTH AMENDMENT WHEN IT OBTAINED CELL SITE RECORDS WITHOUT A WARRANT

The government also violated the Fourth Amendment by obtaining 38 days of historical cell site information from Verizon without a warrant.[23]

The Supreme Court's recent decision in *Jones* – in which nine justices agreed that

---

out of circuit *dictum, see United States v. Lewis*, 738 F.2d 916, 919 n.2 (8th Cir. 1984) ("the challenged search warrants may be decided on other grounds").

[22] Nor is his legitimate interest in his residence diminished by use of an alias. The government asserts "fraud" but nowhere demonstrates that Mr. Rigmaiden's name was material to the rental transaction (or his purchase of the aircard and laptop); because he fully paid his rent with money orders (and for the aircard and laptop with cash and a prepaid debit card) (Def's. Mot. to Suppress, Doc. 824 at 196-99), there is no showing that any vendor suffered damage. *But see Haisch v. Allstate Ins. Co.,* 197 Ariz. 606, 610 (App. Div. 2000) (elements of fraud include "false, material representation" by defendant and detrimental reliance and proximate damage by victim). Moreover, an individual retains a reasonable privacy expectation even in a fraudulently procured location, until evicted. *See United States v. Young,* 573 F.3d 711, 716 (9th Cir. 2009); *United States v. Bautista,* 362 F.3d 584, 590 (9th Cir. 2004). Because Mr. Rigmaiden had not been evicted at the time of the search, he maintained a reasonable privacy expectation in his apartment.

[23] The government's brief does not specify the time period; Mr. Rigmaiden contends it was 38 days. *See* Gov.'s Resp., Doc. 873 at 32; Def's Mot. to Supress, Doc 824-1 at 217.

installation and monitoring of a GPS device on a car over 28 days constituted a Fourth Amendment search – supports the conclusion that location tracking using 38 days of cell site records is also a search. The *Jones* majority relied on a narrow "trespass" theory. *See Jones*, 132 S.Ct. at 949. But five justices in two concurrences agreed that prolonged electronic location tracking, even while a suspect travels in public areas, violates reasonable privacy expectations because it generates a "precise [and] comprehensive" record about intimate details, such as "familial, political…, and sexual associations." *See id.* at 955 (Sotomayor, J., concurring); *accord id.* at 964 (Alito, J., concurring).

Cell site information can track location with a precision similar to GPS technology. *See*, *e.g.*, *In re Application for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel* (*In re Cell Location Info*)., 849 F. Supp. 2d 526, 540 (D. Md. 2011). Both *Jones* concurrences cited data disclosed to cell phone providers as issues of Fourth Amendment concern. *See.* 132 S.Ct. at 957 (Sotomayor, J., concurring); *id.* at 963 (Alito, J., concurring). Given the similar precision of the technology, the conclusion of five justices in *Jones* that 28 days of GPS tracking violated reasonable privacy expectations compels the same conclusion with 38 days of cell site information.

The government contends that no federal court has ever suppressed cell site records. *See* Gov.'s Resp., Doc. 873 at 45:6-16. But many courts have denied statutory requests for cell site data and required the government to satisfy warrant requirements.[24] The only two circuits to decide the issue have issued conflicting opinions.[25]

---

[24] *See e.g., In re Cell Location Info*, 849 F. Supp. 2d at 583; *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011); *In re Application for an Order Authorizing the Installation & Use of a Pen Register Device*, 497 F. Supp. 2d 301, 311 (D.P.R. 2007); *In re Application for an Order Authorizing Installation & Use of a Pen Register*, 415 F. Supp. 2d 211, 214 (W.D.N.Y. 2006); *In re Application for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947. 958 (E.D. Wis. 2006) *aff'd*, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006); *In re U.S. for Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices on Tel. Numbers*, 416 F. Supp. 2d 390, 396-97 (D. Md. 2006); *see also In re Application for Historical Cell Site Data*, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) (on appeal to Fifth Circuit, No. 11-20884).

[25] *Compare In re Application for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't* (*In re Cell Provider Disclosure*), 620 F.3d 304 (3d Cir. 2010) (judge may require government to obtain search warrant for cell site records), *with United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012) (no search warrant needed).

The government's reliance on the third-party doctrine is misplaced. Gov.'s Resp., Doc. 873 at 40-45. The Third Circuit and other courts have rejected the applicability of the doctrine to cell site records, which are often generated automatically by the device, not voluntarily by the user. *See In re Cell Provider Disclosure*, 620 F.3d at 317-18.[26] Justice Sotomayor in her *Jones* concurrence observed that the doctrine 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." 132 S. Ct. at 957 (Sotomayor, J., concurring); *see also United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (rejecting application of third-party doctrine to email, even though stored with internet service provider).[27]

Further, the government's argument that the Pen/Trap Statute, 18 U.S.C. §§3121, *et seq*., and Stored Communication Act, 18 U.S.C. §§ 2701, *et seq.*, authorize the disclosure of cell site information has been rejected by many courts.[28] This Court should do so for the reasons set forth in those decisions.

## V. CONCLUSION

For the foregoing reasons, the government's use of the stingray and collection of cell site location information violated the Fourth Amendment.

---

[26] *See also In re Application for Historical Cell Site Data*, 747 F. Supp. 2d at 844-45; *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.* (*In re Trap/Trace*), 396 F. Supp. 2d 747, 756-57 (S.D. Tex. 2005); *Commonwealth v. Pitt*, 2012 WL 927095, at *4 (Mass. Super. Feb. 23, 2012).

[27] The government cites *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007), in which the court found no expectation of privacy in IP address information. But *Forrester* "does not imply that more intrusive techniques … are also constitutionally identical." *Id.* at 511. Cell site location data over a 38-day period is more intrusive than simple IP address information because it reveals intimate details about familial and other associations. *See Jones,* 132 S.Ct. 955 (Sotomayor, J., concurring).

[28] *See, e.g.,* cases cited, *supra* note 24; s*ee also In re Application for an Order Authorizing the Release of Prospective Cell Site Info.*, 407 F. Supp. 2d 132 133 (D.D.C. 2005); *In re Application for an Order: (1) Authorizing Use of a Pen Register & Trap & Trace Device, (2) Authorizing Release of Subscriber & Other Info., (3) Authorizing Disclosure of Location-Based Services*, 727 F. Supp. 2d 571, 575 (W.D. Tex. 2010); *In re Application for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Numbers*, 402 F. Supp. 2d 597, 600 (D. Md. 2005); *In re Trap/Trace*, 396 F. Supp. 2d at 765; *In re Application for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d 294, 326-27 (E.D.N.Y. 2005); *see also In re Application for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 2006 WL 468300, at *2.

Dated: October 19, 2012

Respectfully submitted,

By: /s/ Daniel J. Pochoda
Daniel J. Pochoda

Linda Lye*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm St., 2nd Floor
San Francisco, California 94111
Telephone: (415) 621-2493
llye@aclunc.org

Daniel J. Pochoda (SBA 021979)
Kelly J. Flood (SBA 019772)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF ARIZONA
3707 N. 7th Street, Suite 235
Phoenix, AZ 85014
Telephone: (602) 650-1854
dpochoda@acluaz.org
kflood@acluaz.org

Ben Wizner*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
bwizner@aclu.org

Hanni M. Fakhoury*
Staff Attorney
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x. 117
hanni@eff.org

*Application for admission *pro hac vice* pending

Attorneys for *amici curiae*

CERTIFICATE OF SERVICE

I hereby certify that on October 19, 2012 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:

Florence, AZ 85132Taylor W. Fox, PC
2 North Central Ave., Suite 735
Phoenix, AZ 85004
*Attorney for Defendant Ransom Carter*

Frederick A. Battista
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

Peter S. Sexton
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

James R. Knapp
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

*Attorneys for United States*

Copy of the attached document, mailed this 19th day of October, 2012, to:

Daniel David Rigmaiden
Agency No. 10966111
CCA-CADC
PO Box 6300

/s/Gloria Torres