STINGRAYS

The Most Common Surveillance Tool the Government Won't Tell You About

A Guide for Criminal Defense Attorneys

FROM THE ACLU OF NORTHERN CALIFORNIA

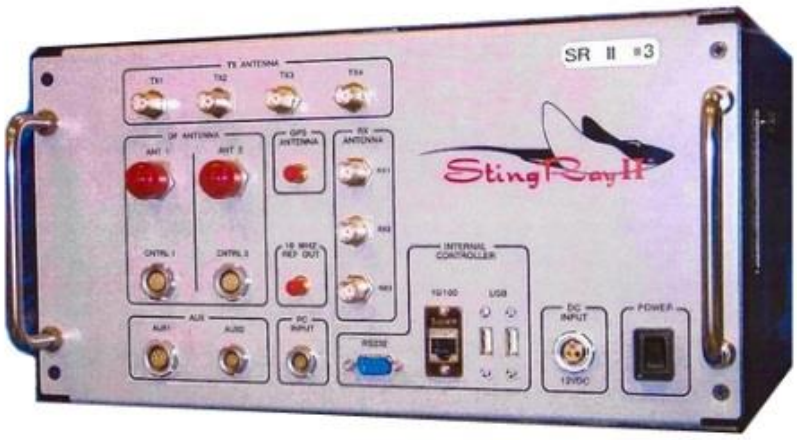


Photo credit: US Patent & Trademark Office

Author: Linda Lye, Senior Staff Attorney, ACLU of Northern California
Cover: Gigi Pandian, ACLU of Northern California
Design: Carey Lamprecht

Published by the ACLU of Northern California, June 27, 2014

The author wishes to thank Nanci Clarence, Josh Cohen, Catherine Crump, Hanni Fakhoury, Carey Lamprecht, Robin Packel, Mindy Phillips, and Nate Wessler for reviewing and commenting on drafts of this paper, and Christopher Soghoian for providing an eye-opening education on IMSI catchers. Special thanks go to Daniel Rigmaiden for his keen insights on legal and technological issues and for shedding light on this important issue.

ACLU FOUNDATION
AMERICAN CIVIL LIBERTIES UNION of NORTHERN CALIFORNIA

TABLE OF CONTENTS

I. Introduction

Federal and state law enforcement entities across the country are using a powerful cell phone surveillance tool commonly referred to as a "StingRay." These devices are capable of locating a cell phone with extraordinary precision, but to do so they operate in dragnet fashion, scooping up information from a target device, as well as other wireless devices in the vicinity. In addition, these devices can be configured to capture the content of voice and data communications. Although the federal government has been using these devices since at least 1995, and use by state and local governments is quite widespread, there are only a handful of opinions addressing their use.

At this juncture, few criminal defense attorneys are aware of these highly intrusive but extremely common surveillance tools. This is entirely understandable because the federal government has a policy of not disclosing information about this device. The government appears to be withholding information from criminal defendants. It even appears to be providing misleading information and making material omissions to judicial officers when it seeks purported court authorization to use this device – inaccurately referring to it as a "confidential source" or calling it a different kind of device (like a pen register), and failing to alert courts to constitutionally material facts about the technology, such as the full breadth of information it obtains from a suspect and its impact on third parties. As a result, courts are probably not aware that they are authorizing use of this device and have not had an opportunity to rule on its legality, except in very rare instances.

The secrecy surrounding these devices is deeply troubling because this technology raises grave constitutional questions. There is a compelling argument that StingRays should never be used. Because they operate in dragnet fashion, they engage in the electronic equivalent of the "general searches" prohibited by the Fourth Amendment. But at a minimum, law enforcement should obtain a warrant. Even in those instances when law enforcement obtains a warrant, however, there are likely strong arguments that the warrant is invalid.

The purpose of this paper is to provide criminal defense attorneys with a basic introduction to StingRays, allowing them to assess whether the devices may have been used in their cases and to outline potential arguments for a motion to suppress.

Part II of this paper provides a brief overview of salient aspects of the technology and uses for the device. Part III describes the types of court authorization, if any, the government likely obtains to use the device. Part IV discusses the guidance courts have offered on the technology. Part V suggests indicia for determining whether the device was used in a particular case. Part VI outlines key constitutional arguments for a motion to suppress, focusing on Ninth Circuit caselaw. Potential issues to pursue in discovery are set forth in an appendix to this paper. Detailed footnotes are intended to assist attorneys preparing briefs.

II. StingRays: What do they do and how do they work?

"StingRay" is the name for a line of "cell site simulator" technology sold by the Harris Corporation.[1] Other Harris cell site simulator models include the "TriggerFish," "KingFish," and "Hailstorm."[2] The more generic term for the technology is "IMSI catcher," in reference to the unique identifier – or international mobile subscriber identity – of a wireless device. Although IMSI catchers may be the most under-litigated surveillance tool in widespread use, there is a fair amount of publicly available information about them.

The government has been using IMSI catchers for approximately two decades. According to documents obtained by the Electronic Privacy Information Center ("EPIC") in a Freedom of Information Act ("FOIA") lawsuit, the Federal Bureau of Investigation ("FBI") has been using the technology since 1995, agents have undergone extensive training on these devices, and usage is dramatically increasing.[3] A number of federal law enforcement agencies, including the FBI, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms and Explosives, Secret Service, Marshals Service, and Immigration and Customs Enforcement, are known to own and use cell site simulators.[4] Use is not limited to the federal government. At least 34 law enforcement agencies in 15 states have purchased IMSI catchers.[5]

Wireless carriers provide coverage through a network of base stations, also called cell sites, that connect wireless devices to the regular telephone network. Cell phones periodically identify themselves to the base station that has the strongest radio signal, which is often, but not always, the nearest base station.[6] A cell phone automatically transmits to the base station "signaling data," which includes the phone's unique numeric identifier, as well as its cell site code, which identifies its location.[7] An IMSI catcher masquerades as a wireless carrier's base station, thereby prompting cell phones to communicate with it as though it were actually the carrier's base station.[8] The equipment consists of "an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information."[9] It "can be carried by hand or mounted on vehicles or even drones."[10]

StingRays are capable of capturing the following types of information:

First, if the government knows a suspect's location, it can use the device to determine the unique numeric identifier associated with her cell phone. To do this, law enforcement agents "position a StingRay in the vicinity of the target['s phone]," which will then transmit to the IMSI catcher the signaling information (including unique numeric identifier) it would normally transmit to the carrier's base station.[11] There are a variety of unique numeric identifiers, including International Mobile Subscriber Identity ("IMSI"),[12] Electronic Serial Number ("ESN"),[13] and Mobile Identification Number ("MIN").[14] Obtaining a cell phone's unique numeric identifier facilitates the government's efforts to obtain a wiretap or call records on a target of an investigation.

Second, if the government knows a cell phone's unique numeric identifier, it can use an IMSI catcher to determine the phone's location.[15] The numeric identifier is programmed into the

IMSI catcher, which then sorts through the signaling data (including location) of cell phones in the area until it finds a match.[16] While law enforcement can also obtain location information through requests to carriers for cell site location information,[17] IMSI catchers vary from carrier requests in at least two regards. IMSI catchers can typically be used without carrier assistance.[18] In addition, IMSI catchers produce extremely precise location information, in some cases "within an accuracy of 2 m[eters]."[19] In one federal case, the government conceded that the IMSI catcher located the defendant's wireless device precisely within a specific apartment in an apartment complex.[20] In Florida, Tallahassee police testified that by "using portable equipment" and going to "every door and every window" in a large apartment complex, they were able to identify the "particular area of the apartment that that handset was emanating from."[21] While carrier-provided cell site location information may under certain circumstances achieve similar precision, it is entirely variable, and depends on a number of factors, including the density of cell towers.[22]

Third, IMSI catchers are capable of capturing the content of communications, such as voice calls and text messages.[23] The devices used by the federal government are likely configured to disable the content intercept function; as the United States Department of Justice ("DOJ") acknowledges, a wiretap order under the heightened Title III standard (18 U.S.C. § 2518) would otherwise be necessary.[24] While some devices can be configured to intercept content, we are not aware of instances in which law enforcement has deployed an IMSI catcher in this fashion and the primary governmental uses appear to be identifying a phone's unique numeric identifier or location.

Several aspects of the technology are salient.

First, an IMSI catcher scoops up information from third parties, not just the target of an investigation. The type of IMSI catcher currently used by law enforcement mimics a wireless company's network equipment, sending signals to and triggering an automatic response from third parties' mobile devices.[25] DOJ concedes as much, as one of its template applications pertaining to IMSI catchers builds in the contingency that "any cellular phone that is within close proximity to the government device . . . may autonomously register with the device."[26] The devices also may disrupt third parties' network connectivity,[27] although DOJ contends that its policy is to take steps to "minimize any potential temporary disruption of service" to "non-target telephones," "by operating the device for limited duration and only when the cellsite information acquired from the provider indicates that the Subject Telephone is operating nearby."[28]

Second, the device broadcasts electronic signals that penetrate the walls of private spaces not visible to the naked eye, including homes and offices.[29] Depending on the device's signal strength, the broadcast radius can reach up to "several kilometers,"[30] allowing the IMSI catcher to scoop up information from any and all private locations in the area.

Third, an IMSI catcher *forces* cell phones to transmit signaling information.[31] As one law enforcement officer has described it, the government's device "actually captures the phone" and "direct[s] the signal from the [carrier's] tower to [the government's] equipment."[32]

Fourth, an IMSI catcher operates in the same basic manner – mimicking a base station and forcing an automatic response from devices in the immediate vicinity – regardless of the type of signaling information captured (unique numeric identifier or location). As DOJ explains:

> A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number ("MIN," *i.e.*, telephone number) and electronic serial number ("ESN," *i.e.*, the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identify the cell location and geographical sub-sector for which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on….If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/triggerfish would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected).[33]

Thus, an IMSI catcher operates in the same fashion, engaging in the same dragnet for information, regardless of whether the government ultimately filters the information obtained for a phone's unique numeric identifier or its location.

III. What kind of court authorization, if any, does the government currently obtain to use the device?

Although the full extent of government use of IMSI catchers remains to be revealed, even less is known about the legal process used by the government when deploying this technology. With respect to federal use, there are a handful of public DOJ documents that reference this technology.[34] The guidance and best practices set forth in these documents are somewhat internally inconsistent. DOJ has resisted disclosing further information about its policies, practices, and procedures for using this device.[35]

A. No court authorization?

In some instances, law enforcement entities, at least at the state and local level, are not obtaining any court authorization to use the device. The police department in Tucson, Arizona, has admitted in court-filed pleadings that while it has used IMSI catchers on at least five occasions, it has never obtained a warrant to do so and has no records of having obtained any other kind of court order authorizing use of the device; similar revelations have been made in Sacramento, California where the Sheriff almost certainly has a IMSI catcher, but the District Attorney's Office and superior court judges state they have no knowledge of the device being used.[36]

B. Pen register/trap and trace order?

It appears that DOJ recommends that the government obtain an order under the Pen Register/Trap and Trace Statute ("Pen/Trap Statute") when using an IMSI catcher to identify a target phone's unique numeric identifier or location. The DOJ documents are somewhat inconsistent and it is unclear if DOJ's position is that a Pen/Trap order is necessary or merely a "best practice."

Under the Pen/Trap Statute, the government may obtain an order authorizing installation of a pen register or trap and trace device upon an application certifying that "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2). A pen register is typically understood to be a device that records the numbers dialed by a particular telephone; a trap and trace device records the incoming numbers to a telephone.[37] The Pen/Trap Statute was amended in 2001 to expand the definition of pen/trap devices to include not only devices that capture incoming and outgoing numbers, but also those that capture "signaling information."[38]

DOJ has taken the following positions:

- *Pen/Trap order necessary and sufficient to obtain numeric identifier and location information*. DOJ's 2005 Electronic Surveillance Manual states that a Pen/Trap order "must be obtained by the government before it can use its own device to capture the [unique numeric identifier] of a cellular telephone" and that a Pen/Trap order would also suffice to obtain location information.[39]

- *Pen/Trap order merely considered a "best practice" to obtain numeric identifier and location information.* Elsewhere, however, the same manual states: DOJ "[does] not concede that a device used to receive[s] radio signals, emitted from a wireless cellular telephone" and that "identif[ies] that telephone to the network," in other words, an IMSI catcher, constitutes a 'pen register' or 'trap and trace' device," but recommends an application for court authorization "out of an abundance of caution."[40] A 2008 PowerPoint training on "Cellular Tracking and Other Legal Issues" produced by the FBI in a FOIA lawsuit describes use of a Pen/Trap order as a "best practice" when using "Cellsite Simulators" to "[i]dentify a target phone **or** . . . [l]ocate a phone."[41]

- *Pen/Trap order necessary to obtain numeric identifier; position as to location information unclear.* A 2013 DOJ document asserts that a Pen Trap Order is necessary (*i.e.*, not merely a "best practice" or sought "out of an abundance of caution"), at least when the government seeks to identify the unique numeric identifier of a target phone using an IMSI catcher.[42] The publicly available portion of the 2013 document does not address DOJ's position with respect to using a Pen/Trap order to obtain a target phone's location with an IMSI catcher.

Any argument that a Pen/Trap order suffices to obtain location information is noteworthy in light of the Communications Assistance for Law Enforcement Act ("CALEA"). Congress enacted CALEA in 1994 for the purpose of requiring telecommunications carriers to adopt the technology necessary to provide, upon appropriate court order, content and "call-identifying information" to law enforcement.[43] The statute, however, expressly prohibits use of a Pen/Trap order to obtain location information: "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 . . . ."[44] DOJ's 2005 Electronic Surveillance Manual states that the government can, notwithstanding CALEA, use an IMSI catcher to obtain location information because CALEA's "prohibition applies only to information collected by a provider and not to information collected directly by law enforcement authorities."[45]

C. Hybrid Order?

Although some DOJ materials state that a Pen/Trap order suffices when the government uses an IMSI catcher to obtain location information, other materials appear to recommend use of a so-called "hybrid order" for this purpose.

A hybrid order is the same type of order that DOJ contends is sufficient to obtain prospective, or real-time, cell site location information from a wireless carrier.[46] As noted above, CALEA prohibits the government from relying "solely" on a Pen/Trap order to obtain location information from a carrier.[47] Under the hybrid theory, the government justifies acquisition of location information from wireless carriers by combining the Pen/Trap Statute with the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(d), which authorizes the government to obtain records from a provider pertaining to certain kinds of records or information pertaining to customers or subscribers. The relevant provision of the SCA requires the government to set forth "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."[48] Notably, a significant majority of courts have held that a hybrid order does *not* suffice to obtain prospective cell site location information, and that a warrant is instead required.[49]

An IMSI catcher, like an order for prospective cell site information, obtains location information in real time. DOJ's 2005 Electronic Surveillance Manual includes a template application for a hybrid order that authorizes use of a device that appears to be an IMSI catcher.[50] Although the template application refers to the device as a "pen register," the template's brief allusions to the manner in which the device operates strongly suggests that the device at issue is actually an IMSI catcher.[51]

Note that although DOJ's template application for a hybrid order provides some description of how the device functions, actual IMSI catcher applications filed in court provide no such information. In *United States v. Rigmaiden,* 844 F. Supp. 2d 982 (D. Ariz. 2012), for example, the government ultimately acknowledged it used an IMSI catcher, but its affidavit in support of the relevant court order nowhere referred to an IMSI catcher or explained how the

device functions. The affidavit instead made fleeting references to an unspecified "mobile tracking device," and the only description of how the device works stated that "[t]he mobile tracking equipment ultimately generate[s] a signal that fixes the geographic position of the Target [Device]."[52]

In short, DOJ appears to take the position that a hybrid order suffices to authorize use of an IMSI catcher to identify a target phone's location in real time, even though most courts have rejected the related argument that a hybrid order suffices when the government seeks to obtain real-time location information from a carrier. In addition, DOJ's template application for an order authorizing use of an IMSI catcher to obtain location information nowhere uses the term "IMSI catcher" or any other related term, and instead is styled as an application to install a "pen register." Finally, even though DOJ's template application for an IMSI catcher contains some description (albeit minimal) of how the technology functions, actual IMSI catcher applications filed in court do not.

D. Warrant?

In at least some instances, the federal government has sought warrants to use a StingRay to obtain location information.[53] Warrants, of course, require, among other things, the government to establish probable cause and to state with particularity the place to be searched, and the persons or things to be seized.[54]

IV. What guidance have courts offered on StingRays?

Only a handful of published decisions have addressed IMSI catchers.

The earliest reported decision involved an early-generation IMSI catcher called a "digital analyzer." *See In re Application for an Order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. 197 (C.D. Cal. 1995) (hereinafter "*In re Digital Analyzer*"). The government submitted an application for a Pen/Trap order to use the device to detect the unique numeric identifier of the cell phones used by five subjects of a criminal investigation. *See id.* at 199. The opinion contains two main holdings, each somewhat difficult to reconcile with the other. The government contended, and the court agreed, that no court order was required because the device – which is not physically attached to a telephone – did not fall under the statutory definition of a pen register or trap and trace device then in effect. *See id.* at 199-200 (citing 18 U.S.C. § 3127(3) & (4)). The court went on to hold, however, that to the extent some procedure was required, the government's proposed procedure lacked sufficient safeguards. *See id.* at 201. The court then denied the application for an order authorizing use of the device, without prejudice to a renewed application proposing greater safeguards. *See id.* at 202.

More recently, the court in *In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device,* 890 F. Supp. 2d 747 (S.D. Tex. 2012) (hereinafter "*In re StingRay*"), also denied the government's application for a Pen/Trap order to use an IMSI catcher to ascertain a suspect's telephone number. Although the statute had been expanded in 2001, after *In re Digital Analyzer*, to set forth a broader definition of "pen

register,"[55] the court still concluded that the statute was inapplicable. *See id.* It held that a Pen/Trap order is only available for known telephone numbers, and not to ascertain unknown numbers. *See id.* But, unlike the Central District of California, the Southern District of Texas did not hold that, given the inapplicability of the Pen/Trap Statute, no court order was required. Instead, it strongly suggested that a warrant would instead be necessary. *See id.* at 752. It also criticized the government's application for failing to "explain the technology, or the process by which the technology will be used to engage in electronic surveillance" or to address key facts about the government's proposed operation of the device and handling of third-party data. *Id.* at 749.

This case suggests that even technology savvy magistrates, such as those in the Southern District of Texas, are not familiar with the device and have many unanswered questions about how it works. As discussed above, the template application to use an IMSI catcher in DOJ's Electronic Surveillance Manual nowhere explicitly mentions an IMSI catcher and instead refers only to "pen register" devices, and actual applications and orders to use IMSI catchers filed in court similarly make no explicit reference to IMSI catchers, let alone how they work.[56] It is thus very likely that judicial officers across the country are unaware that they are being presented with requests and granting authorization to use IMSI catchers.

In *Rigmaiden*, a *pro se* defendant accused of electronic tax fraud succeeded through creative discovery in forcing the government to concede what the government had not acknowledged in any other criminal prosecution until that point, in particular, that:

- the government used a "cell site simulator" to locate the defendant's wireless device;
- the cell site simulator "mimicked a Verizon Wireless cell tower and sent signals to, and received signals from," the defendant's device; and
- the cell site simulator "located [the defendant's device] precisely within Defendant's apartment – Unit 1122 of the Domicilio Apartments."

Id. at 995-96. In addition to these highly noteworthy factual concessions, the government also conceded that the use of the cell site simulator was sufficiently intrusive to constitute a search within the meaning of the Fourth Amendment. *Id.* This was highly significant, in light of the position set forth in DOJ's Electronic Surveillance Manual, that a Pen/Trap or hybrid order suffices. *See supra* Section III.

Thereafter, Rigmaiden brought a motion to suppress on numerous grounds, including a challenge to the use of the IMSI catcher. The government contended that it had obtained a warrant to use the device. Rigmaiden, joined by *amici* ACLU and the Electronic Frontier Foundation, contended, among other things, that the government had withheld constitutionally material information from the issuing magistrate, rendering the order on which the government relied an invalid general warrant. The application failed to alert the issuing magistrate that the government intended to use an IMSI catcher and omitted constitutionally material information about how the technology works, such as its impact on third parties.[57] Emails obtained by the ACLU of Northern California in a FOIA lawsuit suggest that the government's failure to disclose to the court information about IMSI catchers in its applications for authorization to use the

device was not isolated to the *Rigmaiden* case.[58]

Unfortunately, the court denied the motion to suppress. *See United States v. Rigmaiden*, 2013 WL 1932800 (D. Ariz. May 8, 2013). It held that information about how the IMSI catcher operates was a mere "detail of execution which need not be specified." *Id.* at *20. The court also dismissed the significance of the government's capturing of third-party information because the government expunged the data. *Id.* at *22. Finally, although the court found that the government did not violate the Fourth Amendment, it also found that the government acted in good faith because the "agents were using a relatively new technology" and lacked legal precedent on the type of warrant to be sought. *Id.* at *31.

In *United States v. Espudo*, 954 F. Supp. 2d 1029 (C.D. Cal. 2013), an IMSI catcher was also used. But the court denied the motion to suppress, based on a government affidavit stating that evidence from the IMSI catcher was not used to further the investigation. *See id.* at 1045. In *Thomas v. State*, 127 So. 3d 658 (Fla. Dist. Ct. App. 2013), the police used unspecified technology to track a cell phone to the defendant's home. *Id.* at 659-60 & n.2. The ACLU unsealed a transcript from a hearing in the court below and it confirms that the technology at issue was an IMSI catcher.[59] The appellate court in *Thomas* did not address the legality of the use of the technology and resolved the case on other grounds. An IMSI catcher also was used in *Wisconsin v. Tate*, No. 2012AP336 (Wis. Ct. App. June 5, 2011), a case now pending before the Wisconsin Supreme Court.[60] It is not clear if the court will reach the IMSI catcher issue, which was not addressed by the court below.

V. How can you tell if the government used a StingRay in your case?

There are very few cases addressing IMSI catchers, leaving the area ripe for litigation. The challenge lies in determining whether an IMSI catcher was even used. Even in those instances where the government obtains some kind of court authorization to use the device, the application and order will very likely *not* refer to IMSI catcher technology. The FBI has publicly acknowledged that it "has, as a matter of policy, for over 10 years, protected this specific electronic surveillance equipment and techniques from disclosure, directing its agents that while the product of the identification or location operation can be disclosed, neither details on the equipment's operation nor the tradecraft involved in use of the equipment may be disclosed."[61] There are, however, several indications that the government may have used an IMSI catcher in any particular case.

A. Terminology

While technologists use the term "IMSI catcher," DOJ does not and instead uses widely varying, inconsistent terms, including, but not limited to, digital analyzer, cell site simulator, cell site emulator, cell site monitor, triggerfish, StingRay, kingfish, amberjack, hailstorm, and WITT, in reference to the FBI's Wireless Intercept Tracking Team. Be on the lookout for any of the foregoing terms. But the government may also conceal use of an IMSI catcher by instead referring to a "mobile tracking device" or "pen register," even though the former term typically refers to GPS devices (or so-called "bumper beepers"), and the latter to requests for information

from telephone service providers.[62] In some instances, the government is even referring to an unspecified "confidential source."[63] An indicator of potential IMSI catcher use, more reliable than terminology, is how the government's investigation actually unfolded.

B. How did the government find out your client's cell phone number?

IMSI catchers can be used to capture the unique numeric identifier, such as an Electronic Serial Number or Mobile Identity Number, of a wireless device, and public DOJ documents clearly contemplate use of this device for this purpose.[64] The fact that applications and court orders refer only to pen register devices does not rule out the possibility that an IMSI catcher was used.

Obtaining the ESN, IMSI, MIN, or other identification number of a suspect's phone is a necessary predicate for a wiretap order or an order to a carrier for call records. If the government obtained such orders in your case, but it is unclear how it obtained your client's cell phone number, or the only explanation is a highly cryptic reference to an unspecified "confidential source" or "source of information" with no details as to the source, consider pursuing the issue of an IMSI catcher in discovery. (An alternative possibility is that the government obtained the number through another surveillance program known as the "Hemisphere project."[65])

C. How did the government locate your client?

IMSI catchers are also used to locate targets of an investigation. The government is very likely to offer alternative explanations for how it located a suspect to avoid disclosing that a StingRay was used. One email from an FBI Special Agent in *Rigmaiden* read: "The tech guys were able to narrow the signal to 3 apartments. Today, we will be doing as much follow up research as we can. *We need to develop independent probable cause of the search warrant… FBI does not want to disclose the [redacted] (understandably so).*" (Ellipsis in original).[66] If there was any point in the investigation when the government was able to identify the location of your client, and even if the government offered non-StingRay related explanations for how it did so, consider pursuing this issue in discovery.

VI. Key legal arguments to raise if an IMSI catcher was used

There are several broad categories of constitutional concerns that arise from IMSI catcher use. First, use of an IMSI catcher triggers Fourth Amendment scrutiny because it constitutes both a search and a seizure within the meaning of the Fourth Amendment. Second, there is a strong argument that IMSI catchers can never be used consistent with the Fourth Amendment because they engage in the electronic equivalent of a "general search." Third, law enforcement must at least obtain a warrant; a statutory order does not suffice. Fourth, even if law enforcement obtained a warrant, it is likely invalid. While precise legal arguments would vary depending on the actual language of the warrant, one of two scenarios is likely. Any warrant was likely based on an *inaccurate* affidavit that contained materially misleading statements or omissions about the government's intended use of an IMSI catcher; those material statements and omissions render a warrant invalid. Alternatively, if the warrant is *accurate* in describing

the government's intended and actual use of the IMSI catcher, then it almost certainly does not satisfy particularity and breadth requirements and is facially invalid. Additional and more specific legal arguments are almost certainly available, depending on the particular facts and circumstance of each case.

A. IMSI catchers trigger Fourth Amendment scrutiny

IMSI catchers are so intrusive that they violate both reasonable expectations of privacy and property interests. Their use therefore constitutes a search within the meaning of the Fourth Amendment. They also give rise to Fourth Amendment seizures.

1. Use in connection with residences

IMSI catchers invade reasonable expectations of privacy because they can be used to ascertain the location or unique numeric identifier of a suspect's cell phone, while the suspect is located inside her private residence or other private space.[67] The use of an electronic device to determine information about the interior of private residences and other constitutionally protected spaces clearly constitutes a Fourth Amendment search. *See United States v. Karo*, 468 U.S. 705, 715 (1984) (placing beeper into can of ether that was taken into a residence constituted a search because it "reveal[ed] a critical fact about the interior of the premises"); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (thermal imaging to detect heat from home constituted search).

An IMSI catcher allows the government to ascertain whether a suspect is located inside a residence or the number of the cell phone she chooses to use while inside. This is all information "about the interior of the premises that the Government is extremely interested in knowing and that it could not otherwise have obtained without a warrant." *Karo*, 468 U.S. at 716.

To be sure, the Supreme Court has held that individuals lack a reasonable expectation of privacy for incoming and outgoing telephone numbers because the information is "voluntarily" conveyed to the third party telephone company. *See Smith v. Maryland*, 442 U.S. 735, 745-46 (1979) (use of pen register does not constitute search). Relying on this rationale, a number of courts have held, in the context of government requests for cell site location information from wireless carriers, that individuals lack a reasonable expectation of privacy in the location of their phone because the information was voluntarily conveyed to the carrier. *See, e.g.*, *In re Application for Historical Cell Site Data*, 724 F.3d 600, 614-15 (5th Cir. 2013) (hereinafter "*Fifth Circuit Decision*"); *United States v. Skinner*, 690 F.3d 772, 778-79 (6th Cir. 2012); *but see In re Application for an Order Directing a Provider of Electronic Comm. Serv. to Disclose Records*, 620 F.3d 304, 317 (3d Cir. 2010) (rejecting government's argument that subscribers lack reasonable expectation of privacy in cell site location information because they have shared their information with third party communications provider).

But these cases are distinguishable. First, when the government uses an IMSI catcher, it obtains the information directly, not from a third party. *Cf. Smith*, 442 U.S. at 744 (telephone subscriber "assume[s] the risk that the company would reveal to police the numbers he dialed"); *Fifth Circuit Decision*, 724 F.3d at 610 ("the Government . . . draws a line based on whether it is

the Government collecting the information . . . or whether it is a third party, of its own accord and for its own purposes, recording the information"). Second, there is nothing "voluntary" about the information obtained by an IMSI catcher, which "force[s]" cell phones to transmit signaling data.[68] Third, an individual has a reasonable expectation of privacy about her information when she is inside a residence or other private location, even if she would have no such expectation for the same type of information when in a public place. *Compare United States v. Knotts*, 460 U.S. 276, 281 (1983) (use of bumper beeper to track suspect's location did not constitute search because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."), *with Karo*, 468 U.S. at 715 (use of beeper to determine suspect "was actually in the house" constituted search: "[t]he case is thus not like *Knotts,* for there the beeper told the authorities nothing about the interior of Knotts' cabin"). When using an IMSI catcher to locate someone or to identify the number of the phone she chooses to use while inside a private location, the government is obtaining "a critical fact about the interior of the premises," *Karo,* 468 U.S. at 715, rather than information emitted from a phone while the suspect is "traveling on public thoroughfares." *Skinner,* 690 F.3d at 781. The Supreme Court has warned that even if a rudimentary form of surveillance technology appears not to effect a "'significant' compromise of the homeowner's privacy," "we must take the long view" when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion." *Kyllo,* 533 U.S. at 40.

Relatedly, use of an IMSI catcher in connection with residences may constitute a Fourth Amendment search under a property rationale. To the extent investigators use portable IMSI catchers while walking within the curtilage of a home,[69] the use constitutes a search because it entails a physical intrusion on constitutionally protected areas. *See Florida v. Jardines,* 133 S. Ct. 1409, 1417 (2013) (use of drug-sniffing dog on front porch of home constituted search under trespass theory); *United States v. Broadhurst,* 2012 WL 5985615 at *6 (D. Or. Nov. 28, 2012) (use of "Shadow," a handheld device that scans wireless networks to determine devices connected to it, while on front lawn constituted search under trespass theory). Even without a physical intrusion into the curtilage by the operator of an IMSI catcher, the IMSI catcher itself broadcasts electronic signals that penetrate the walls of private locations. *See supra* Section II & n.29. This "unauthorized physical penetration into the premises" constitutes 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); *but see United States v. Jones,* 132 S. Ct. 945, 949, 953 (2012) (holding that installation and monitoring of GPS on suspect's vehicle constituted search because of "physical intrusion" "for the purpose of obtaining information" but observing that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to [reasonable expectation of privacy] analysis").

2. Use in public

IMSI catcher use in public locations may also trigger Fourth Amendment scrutiny.

An "intrusion on possessory interests" gives rise to a Fourth amendment seizure, even when it occurs in a public place. *United States v. Place,* 462 U.S. 696, 705 (1983); *see also id.* at

707 (seizure occurred when agent told defendant at airport he was going to take luggage). The types of IMSI catcher currently used by the government "capture" a target cell phone and "force" it to disconnect from the carrier's base station and instead "to register" with the government's fake base station.[70] By commandeering a target phone in this fashion, the government seizes it.

IMSI catcher use in public places may also constitute a search, depending on the type of data collected and the duration of the surveillance. For example, IMSI catchers are capable of intercepting content. *See supra* Section II. Although DOJ materials make clear that such functions should be disabled absent a Title III wiretap order (18 U.S.C. § 2518),[71] little is known about state and local government protocols for using these devices. In any event, it is essential to obtain discovery about the type of data that was actually collected by the government and, to the extent voice, email, text messages or other private communications were obtained, the Fourth Amendment and Title III or analogous state wiretap statutes are triggered. *See United States v. U.S. Dist. Ct. for the E. Dist. of Michigan, S. Div.*, 407 U.S. 297, 313 (1972) ("[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."); *Katz v. United States*, 389 U.S. 347, 352 (1967) (caller in phone booth had reasonable expectation of privacy: "To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication"); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (reasonable expectation of privacy in content of emails).

In addition, if the government used the IMSI catcher to monitor location over a prolonged period, [72] its use may constitute a search.[73]

B. IMSI catchers engage in the electronic equivalent of a "general search" and their use therefore violates the Fourth Amendment

IMSI catchers engage in the electronic equivalent of the general searches prohibited by the Fourth Amendment. 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, 481-82 (1965). "General searches have long been deemed to violate fundamental rights. It is plain that the [Fourth] [A]mendment forbids them." *Marron v. United States*, 275 U.S. 192, 195 (1927). "[T]he Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched and the persons or things to be seized.' The manifest purpose of this particularity requirement was to prevent general searches." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *see also Marron*, 275 U.S. at 196 (particularity requirement prohibits general searches by "prevent[ing] the seizure of one thing under a warrant describing another"). By scooping up all manner of information from a target cell phone, as well as all nearby cell phones, an IMSI catcher engages in "general, exploratory rummaging." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *see also United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) ("[T]he wholesale *seizure* for later detailed examination of records not described in a warrant . . . has been characterized as 'the kind of investigatory dragnet that the fourth amendment was designed to prevent.'").

The device scoops up *all* signaling information from a suspect's cell phone, rather than targeting evidence of particular crimes as to which there is probable cause. *See, e.g., Groh v. Ramirez,* 540 U.S. 551, 563 (2004) (finding invalid warrant that authorized seizure of suspect's house and that failed to identify any particular items and explaining that "a search warrant for 'evidence of crime' was '[s]o open-ended' in its description that it could 'only be described as a general warrant'") (quoting *United States v. Stefonek,* 179 F.3d 1030, 1032-33 (7th Cir. 1999)); *United States v. Kow,* 58 F.3d 423, 427-28 (9th Cir. 1995) (warrant overbroad where it authorized widespread seizure of documents at business even though affidavit contained only probable cause pertaining to profit skimming and tax violations); *United States v. Cardwell,* 680 F.2d 75, 77 (9th Cir. 1982) (warrant overbroad where it permitted seizure of all of "appellants' business papers" that were "instrumentality or evidence of violation of the general tax evasion statute"). For example, if an individual is suspected of using a phone to engage in criminal activity in the park during the day, what is the probable cause to obtain signaling data from the phone she uses when she is at home at night? The constitution "demands" that the surveillance "be conducted in such a way as to minimize the" collection of information unsupported by probable cause. *United States v. Koyomejian,* 970 F.2d 536, 542 (9th Cir. 1992) (adopting minimization and other requirements, in addition to probable cause, for warrants to conduct video surveillance).

In addition, an IMSI catcher also scoops up information from the devices of innocent third parties as to whom the government has no probable cause, or reasonable suspicion, whatsoever. *See United States v. Whitney,* 633 F.2d 902, 907 (9th Cir. 1980) ("The command to search can never include more than is covered by the showing of probable cause to search.") (internal quotation marks, citation omitted).

In short, IMSI catchers operate in indiscriminate fashion, scooping up too much information, from too many people. This is precisely the type of general rummaging prohibited by the Fourth Amendment.

C. Statutory orders do not suffice to authorize IMSI catcher use

At a minimum, however, the government should presumptively obtain a probable cause warrant because the government's use of an IMSI catcher constitutes a Fourth Amendment search and/or seizure. *See supra* Section VI-A; *Kyllo,* 533 U.S. at 40 (surveillance that constitutes "search" is "presumptively unreasonable without a warrant").

DOJ contends that a Pen/Trap or hybrid order suffices. *See supra* Section III-B&C. But these statutory orders – based on "relevant" or "relevant and material" standards (*see* 18 U.S.C. § 3122(b)(2); 18 U.S.C. § 2703(d)) – do not satisfy the Fourth Amendment's probable cause requirement or other safeguards.

Note also that DOJ materials suggest that the government seeks a Pen/Trap order when using an IMSI catcher to obtain a device's unique numeric identifier, but a hybrid order to obtain location information. *See supra* Section III-B&C. Warrants, rather than statutory orders, should

be obtained in both cases. There is no reason to apply a different legal standard depending on the government's motivation in using the IMSI catcher. This is so because IMSI catcher technology operates in the same fashion and captures the same type of signaling data – and thus invades privacy expectations and property interests, and effects seizures to the same degree – whether the government deploys the device for the purpose of obtaining the unique numeric identifier of a suspect's device in a known location, or the location of a suspect whose device's numeric identifier is known. In both instances, the IMSI catcher engages in the same dragnet.

D. Even if the government obtained a warrant, use of an IMSI catcher is still invalid

Even if a court were to conclude that IMSI catchers are not *per se* violative of the Fourth Amendment and assuming law enforcement obtained a warrant, there are likely strong arguments that use of an IMSI catcher was still illegal. It is impossible to anticipate all of the potential arguments, which will depend on the language of the warrant and the execution of the search. This section sets forth potential challenges that address two alternative scenarios, one in which the warrant and application fail to describe the government's intended use of an IMSI catcher and another in which they do.

1. The government's omission of information about new surveillance technology from a warrant application prevents courts from exercising their constitutional oversight function and would render a warrant invalid

A warrant application for authorization to use an IMSI catcher is very likely to be *inaccurate*. *See supra* Section III-C & V at n.61 (discussing FBI policy of non-disclosure). In particular, it may omit the critical fact that the government intends to use an IMSI catcher, provide affirmatively misleading information that the government intends to use a pen register instead, or fail to provide any information on what the technology is and how it works.[74]

New technology often raises complex and cutting edge constitutional questions. *Cf., e.g., Jones,* 132 S. Ct. at 946-47 (addressing whether installation and monitoring of GPS device constitutes a "search" within the meaning of the Fourth Amendment). These are questions for the courts, and not the government unilaterally, to decide. 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). 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.,* 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (hereinafter "*CDT*").

Information about the government's intended use of new technology, and how the technology works, is material to pressing constitutional questions, such as whether all aspects of the search are supported by probable cause. The courts cannot exercise their constitutional oversight function if deprived of this information. A warrant application that fails to disclose the

government's intended use of an IMSI catcher, or to provide basic information about the technology, omits material information. Equally troubling is an application that refers to a "pen register device" when the government actually intends to use an IMSI catcher. Both circumstances require suppression. *See United States v. Rettig*, 589 F.2d 418, 422-23 (9th Cir. 1979) (suppressing information obtained from warrant procured on basis of material omission). At a minimum, however, the defendant in such a case should be entitled to an evidentiary hearing on whether the omission of information about the IMSI catcher is intentional and material. *See Franks v. Delaware*, 438 U.S. 154 (1978).

a. A warrant that fails to disclose the government's intended use of an IMSI catcher is predicated on a material omission

Information about the government's intended use of an IMSI catcher is material. When the government omits this information from its warrant application, it interferes with the court's ability to supervise the search and any evidence obtained from such a search should be suppressed.

The misleading statements and/or omissions are likely to involve: (a) failure to state that the government intends to use an IMSI catcher or, worse, an affirmative statement that the government intends to use a "pen register" device, (b) failure to acknowledge that the IMSI catcher will scoop up all signaling information from phones used by the target, including from phones and at times and locations unrelated to suspected criminal activity, (c) failure to acknowledge that the IMSI catcher will scoop up all signaling information from phones used by third parties as to whom the government lacks probable cause or even reasonable suspicion, and/or (d) failure to acknowledge that IMSI catchers are capable of capturing content and to address whether that function has been disabled on the particular device.[75]

"Just as the Fourth Amendment prohibits warrantless searches generally, so too does it prohibit a search conducted pursuant to an ill-begotten or otherwise invalid warrant." *Bravo v. City of Santa Maria*, 665 F.3d 1076, 1083 (9th Cir. 2011). One of the purposes of the Fourth Amendment's particularity requirement is to "ensure[] 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." *Spilotro*, 800 F.2d at 963. 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 failing to obtain warrant for cocaine-related evidence, government went to different magistrate seeking warrant for marijuana-related evidence, and then conducted broad search including for cocaine-related items). "By failing to advise the judge of all the material facts, including the purpose of the search and its intended scope, the officers deprived him of the opportunity to exercise meaningful supervision over their conduct and to define the proper limits of the warrant." *Id.* at 422. "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; *see also Liston v. Cnty. of Riverside*, 120 F.3d 965, 974 (9th Cir. 1997) (finding information material where "the magistrate would not have issued the warrant without requiring additional information and in addition imposing specific restrictions on its execution").[76]

Information that the government intends to use an IMSI catcher would prompt a reasonable magistrate to "require[e] additional information." *Id.* In ruling on a statutory application to use an IMSI catcher, for example, one court conducted "an *ex parte* hearing . . . with the special agent leading the investigation," and faulted the government's application for not "explain[ing] the technology, or the process by which the technology will be used to engage in the electronic surveillance." *In re StingRay*, 890 F. Supp. 2d at 749. The court was specifically troubled that the application contained "no discussion" about the manner in which the government intended to operate the StingRay, and identified the numerous factual issues it believed material to evaluating the government's application. *See id.* This included information about "how many distinct surveillance sites they intend to use, or how long they intend to operate the StingRay equipment to gather all telephone numbers in the immediate area. It was not explained how close they intend to be to the Subject before using the StingRay equipment. They did not address what the government would do with the cell phone numbers and other information concerning seemingly innocent cell phone users whose information was recorded by the equipment." *Id.*

In addition, some IMSI catchers are capable of capturing content. *See supra* Section II. Notification that the government intends to use an IMSI catcher would prompt a reasonable magistrate to inquire whether the device the government proposes to use has such a feature and, if so, whether it has been disabled. *Cf.* 18 U.S.C. § 2518 (setting forth heightened standard for wiretap orders).

Factual information of the type discussed above is necessary for the court to exercise its constitutional duty to "define the proper limits of the warrant." *Rettig*, 420 U.S. at 422. Such limits include restrictions that would minimize the intrusive impact of the IMSI catcher on the suspect, for example, by setting limits on when, where, and for how long the device is operated (if the suspect is only believed to engage in criminal activity in parks in the afternoon, there is no probable cause to collect information from the suspect when he is sleeping at home at night, particularly when he may be using a different phone at that time and location), as well as by prohibiting interception of content (absent compliance with requirements for a Title III wiretap).

These or similar limitations (*e.g.*, prohibitions against using the device in dense residential areas or at night when third parties are likely to be at home, restrictions on the size of geographic area in which the device is used) would also serve to minimize the intrusion on third parties. In addition to limiting the amount of third-party information collected, there is the question of what to do with any such information (delete it immediately, segregate and redact).[77] It is for the issuing magistrate, not the government, to determine how best to balance the government's need for information, third-party privacy, and the need to preserve evidence "helpful to the accused." *United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) ("[S]uppression 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.").

Also noteworthy is any case in which the government submits an application seeking authorization to use a "pen register device," when the government actually intends to use an IMSI catcher. *See supra* Section III & nn.50 & 51 (discussing template DOJ application). Such an application would be especially misleading. A pen register device, by definition, is "a device or process which records . . . signaling information transmitted by *an* instrument or facility, . . . provided, however, that such information *shall not include the contents* of any communication." 18 U.S.C. § 3127(3) (emphasis added). The statutory definition does not encompass a device that records signaling information from *multiple* instruments in its vicinity, which is precisely what an IMSI catcher does. Nor does it encompass devices, like IMSI catchers, which are capable of capturing *content*. Relying on the statutory definition of "pen register," a court would be lulled into believing there were no need to seek additional information about the kind of data intercepted by the IMSI catcher from the target, or to impose restrictions related to third parties.

In short, the failure to apprise the court that IMSI catchers scoop up all signaling information from target and third-party cell phones leaves a court in the dark about the "intended scope" of the search and thus deprives the court "of the opportunity to exercise meaningful supervision over [the officers'] conduct and to define the proper limits of the warrant." *Rettig*, 589 F.2d at 422.[78] A warrant procured under these circumstances can "bec[o]me an instrument for conducting a general search." *Id.* at 423. As a result, "all evidence seized during the search must be suppressed." *Id.*[79]

b. A defendant is entitled to a *Franks* hearing

Alternatively, a defendant should be entitled to an evidentiary hearing under *Franks* to determine whether the affidavit misrepresented or omitted material facts. "To allow a magistrate to be misle[]d . . . could denude the probable cause requirement of all meaning. Accordingly, a Fourth Amendment violation occurs where the affiant intentionally or recklessly omitted facts required to prevent technically true statements in the affidavit from being misleading." *Liston*, 120 F.3d at 973 (internal quotation marks, citations omitted). A defendant seeking a *Franks* hearing must "make[] a two-fold showing: intentional or reckless inclusion or omission, and materiality." *United States v. Bennett*, 219 F.3d 1117, 1124 (9th Cir. 2000).

Omissions or misrepresentations pertaining to the government's intended use of an IMSI catcher are material for the reasons discussed above. *See supra* Section VI-D-1-a. They are also intentional.

In court-filed pleadings, the FBI has acknowledged that it has a longstanding policy of not disclosing information about IMSI catchers.[80] In addition, an internal email from the United States Attorney's Office for the Northern District of California shows that "many" law enforcement agents in that district, under the auspices of pen register orders, were using the device – but without "mak[ing] that explicit" in the application; even worse, this occurred *after* the federal magistrates had expressed "collective concerns" that pen register orders would not suffice to authorize use of the device.[81] An email produced in discovery in *Rigmaiden* stated that the investigative team "need[ed] to develop independent probable cause of the search warrant … FBI does not want to disclose the [redacted] (understandably so)."[82] In addition, the Sarasota

Police Department in Florida acknowledged, in an email obtained by the ACLU of Florida through a public records request, that, "at the request of U.S. Marshalls," local police officers "simply refer to [information from an IMSI catcher] as ' . . . information from a confidential source regarding the location of the suspect.' To date this has not been challenged . . . ."[83] All of this demonstrates that the government's omission of information about IMSI catchers – or affirmative misrepresentation that it is instead using a "pen register" device or obtaining information from a "confidential source" – is hardly innocent.[84]

Even in the absence of such stark revelations, it seems clear that misrepresentations and omissions pertaining to the government's use of IMSI catchers are intentional. The issue is not whether the government should have followed-up on or disclosed facts not of its own making. *Cf. Bravo,* 665 F.3d at 1087, 1088 (where officer obtained a warrant to search home, even though he knew that suspect had received two-year prison sentence and thus not likely to be living at his prior residence, officer's "failure to . . . follow up and inquire about [the suspect's] custody status amounted to at least reckless disregard for the truth"). The government cannot disclaim responsibility for knowing what device it has chosen to use.

Nor can ignorance about the technology excuse any omission. The functioning of the technology has constitutional significance. It is therefore incumbent on the government to understand the technology and disclose it to the courts. *See In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(D),* Nos. C-12-670M, C-12-671M, 2012 WL 4717778 *702 (S.D. Tex. Sept. 26, 2012) (rejecting application for so-called "cell tower dump," *i.e.*, all information from specified cell towers: "[I]t is problematic that neither the assistant United States Attorney nor the special agent truly understood the technology involved in the requested applications. Without such an understanding, they cannot appreciate the constitutional implications of their requests. They are essentially asking for a warrant in support of a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment.").

* * *

In short, to the extent the warrant application fails to alert the issuing magistrate that the government intends to use an IMSI catcher, misleadingly states it intends to use a "pen register," or fails to provide basic information about what the technology is and how it works, the omissions are intentional and material. The defendant in such a case is therefore entitled to suppression or a *Franks* hearing, to ensure that the government is not permitted to conduct searches "pursuant to an ill-begotten or otherwise invalid warrant." *Bravo,* 665 F.3d at 1083.

2. A warrant that accurately describes the IMSI catcher's capabilities would be facially invalid

For the reasons discussed above, a warrant and application that *inaccurately* describes the government's intended use of an IMSI catcher should be held invalid. But it is possible that a warrant and application will *accurately* describe the proposed use of the device. In that, somewhat less likely event, the warrant will almost certainly fail to satisfy particularity or breadth requirements and should thus be held facially invalid.

Particularity. "Particularity is the requirement that the warrant must clearly state what is sought." *In re Grand Jury Subpoenas v. United States*, 926 F.2d 847, 856 (9th Cir. 1991). This means that the warrant must contain "limitations on which [items] within each category [can] be seized [and] suggest[] how they relate[] to specific criminal activity." *Kow*, 58 F.3d at 427. A warrant is not sufficiently particular if it "provide[s] the search team with discretion to seize records wholly unrelated to the" "crimes and individuals under investigation." *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 705 (9th Cir. 2009). A warrant that expressly authorizes the search that an IMSI catcher will actually perform – a dragnet for *all* signaling information from the suspect's wireless device and *all other* devices in the vicinity of the IMSI catcher – contains no practical limitations on the scope of the search and will authorize the government to search and seize information entirely unrelated to the specific criminal activity of which the target is suspected, as well as information from innocent third parties.

To be sure, courts will sustain warrants with "generic descriptions" of the information to be searched and seized "where the government lacked information necessary to describe the items to be seized more precisely." *Spilotro*, 800 F.2d at 966. But warrants involving IMSI catchers involve impermissibly "generic descriptions" because of the government's choice to use a technology that scoops up far more information than what actually "relate[s] to specific criminal activity." *Kow*, 58 F.3d at 427. That knowing choice does not excuse reliance on "generic descriptions." Indeed, the fact that searches performed by IMSI catchers are not susceptible of being described with particularity underscores the grave concern that IMSI catchers engage in the very general rummaging prohibited by the Fourth Amendment. *See Garrison*, 480 U.S. at 85 ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [particularity] requirement ensures that the search will be carefully tailored to its justification, and will not take on the character of the wide-ranging exploratory searches the framers intended to prohibit."); *CDT*, 621 F.3d at 1176 (noting, in context of searches for electronic information, "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant").

Overbreadth. Any warrant that accurately describes the search performed by an IMSI catcher but that fails to impose explicit restrictions on how and when it is used would also be overbroad because it would authorize the government to search and seize information from the defendant unrelated to specific suspected criminal activity and also information pertaining to third parties as to whom it lacks any probable cause.

"Courts have repeatedly invalidated warrants authorizing a search which exceeded the scope of the probable cause shown in the affidavit." *In re Grand Jury Subpoenas*, 926 F.2d at 857. A warrant is overbroad where the affidavit establishes probable cause to seize some but not all materials from the target of an investigation. *See, e.g.*, *Kow*, 58 F.3d at 427-28 (warrant overbroad where it authorized widespread seizure of documents at business even though affidavit contained only probable cause pertaining to profit skimming and tax violations); *Center Art Galleries-Hawaii, Inc. v. United States*, 875 F.2d 747, 750 (9th Cir. 1989) (warrant overbroad where it "failed to limit the warrants to items [at art gallery] pertaining to the sale of Dali artwork despite the total absence of any evidence of criminal activity unrelated to Dali"); *Spilotro*, 800

F.2d at 965 (warrant invalid and "authorization to seize 'gemstones and other items of jewelry' [from business] was far too broad" because affidavit only established probable cause pertaining to a few stolen diamonds).

Absent explicit restrictions on how and when it is used, an IMSI catcher would intercept all information from a target's phone about location and calls made, not merely location and calls pertaining to suspected criminal activity. If used to identify the numeric identifier of the phone(s) used by a suspect, it would also intercept the information from *all* phones used by the suspect, not only the phone used in connection with suspected criminal activity.[85] *See supra* Section VI-A (discussing why interception of this information gives rise to a search and seizure).

While the suppression analysis will focus largely on the information obtained from the defendant, it is also worth noting the impact on third parties. Courts are sensitive to overbreadth issues when the search extends to third parties as to whom there is no probable cause at all. In *Maryland v. Garrison*, the affidavit established probable cause to search the residence of one individual, who was identified as living on the third floor of a particular apartment building; the building, it turned out, had two units on the third floor and the question was whether the search of the second unit was lawful. 480 U.S. at 81. "Plainly," the Court emphasized, "if the officers had known, or even if they should have known, that there were two separate dwelling units on the third floor of [the building], they would have been obligated to exclude respondent's apartment from the scope of the requested warrant." *Id.* at 85. *Garrison* thus makes clear that officers are obligated to exclude from the scope of a requested warrant third parties as to whom they lack probable cause.[86]

Severability and suppression. The Ninth Circuit "follow[s] 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." *Spilotro,* 800 F.2d at 967. But "[i]f no portion of the warrant is sufficiently particularized to pass constitutional muster, then total suppression is required. Otherwise the abuses of a general search would not be prevented." *Cardwell,* 680 F.2d at 78 (citation omitted). When confronted with an insufficiently particularized or an overbroad warrant, a court must therefore first determine whether the defective portions of the warrant are severable.

Relevant to the analysis is whether improperly authorized "items were set forth in textually severable portions." *Spilotro,* 800 F.2d at 968. It is exceedingly unlikely that a warrant authorizing use of an IMSI catcher would use a formulation that distinguishes between signaling information from the suspect's device that pertains to suspected criminal activity and signaling information that does not, or distinguishes between signaling information from the target device and third-party devices. To the extent the warrant does not contain "identifiable portions [that are] sufficiently specific and particular to support severance," severance is not available. *Id.* at 967.

In addition, "severance is not available when the valid portion of the warrant is 'a relatively insignificant part' of an otherwise invalid search." *In re Grand Jury Subpoenas,* 926 F.2d at 858 (quoting *Spilotro,* 800 F.2d at 967); *accord Kow*, 58 F.3d at 428. To the extent the

government used an IMSI catcher to conduct a dragnet search for *all* signaling information from the target (even from phones and at times and locations unrelated to suspected criminal activity) and for all signaling information from *all* cell phones in the vicinity of the target (even from third parties as to whom the government lacks probable cause), the information from the target cell phone pertaining to criminal activity would be a "relatively insignificant part" of the warrant and severance would not be available.[87]

Where a warrant is not severable, the remedy is blanket suppression. *See Spilotro,* 800 F.2d at 968 (ordering blanket suppression where warrant not severable); *Cardwell*, 680 F.2d at 78 (same); *Kow,* 58 F.3d at 428, 430 (same).

Good faith exception inapplicable. Courts have typically rejected the argument that the "good faith" exception to the suppression doctrine, *see United States v. Leon,* 468 U.S. 897 (1984), applies where the warrant is facially invalid. *See United States v. Clark,* 31 F.3d 831, 836 (9th Cir. 1994) (where warrant was facially overbroad, "the officers could not reasonably rely on it under the objective test of *Leon*"); *Center Art Galleries-Hawaii,* 875 F.2d at 753 (declining to apply good faith exception where "the warrants contained no meaningful restriction on which documents could be seized"); *Kow,* 58 F.3d at 429 ("when a warrant is facially overbroad, absent *specific assurances* from an impartial judge or magistrate that the defective warrant is valid despite its overbreadth, a reasonable reliance argument fails"). Depending on its language, a warrant authorizing the use of an IMSI catcher is likely "so overbroad that absent some exceptional circumstance, no agent could reasonably rely on them." *Center Art Galleries-Hawaii,* 875 F.2d at 753.

VI. CONCLUSION

Federal, state, and local law enforcement agencies have been using IMSI catchers to engage in dragnet searches and seizures of information from cell phones without disclosing this use to the courts or criminal defendants. By shrouding this technology in secrecy, the government has succeeded in deploying a highly intrusive form of surveillance. In cases where the government may have used an IMSI catcher, vigorous advocacy is necessary to obtain full discovery and suppression of tainted evidence. Unless criminal defense attorneys pursue these issues aggressively, the government will continue to write its own rules for conducting surveillance, without the benefit of court oversight or an adversarial process.

APPENDIX

Issues to Pursue in Discovery

The following is a non-exhaustive list of issues to pursue in discovery broken into two main topics. One set of issues is intended to ferret out whether the government used an IMSI catcher, and the other presses on the constitutional implications of its use.

A. Was an IMSI catcher used?

1. All subpoenas, court orders, and warrants, as well as applications and affidavits in support thereof, for electronic surveillance, and returns thereto.
2. All information obtained via each such subpoena, court order, or warrant.
3. All documents identifying equipment used to [identify the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].
4. All emails, notes, logs, reports (including but not limited to Investigation Details Reports), and any other documents regarding efforts to [identify the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].[88]
5. All documents describing or reflecting categories of data (*e.g.*, incoming or outgoing telephone numbers; IP addresses; date, time and duration of call; cell site ID; cell site sector; location area code; signal strength; angle of arrival; signal time difference of arrival; ESN or MIN) obtained through real-time tracking of the location of the defendant's cell phone.[89]
6. All documents reflecting the cell site ID and location area code of the device used to monitor the defendant's cell phone.[90]
7. All documents reflecting the cell site IDs and location area codes collected by the device used to monitor the defendant's cell phone.[91]
8. All documents reflecting the GPS coordinates of any device while it was mobile and was used to monitor the defendant's cell phone.[92]
9. All information obtained through real-time tracking of the location of the defendant's cell phone.[93]
10. All reports of investigation, location calculations, and other relevant documents authored and/or signed by the individuals who participated in the investigation to [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].
11. All operator's logs, training records, score sheets, certification records, training standards, and training manuals related to the device used to [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].[94]

12. All reports of investigation, location calculations, and other relevant documents reflecting the agencies that participated in the investigation to [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].[95]
13. All test protocols and results of tests performed on the device used to [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone], prior to deploying the device on the defendant's cell phone. These test results shall include, but not be limited to, base station survey results of the immediate area where the defendant's cell phone was [identified] or [located].[96]
14. All experts' qualifications, summary of expected testimony, list of cases in which any such expert(s) has testified, and summary of the bases for any expert opinion related to testimony regarding the [identification of the unique numeric identifier associated with defendant's cell phone] or [identification of the geographic location of the defendant's cell phone].

B. If an IMSI catcher was used, the following issues are material to a potential motion to suppress.

1. Topics and document requests that would shed light on the intrusive nature of the IMSI catcher and why its use constituted a search:

    a. Where was the IMSI catcher used? Was it used to determine that the defendant was inside a private location such as a residence? Was there a trespass to property in connection with its use?
        (i) All documents reflecting capacity of IMSI catcher to locate cell phones while inside physical structures.
        (ii) All documents reflecting geographic accuracy with which the IMSI catcher is able to locate the target cell phone.
        (iii) All documents reflecting path movement of the IMSI catcher, including both the path the device traveled if used on the inside of a vehicle or mounted on an aerial vehicle, and the path the device traveled if carried by a human on foot.
    b. What kind of information did the IMSI catcher scoop up from the defendant (relevant to whether use constituted a search and also whether search was overbroad, *i.e.*, not limited to information pertaining to defendant's suspected criminal activity)?
        (i) All documents describing categories of data (*e.g.*, incoming or outgoing telephone numbers; date, time and duration of call; cell site number/sector or other information pertaining to geographic location of cell phone; signal strength; ESN

or MIN; ping time; content of communications) collected by the IMSI catcher from the defendant's cell phone.

(ii) All underlying data obtained by the IMSI catcher from the defendant's cell phone.

(iii) [If defendant has more than one cell phone and one or more has no connection to any criminal activity:] All documents reflecting the numeric identifiers obtained from defendant's cell phones.

c. How long was the IMSI catcher used and at what times of day (relevant to whether use constituted a search and also whether search was overbroad, *i.e.*, not limited to information pertaining to defendant's suspected criminal activity)?

(i) All documents reflecting times during which IMSI catcher was used.

2. Topics and document requests that would shed light on the intrusive nature of the IMSI catcher and why its use constituted a seizure.

a. Did the IMSI catcher interfere with the defendant's possessory interest in the cell phone?

(i) Did the government's use of the IMSI catcher deny the target phone service?

(a) All documents related to any agreements or arrangements with the wireless carrier authorizing the IMSI catcher to become part of its network or authorizing the IMSI catcher to monitor a phone that receives service through its network.

(b) All documents pertaining to any forwarding of data from defendant's phone to the wireless carrier's network while the IMSI catcher was in operation.[97]

(c) All documents reflecting impact of the use of the IMSI catcher on access by the defendant's cell phone to cellular service.

(ii) Try to document the fact that the IMSI catcher forces the phone to establish a connection with it and in the process forces the phone to transmit at full power, thus draining the battery faster.[98]

(a) All training materials, including but not limited to training records, certification records, training standards, and training manuals related to the device used to [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].[99]

(b) All user manuals related to the device used [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].

3. Topics and document requests that would shed light on the constitutionality of any warrant obtained:

   a. What kind of information did the IMSI catcher scoop up from the defendant? *See supra* B-1-b.
   b. What was the impact on third parties?[100]
      (i) All underlying data obtained by the IMSI catcher, whether or not pertaining to the defendant's cell phone.
      (ii) All documents reflecting the broadcast radius of the IMSI catcher.
      (iii) All documents reflecting the number of third-party cell phones with which the IMSI catcher exchanged information.
      (iv) All documents describing categories of data (*e.g.*, incoming or outgoing telephone numbers; date, time and duration of call; cell site number/sector or other information pertaining to geographic location of cell phone; signal strength; ESN or MIN; ping time) collected by the IMSI catcher from the third-party cell phones.
      (v) All underlying data obtained by the IMSI catcher from third-party cell phones, replacing any actual unique numeric identifiers with substitute numeric identifiers, to protect third-party privacy interests.
      (vi) All documents regarding subsequent use or destruction of third-party data obtained by the IMSI catcher.
      (vii) All documents reflecting impact of the use of the IMSI catcher on access by third-party cell phones to cellular service.
      (viii) All documents reflecting the data gathered by the IMSI catcher while it conducted base station surveys prior to being used to identify or locate the target cell phone.
   c. Other
      (i) All policies and procedures governing IMSI catcher use, including instructions about what court orders if any to seek, what information to present to courts in seeking court authorization, and standard operating procedures for using IMSI catchers to [identify a unique numeric identifier associated with a suspect's cell phone] or [identify the geographic location of a suspect's cell phone].[101]

The government's obligations under *Brady v. Maryland*, 373 U.S. 83 (1963), and Fed. R. Crim. P. 16 extend to information relevant to a Fourth Amendment motion to suppress. Rule 16 requires the government to disclose in discovery items that are "material to preparing the defense," Fed. R. Crim. P. 16(a)(1)(E), including items that are materials to a possible motion to suppress. *See, e.g., United States v. Thomas*, 726 F.3d 1086, 1096 (9th Cir. 2013) (reversing conviction where government failed to disclose records regarding training and experience of drug-detecting dog); *see also United States v. Budziak*, 697 F.3d 1105, 1111-12 (9th Cir. 2012) ("Materiality is a low threshold; it is satisfied so long as the information in the [document] would have helped [the defendant] prepare a defense."); *United States v. Feil*, 2010 WL 3834978 *1 (N.D. Cal. Sept. 29, 2010) (finding defendants "entitled to discovery on the limited issue of whether the investigation that led to this indictment is tainted by [an illegal] search").

Defendants should be entitled to disclosure of the full extent of the electronic surveillance used against them. Given the grave constitutional concerns raised by IMSI catchers, defendants should have a right to information showing whether the government relied on them; for if it did, defendants would have more than a reasonable probability of prevailing on a motion to suppress. *See Gamez-Orduno*, 235 F.3d at 461 ("[S]uppression 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.").

Note that the defendant in *Rigmaiden* sought in discovery highly "detailed technical information related to the devices and techniques used during the [location tracking] mission." 844 F. Supp. 2d at 998. The government opposed the discovery, invoking the qualified law enforcement privilege recognized in *Rovario v. United States*, 353 U.S. 53 (1957) (qualified privilege for identity of confidential informants). To avoid disclosure, the government made significant factual and legal concessions – that a StingRay was used and that the device was sufficiently intrusive to constitute a search within the meaning of the Fourth Amendment. *See* 844 F. Supp. 2d at 996. Based on these concessions, the defendant did not obtain all of the information he had sought in discovery. *See Rigmaiden*, 844 F. Supp. 2d at 999 ("Because each of Defendant's reasons for obtaining this information has been satisfied by the government's concessions, no additional disclosure will be required."). But the broad disclosure requests did result in the government making significant factual concessions that were crucial to the defendant's ability to formulate a motion to suppress.

ENDNOTES

[1] Harris, Wireless Products Group Price List, 4 (Sept. 2008), https://info.publicintelligence.net/Harris-SurveillancePriceList.pdf (StingRay line of products includes "Intercept Software Package" for GSM phones).
[2] *See* Ryan Gallagher, Meet the Machines That Steal Your Phone's Data, Ars Technica, (Sept. 25, 2013), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/ (describing various models of Harris Corporation's cell site simulators and related equipment); *see also* Harris, Wireless Products Group, StingRay & AmberJack Product Descriptions, http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf (last visited June 18, 2014); Harris, Wireless Products Group, KingFish (Preliminary) Product Description, 2, http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf (last visited June 18, 2014).
[3] *See* Electronic Privacy Information Center ("EPIC"), EPIC v. FBI – Stingray/Cell Site Simulator, http://epic.org/foia/fbi/stingray/. A 2008 PowerPoint on "Cell Site Simulators" includes a slide with the headline: "Increased Investigative Use of Technique" and a large arrow pointing upward (the remainder of the text on the slide is redacted). *See* Letter from FBI to EPIC Releasing Documents Pursuant to FOIA Request regarding Stingray/Cell Site Simulator Devices, 56 (Dec. 7, 2012), http://epic.org/foia/fbi/stingray/FBI-FOIA-Release-12072012-OCR.pdf [hereinafter "FBI FOIA Release to EPIC"] (including "Cellular Tracking and Other Legal Issues," June 2008 PowerPoint, Slide 28).
[4] *See* American Civil Liberties Union ("ACLU"), Stingray Tracking Devices: Who's Got them?, https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them (last visited June 18, 2014).
[5] For a compilation of known uses of this device by local law enforcement, *see* ACLU, https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them (last visited June 18, 2014). *See also, e.g.*, John Kelly, *Cellphone data spying: It's not just the NSA*, USA TODAY, Dec. 8, 2013, http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/ (records from more than 125 police agencies in 33 states revealed that at least 25 departments own a StingRay); Michael Bott & Thom Jensen, *9 Calif. law enforcement agencies connected to cellphone spying technology*, SACRAMENTO NEWS 10, Mar. 6, 2014, http://www.news10.net/story/news/investigations/watchdog/2014/03/06/5-california-law-enforcement-agencies-connected-to-stingrays/6147381/.
[6] *See generally* Hearing on Electronic Communications Privacy Act ("ECPA") Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong., 4 (2010) [hereinafter *"Blaze Congressional Testimony"*] *available at* http://www.crypto.com/papers/blaze-judiciary-20100624.pdf (statement of Professor Matt Blaze).
[7] Letter from US Department of Justice ("DOJ") to ACLU of Northern California attaching USA Book, Electronic Surveillance Manual Chapter XIV, 2 (Aug. 22, 2013), *available at* https://www.aclunc.org/sr03 [hereinafter USA Book, Electronic Surveillance Manual Chapter XIV] (obtained by the ACLU of Northern California in FOIA litigation).
[8] *See* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. OF L. & TECH. 134, 145-46

(2013-14) [hereinafter Pell & Soghoian]; Daehyun Strobel, *IMSI Catcher*, Ruhr-Universität, Bochum, Germany, 13 (July 13, 2007) *available at* http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf [hereinafter Strobel] ("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."). IMSI catchers vary in their operation, depending on among other things, whether the target phone is on a "GSM" (*e.g.*, AT&T) or "CDMA" (*e.g.*, Verizon) network. This paper focuses on the type of StingRays currently in use.

[9] DOJ Electronic Surveillance Unit, Electronic Surveillance Manual, 44 (June 2005) [hereinafter Electronic Surveillance Manual], http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

[10] Jennifer Valentino-DeVries, *Judge Questions Tools That Grab Cellphone Data on Innocent People*, WALL ST. J., Oct. 22, 2012, http://blogs.wsj.com/digits/2012/10/22/judge-questions-tools-that-grab-cellphone-data-on-innocent-people/. *See also* Transcript of Hearing on Motion to Suppress at 16, 23, *Florida v. Thomas*, Fla. Cir. Leon Cnty. Ct. (2010) (No. 2008-CF-3350A), https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf [hereinafter "*Florida v. Thomas*, Hearing on Motion to Suppress"].

[11] Pell & Soghoian, *supra* note 8, at 147 & n.43 ("Investigators can position a StingRay in the vicinity of the target to capture the unique serial number of the target's phone."); *see also* Executive Office for United States Attorneys, *Electronic Investigative Techniques*, 45 U.S. ATTORNEYS' BULLETIN 5, Sept. 1997 [hereinafter Electronic Investigative Techniques], http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf at 13; *In re Application for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012) (addressing request to use an IMSI catcher to identify telephone number of subject of investigation; application for court order stated that device would "detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones (*e.g.*, by transmitting the telephone's serial number and phone number) to the network for authentication" and that "[b]y determining the identifying registration data at various locations in which the [Subject's] Telephone is reasonably believed to be operating, the telephone number corresponding to the [Subject's] Telephone can be identified"); Criminal Complaint, *United States v. Arguijo*, No. Under Seal (D. Ill. Feb. 13, 2012), Affidavit in support of Criminal Complaint at 8 ¶10 n.1, http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222_01d.pdf ("On or about July 27, 2012, pursuant to the Court's Order, law enforcement officers familiar with Chaparro's appearance, having previously viewed photographs of him and observed him during prior surveillance, used a digital analyzer device on three occasions in three different locations where Chaparro was observed to determine the IMSI associated with any cellular telephone being carried by Chaparro. Using the digital analyzer device, in conjunction with surveillance of Chaparro, law enforcement determined that the telephone number bearing IMSI 316010151032079 was in the same vicinity in the three separate locations where Chaparro was observed.").

[12] IMSI is "a unique number burned into a removable security identify module (SIM) card that identifies a cell phone subscriber used in GSM and UMTS networks." Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, 59 U.S. ATTORNEYS' BULLETIN 6, Nov. 2011 [hereinafter O'Malley], http://www.justice.gov//usao/eousa/foia_reading_room/usab5906.pdf at 16, 20.

[13] The ESN, used in a CDMA network, consists of a unique 32-bit number assigned to the phone by the manufacturer. It is stored within the phone's permanent memory, rather than on a removable SIM card, and typically cannot be changed by the phone's user. *See* Telecommunications Industry Association, Electronic Serial Number Manufacturer's Code Assignment Guidelines and Procedures Ver. 2.0, 6-7, 12 (Aug. 2008), http://ftp.tiaonline.org/wcd/WCD%20Meeting%20Sept.%204%202008/WCD-20080904-002_ESN_Guidelines_v2.0.pdf. The ESN is used by a carrier to connect the phone to a subscriber account. *See* MobileBurn, What is "ESN?", http://www.mobileburn.com/definition.jsp?term=ESN (last visited June 18, 2014); Andy Hellmuth, What is an ESN, and Why Should I Care?, (Sept. 16, 2011) http://www.buymytronics.com/blog/post/2011/09/16/What-Is-An-ESN-And-Why-Should-I-Care.aspx.

[14] The MIN is a "34-bit number that is a digital representation of the 10-digit [telephone] number assigned to a [cell phone]." 3rd Generation Partnership Project 2 "3GPP2", Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, § 1.2.1, 1.2 (Dec. 1999), http://www.3gpp2.org/public_html/specs/c.s0016-0with3gcover.pdf. The MIN is "a unique provider-assigned number for each cell phone in the cellular provider's network." O'Malley at 20.

[15] *See* DOJ, Office of Enforcement Operations Criminal Division, Electronic Surveillance Issues, 153 (Nov. 2005) [hereinafter Electronic Surveillance Issues], http://www.justice.gov/criminal/foia/docs/elec-srvlnce-issuse.pdf; Letter from Harris Corporation to Raul Perez, City of Miami PD, Law Enforcement Trust Fund Sole Source Vendor Letter, 6 (Aug. 25, 2008), http://egov.ci.miami.fl.us/Legistarweb/ Attachments/48003.pdf (Harris Corporation "AmberJack" operates with other Harris products, "enabling tracking and location of targeted mobile phones").

[16] *See Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 14; USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1.

[17] Electronic Surveillance Manual, *supra* note 9, at 41 ("In order to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular cell phone, the portion of that tower facing the phone, and often the signal strength of the phone. Depending on the number of towers in a particular area and other factors, this information may be used to identify the location of a phone to within a few hundred yards . . . Carriers generally keep detailed historical records of this information for billing and other business purposes.").

[18] *See* Pell & Soghoian, *supra* note 8, at 146-47 ("[U]nlike carrier-assisted surveillance, in which the third-party provider necessarily has knowledge of surveillance performed and copies of records disclosed at the request of law enforcement, the unmediated nature of the StingRay dictates that only the operator of the device has: (1) knowledge that an interception ever took place; and (2) . . . access to the information intercepted. Thus, to the extent that telephone companies are able to act as a proxy for their customers' privacy interests and may 'push back' against overbroad or otherwise improper government surveillance, no such advocate exists for the target when a StingRay is used.") (footnotes omitted).

[19] *See, e.g.*, PKI Electronic Intelligence, GSM Cellular Monitoring Systems (product brochure), 12, http://www.docstoc.com/docs/99662489/GSM-CELLULAR-MONITORING-SYSTEMS---PKI-Electronic-# (last visited June 23, 2014) (device can "locat[e] . . . a target mobile phone with

an accuracy of 2 m[eters]"); Bahia 21 Corporation, Resp. to National Telecommunications Information Administration Notice of Inquiry (Doc. #100504212-0212-01) Requesting Information on Preventing Contraband Cell Phone Use in Prisons, 3 (June 11, 2010), 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).

[20] *See United States v. Rigmaiden*, 844 F. Supp. 2d 982, 996 (D. Ariz. 2012).

[21] *Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 15.

[22] *See Blaze Congressional Testimony*, *supra* note 6, at 12 (cell site location information "[i]n legacy systems or in rural areas . . . [may] specify only a radius of several miles, while in a dense urban environment with microcells, it could identify a floor or even a room within a building. How precise sector identity is depends on the particular location of the target and on the layout of the particular carrier's network.").

[23] *See* Pell & Soghoian, *supra* note 8, at 146 & n.36; Electronic Surveillance Manual at 41; Harris, Wireless Products Group Price List, *supra* note 1, at 8 (StingRay line of products includes "Intercept Software Package" for GSM phones); *Active GSM Interceptor*, Ability http://www.interceptors.com/intercept-solutions/Active-GSM-Interceptor.html (last visited June 18, 2014) (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); *see also* Juliam Dammann, Presentation at the University of Bonn Seminar on Mobile Security: IMSI-Catcher and Man-in-the-Middle Attacks, 5 (Feb. 9, 2011), http://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/10ws/10ws-sem-mobsec/talks/dammann.pdf [hereinafter Dammann] ("is able to eavesdrop").

[24] *See* Electronic Surveillance Manual, *supra* note 9, at 41. A wiretap order under Title III requires, among other things, the government to show probable cause to believe that an individual is committing a statutorily enumerated offense, probable cause to believe that "particular communications concerning that offense will be obtained through such interception," and "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(3).

[25] *See, e.g.*, Pell & Soghoian, *supra* note 8, at 145-46; HANNES FEDERRATH, PROTECTION IN MOBILE COMMUNICATIONS 5 (Günter Müller et al. eds., Multilateral Security in Communications) (1999), *available at* http://epub.uni-regensburg.de/7382/1/Fede3_99Buch3Mobil.pdf; Strobel, *supra* note 8, at 13 ("possible to determine the IMSIs of all users of a radio cell"). This paper focuses on "active IMSI catchers," which are the type of IMSI catcher currently and predominantly used by law enforcement. Early models of IMSI catchers were "passive" and merely read transmissions, but did not simulate base stations and force devices to connect with them.

[26] Electronic Surveillance Manual, *supra* note 9, at 182.

[27] Dammann, *supra* note 23, at 19.

[28] Electronic Surveillance Manual, *supra* note 9, at 182 n.48.

[29] The devices send signals like those emitted by a carrier's own base stations. *See, e.g.*, Harris, Wireless Products Group, StingRay & AmberJack Product Descriptions, 1

http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf (last visited June 19, 2014) ("Active interrogation capability emulates base stations"). Those signals, of course, "penetrate walls" (necessarily, to provide connectivity indoors). AT&T, *What You Need to Know About Your Network,* http://www.att.com/gen/press-room?pid=14003 (last visited June 19, 2014); *see also* E.H. Walker, *Penetration of Radio Signals Into Buildings in the Cellular Radio Environment,* 62 THE BELL SYSTEMS TECHNICAL J. 2719 (1983) *available at* http://www.alcatel-lucent.com/bstj/vol62-1983/articles/bstj62-9-2719.pdf.

[30] Strobel, *supra* note 8, at 13.

[31] *See* USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1 ("A cell site simulator, digital analyzer, or a triggerfish can electronically *force a cellular telephone to register* its mobile identification number ("MIN," *i.e.,* telephone number) and electronic serial number ("ESN," *i.e.,*, the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on") (emphasis added).

[32] *Florida v. Thomas,* Hearing on Motion to Suppress, *supra* note 10, at 15; *see also id.* at 12 ("[W]e emulate a cellphone tower. [S]o just as the phone was registered with the real verizon tower, we emulate a tower; we *force* that handset to register with us.") (emphasis added).

[33] USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1.

[34] *See* Electronic Investigative Techniques, *supra* note 11, at 13-15, 23; Electronic Surveillance Manual, *supra* note 9, at 41; USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1; *see generally* Electronic Surveillance Issues, *supra* note 15.

[35] The ACLU of Northern California has filed two FOIA lawsuits to obtain DOJ's polices, practices, and procedures regarding location tracking in general and StingRays in particular. DOJ has resisted producing the materials and the litigation is on-going. *See ACLU of Northern California et al. v. Dep't of Justice,* No. 12-cv-4008-MEJ (N.D. Cal. filed July 31, 2012) and *ACLU of Northern California v. Dep't of Justice,* No. 13-cv-3127-MEJ (N.D. Cal. filed July 8, 2013); *see also* Linda Lye, Fighting for Transparency, ACLU of Northern California Blog (July 31, 2012), https://www.aclunc.org/blog/fighting-transparency and Linda Lye, ACLU Sues Government for Information About "Stingray" Cell Phone Tracking, ACLU of Northern California Blog (July 8, 2013), https://www.aclunc.org/blog/aclu-sues-government-information-about-stingray-cell-phone-tracking.

[36] Reporter Beau Hodai, represented by the ACLU of Arizona, has sued the city of Tucson and the Tucson Police Department for failing to disclose IMSI catcher documents in response to a public records request. *See Hodai v. City of Tucson,* No. C20141225 (Ariz. Super. Ct. filed Mar. 4, 2014). An affidavit by Lieutenant Kevin Hall of the Tucson Police Department attached to the defendants' verified answer, filed on April 14, 2014, states: "I am not aware of a use of this equipment by the Tucson Police Department wherein a warrant was obtained by the Tucson Police Department" and "In each of the five cases where I personally know that the technology was used, there is no written record of that use in the respective case reports and other documents, and no public record that I can find documenting the use of the technology in those cases." Hall Aff. at ¶¶10, 14, *available at* http://bloximages.chicago2.vip.townnews.com/azstarnet.com/content/tncms/assets/v3/editorial/6/7f/67fb460f-c2f6-51b9-8639-a36371622133/537d2509b468c.pdf.pdf. And in Sacramento, "[d]espite evidence showing the sheriff's department is utilizing the device, the Sacramento County District Attorney's Office and Sacramento Superior Court judges said they have no knowledge of StingRays or similar tools being used in Sacramento." Thom Jensen & Michael

Bott, *Is sheriff's department using tracking and data-collecting device without search warrants?*, SACRAMENTO NEWS 10, June 23, 2014, http://www.news10.net/story/news/investigations/2014/06/23/is-sacramento-county-sheriff-dept-using-stingray-to-track-collect-data/11296461/.

[37] *See Smith v. Maryland*, 442 U.S. 735, 736 & n.1 (1979); *United States v. Garcia-Villalba*, 585 F.3d 1223, 1226 (9th Cir. 2009).

[38] 18 U.S.C. § 3127(3) & 3127(4), amended by Patriot Act, Pub. L. No. 107-56, Title II, § 216(c)(2)(A) & (3)(A), 215 Stat. 290 (2001).

[39] *See* Electronic Surveillance Manual, *supra* note 9, at 41, 47-48.

[40] *See id.* at 182 n.48.

[41] *See* FBI FOIA Release to EPIC, *supra* note 3, at 32-33, 36-37 (Slides 1-2, 5-6).

[42] *See* USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1 ("a pen register/trap and trace order *must be obtained* by the government before it can use its own device to capture the ESN or MIN of a cellular telephone, even though there will be no involvement by the service provider") (emphasis added).

[43] 47 U.S.C. § 1002(a)(2); H.R. Rep. 103-827(I) (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3489-90.

[44] 47 U.S.C. § 1002(a)(2)(B).

[45] Electronic Surveillance Manual, *supra* note 9, at 47.

[46] *See id.* at 42-44; *see also* RICHARD M. THOMPSON, CONG. RESEARCH SERV., R42109, GOVERNMENTAL TRACKING OF CELL PHONES AND VEHICLES: THE CONFLUENCE OF PRIVACY, TECHNOLOGY, AND LAW, 12 (2011) [hereinafter Thompson], *available at* https://www.fas.org/sgp/crs/intel/R42109.pdf.

[47] *See* 47 U.S.C. § 1002(a)(2)(B).

[48] 18 U.S.C. § 2703(d).

[49] *See In re Application for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 310 n.6 (3d Cir. 2010) (citing cases); *Espudo*, 954 F. Supp. 2d at 1038-39 ("A significant majority of courts have rejected the hybrid theory and has found that real-time cell site location data is not obtainable on a showing of less than probable cause. A minority of courts, on the other hand, have found that it is.") (citations omitted); Thompson, *supra* note 46, at 13-14 (citing cases).

[50] *See* Electronic Surveillance Manual, *supra* note 9, at 175-87 ("Combined 3123/2703 Application").

[51] One of the requests built into the template is authorization to permit installation and use of the "pen register and trap and trace device not only on the Subject Telephone Number[s], but also . . . *on any cellular phone that is within close proximity to the government device that may autonomously register with the device* . . . . " *See id.* at 181-82 (emphasis added). A pen register or trap and trace device would not cause cellular phones within a target phone's vicinity to register autonomously; an IMSI catcher would. The footnote to this template request goes on to describe the device as one that is "used to receive radio signals, emitted from a wireless cellular telephone, that merely identify that telephone to the network (*i.e.*, registration data)." *See id.* at n.48. This, too, appears to describe the operation of an IMSI catcher. Notably, the footnote also takes the position that the device does *not* constitute a pen register or trap and trace device (and that the application is nonetheless submitted "out of an abundance of caution"), and cites one of the few known cases expressly addressing use of an IMSI catcher. *See id.* (citing *In the Matter*

of the Application of the U.S. for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197, 201 (C.D. Cal. 1995). *See infra* Section IV discussing this and other cases on IMSI catchers.

[52] Affidavit in Support of N.D. Cal. Order 08-90330 ¶42, at 34, *United States v. Rigmaiden*, No. 08-cr-00814-DGC (D. Ariz. Jan. 4, 2012), ECF No. 920-1 (Lye Decl., Exh. 2), *available at* https://www.aclunc.org/sr04. Sample IMSI catcher orders introduced by the government in the same case similarly provided no information about the unique and intrusive ways in which an IMSI catcher functions. *See, e.g.*, Supplemental Memorandum to Government's Response to Defendant's Motion to Suppress, Exhibit 1 ¶¶3-4, at 2, *United States v. Rigmaiden*, No. 08-cr-00814-DGC (D. Ariz. Jan. 4, 2012) [hereinafter "Sample IMSI Catcher Order"], ECF No. 986-1 (Sample IMSI Catcher Order Application from a Warrant for a Tracking Device in District of Arizona proceeding, case number redacted), *available at* https://www.aclunc.org/sr05, ("Applicant requests . . . authorization to install, operate, and monitor the mobile tracking device. . . . The United States seeks the cellular telephone location information on an ongoing and real-time basis, including but not limited to identifying the specific nearest cell sites activated or accessed by the target[']s cellular telephone, and identifying the signal direction and strength of communications between the activated cell site(s) and the targets[']s cellular telephone. The United States does not seek the content of any wire or electronic communications. Used in this manner, the cellular telephone location information will generate data to track the general location of the user of the target cellular telephone."). There is no reference in these *filed* applications and orders to the fact that "any cellular phone that is within close proximity to the government device . . . may autonomously register with the device." Electronic Surveillance Manual, *supra* note 9, at 182 (sample application for hybrid order to use IMSI catcher).

[53] *See* Sample IMSI Catcher Order, *supra* note 52.

[54] U.S. CONST. amend IV.

[55] *See* 18 U.S.C. §§ 3127(3), (4) (defining pen register and trap and trace devices to include not only incoming and outgoing numbers but also "signaling information").

[56] *See supra* Section III-C (discussing hybrid orders).

[57] *See* Brief Amici Curiae in Support of Daniel Rigmaiden's Motion to Suppress at 7, *United States v. Rigmaiden*, No. 08-cr-00814-DGC (D. Ariz. Jan 4, 2012), ECF No. 904-3, *available at* https://www.aclu.org/files/assets/rigmaiden_amicus.pdf.

[58] *See, e.g.*, Jennifer Valentino-Devries, *Judges Questioned Use of Cellphone Tracking Devices*, WALL ST. J., Mar. 27, 2013, http://blogs.wsj.com/digits/2013/03/27/judges-question-use-of-cellphone-tracking-devices/; Ellen Nakashima, *Little-known surveillance tool raises concerns by judges, privacy activists*, WASH. POST, Mar. 27, 2013, http://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html; Linda Lye, DOJ Emails Show Feds Were Less Than 'Explicit' With Judges On Cell Phone Tracking Tool, ACLU of Northern California Blog (Mar. 27, 2013), https://www.aclu.org/blog/national-security-technology-and-liberty/doj-emails-show-feds-were-less-explicit-judges-cell.

[59] *See Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 12 ("[W]e emulate a cellphone tower. So just as the phone was registered with the real Verizon tower, we emulate a tower; we force that handset to register with us. We identify that we have the correct handset

and then we're able to, by just merely direction finding on the signal emanating from that handset – we're able to determine a location.").

[60] The brief filed by the defendant in the intermediate appellate court stated that "The ESN and initial location data obtained from the cell phone company, together with the Stingray antenna mounted on the police vehicle, led officers to the corner of a private apartment building where the defendant's cellular phone was located." Brief of Defendant-Appellant at 8, *Wisconsin v. Tate*, No. 2012AP336 (Wis. Ct. App. June 5, 2011), *available at* https://www.aclunc.org/sr02. The case was argued in the state Supreme Court on October 3, 2013, but as of the date of this publication, no opinion had yet issued. *See* Wisconsin Court System, State v. Bobby L. Tate Case History, http://wscca.wicourts.gov/appealHistory.xsl;jsessionid=1FC6F48B94D421C1C2ED4BA85548AB98?caseNo=2012AP000336&cacheId=B14C504915CF7D52C2700564DA05E6C8&recordCount=1&offset=0&linkOnlyToForm=false&sortDirection=DESC (last visited June 27, 2014).

[61] *See* City's Verified Answer, *Hodai v. City of Tucson*, No. C20141225 (Ariz. Super. Ct. filed Mar. 4, 2014) (aff. of Bradley S. Morrison at 2), *available at* http://bloximages.chicago2.vip.townnews.com/azstarnet.com/content/tncms/assets/v3/editorial/6/7f/67fb460f-c2f6-51b9-8639-a36371622133/537d2509b468c.pdf.pdf.

[62] *See supra* Section III.

[63] According to emails obtained by the ACLU of Florida through a public records request, police officers with the Sarasota Police Department in Florida "[i]n reports or depositions" "simply refer [to information from an IMSI catcher] as '… information from a confidential source regarding the location of the suspect." They have done so "at the request of the U.S. Marshalls." *See* Email from Kenneth Castro, Sergeant, Sarasota Police Department, to Terry Lewis, (Apr. 15, 2009, 11:25 EST) [hereinafter "Email from Kenneth Castro"], *available at* https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf.

[64] DOJ's Electronic Surveillance Manual contains a template "Application for Order Permitting Government To Use Its Own Pen Register/Trap and Trace Equipment (Triggerfish/Digital Analyzer or Similar Device)," which states that the application seeks "an order authorizing the installation and use of a pen register to identify the Electronic Serial Number (ESN) and Mobile Identification Number (MIN) of a cellular telephone (being used by_ (if known)_) (within a (color, make, model of vehicle) (bearing _ state license plate number_))." Note that although the internal DOJ title for the template refers to the "Triggerfish/Digital Analyzer or Similar Device," the actual text of the template application nowhere references any device other than a pen register/trap and trace. *See* Electronic Surveillance Manual, *supra* note 9, at 171-72.

[65] Particularly in the context of a drug case where a defendant used so-called "burner" phones, frequently replacing one phone with another, the government may have obtained the new telephone number through the "Hemisphere Project," in which the "government pays AT&T to place its employees in drug-fighting units around the country. Those employees sit alongside Drug Enforcement Administration agents and local detectives and supply them with the phone data from as far back as 1987." Scott Shane & Colin Moynihan, Drug Agents Use Vast Phone Trove Eclipsing N.S.A.'s, N.Y. TIMES, Sept. 1, 2013 at A1, *available at* http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html. By matching calling patterns, the Hemisphere Project is able to identify replacement phone numbers as targets of an investigation discard old ones. Do not expect to find any reference to the Hemisphere Project, as law enforcement agents are trained "to never refer to Hemisphere in

any official document" and to "keep the program under the radar." Office of Nat'l Drug Control Policy, *Los Angeles Hemisphere*, Slides 8, 12, *available at Synopsis of the Hemisphere Project*, N.Y. TIMES, Sept. 1, 2013, http://www.nytimes.com/interactive/2013/09/02/us/hemisphere-project.html.

[66] First Submission of Consolidated Exhibits Relating to Discovery and Suppression Issues, Exhibit 34 at 51, *United States v. Rigmaiden*, No. 08-cr-00814-DGC (D. Ariz. Jan 4, 2012), ECF No. 587-2, (Email from Denise L Medrano, Special Agent, Phoenix Field Office, to Albert A. Childress (July 17, 2008 6:01 AM)) (emphasis added), *available at* https://www.aclunc.org/sr06; *see also id.* Exhibit 38 at 12, ECF No. 587-3, (Email from Fred Battista, Assistant United States Attorney, to Shawna Yen (July 17, 2008 3:56 PM): "The main effort now may be to tie the target to the case without emphasis on the [redacted]."), *available at* https://www.aclunc.org/sr07.

[67] *See, e.g., Thomas v. State*, 127 So. 3d 658, 659-60 (Fla. Ct. App. 2013) (technology used to track suspect to his apartment in a large apartment complex); *United States v. Rigmaiden*, 2013 WL 1932800 *3 (D. Ariz. 2013) (technology used to track suspect to "unit 1122 of the Domicilio apartment complex in Santa Clara").

[68] *See* USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1; *Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 12 ("So just as the phone was registered with the real Verizon tower, we emulate a tower; we *force* that handset to register with us."); *id.* at 17 ("once the equipment comes into play and we *capture* that handset, to make locating it easier, the equipment *forces* that handset to transmit at full power") (emphases added).

[69] *See Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 15 ("[U]sing portable equipment we were able to actually basically stand at every door and every window in that [apartment] complex and determine, with relative certainty you know, the particular area of the apartment that that handset was emanating from").

[70] *See id.* at 12, 15.

[71] *See* USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1.

[72] We are not currently aware of IMSI catchers being used over prolonged periods, but this is an issue that should be pursued in discovery.

[73] Five justices of the Supreme Court agree 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 Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring); *accord id.* at 964 (Alito, J., concurring). *See also Commonwealth of Massachusetts v. Augustine*, 467 Mass. 230, 254 (2014) (government's collection of two weeks' worth of cell site location information from cellular provider invaded reasonable expectations of privacy); *State of New Jersey v. Earls*, 214 N.J. 564, 588 (2013) (holding that New Jersey Constitution "protects an individual's privacy interest in the location of his or her cell phone"); *People of the State of New York v. Weaver*, 12 N.Y.3d 433, 444-45 (2009) (installation and monitoring of GPS device on vehicle to monitor suspect's movements over 65-day period constitute search requiring a warrant under New York Constitution); *State of Washington v. Jackson*, 150 Wash. 2d 251, 262, 264 (2003) (installation and use of GPS on vehicle constitutes search and seizure under Washington Constitution because "24-hour a day surveillance possible through use of" device "intru[des] into private affairs"); *State of Oregon v. Campbell*, 306 Or. 157, 172 (1988) ("use of radio transmitter to locate defendant's automobile" constituted search under Oregon Constitution; "[a]ny device that enables the police quickly to locate a person or object anywhere within a 40-mile radius, day

or night, over a period of several days, is a significant limitation on freedom from scrutiny"); *State of South Dakota v. Zahn,* 812 N.W.2d 490, 497-98 (2012) (installation and monitoring of GPS device on suspect's vehicle over 26-day period invaded reasonable expectations of privacy and constituted search within meaning of Fourth Amendment).

[74] In *Rigmaiden,* the government ultimately acknowledged it used an IMSI catcher, but its affidavit in support of the warrant nowhere referred to the device. The affidavit instead made fleeting references to an unspecified "mobile tracking device" and the only description of how the device works stated "[t]he mobile tracking equipment ultimately generate[s] a signal that fixes the geographic position of the Target [Device]." Affidavit in Support of N.D. Cal. Order 08-90330 ¶42, at 34, *United States v. Rigmaiden,* No. 08-cr-00814-DGC (D. Ariz. Jan. 4, 2012), ECF No. 920-1 (Lye Decl., Exh. 2), *available at* https://www.aclunc.org/sr04. Similarly, in *In re StingRay,* the government's application requested authorization to install and use "a pen register and trap and trace device"; apparently it was only after the court conducted an *ex parte* hearing with the special agent leading the investigation that the agent "indicated that this equipment designed to capture these cell phone numbers was known as a 'stingray.'" 890 F. Supp. 2d at 748. The application did "not explain the technology, or the process by which the technology will be used to engage in the electronic surveillance to gather the Subject's cell phone number." *Id.* at 749.

[75] Depending on the language of the warrant, a separate argument turning on *scope* may also be available. *See United States v. Hurd,* 499 F.3d 963, 964 (9th Cir. 2007) (in evaluating whether search falls outside the scope of a warrant, court looks to "the circumstances surrounding the issuance of the warrant, the contents of the warrant, and the circumstances of the search") (internal quotation marks, citation omitted). If the contents of the warrant nowhere reference an IMSI catcher, it may be possible to argue that the government's use of the IMSI catcher fell outside the warrant's *scope* and was thus warrantless.

[76] *Bravo* and *Liston* are civil cases, but claims by a criminal defendant about materially misleading statements in an affidavit and civil claims of "judicial deception" are governed by the same legal standard. *See Liston,* 120 F.3d at 972.

[77] In *Rigmaiden,* the government deleted third-party information immediately after it used the IMSI catcher to locate the defendant. *See* 2013 WL 1932800 at *20. Immediate deletion of this information may mitigate some of the harm to third-party privacy interests, but it also deprives the defendant of concrete evidence regarding the impact of IMSI catchers on third parties as to which the government lacked probable cause, and the extent to which information about the defendant was or was not a "relatively insignificant part of" the government's overall dragnet. *Spilotro,* 800 F.2d at 967. These issues bear directly on the warrant's overbreadth and whether blanket suppression is the appropriate remedy. A magistrate alerted to the existence of the third party issue may choose to develop 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).

[78] In *Rigmaiden,* the court denied the motion to suppress, opining that the application's failure to "disclose that the mobile tracking device would capture from other cell phones," was a mere "detail of execution which need not be specified under" *Dalia v. United States,* 441 U.S. 238, 258 (1979). *Rigmaiden,* 2013 WL 1932800 at *20. The court distinguished *Rettig* on the ground that in the case before it, the "agents . . . did not seek to capture third-party cell phone and aircard information so they could use it in a criminal investigation, nor is there any evidence that they

used the third-party information in that manner." *Id.* But the Ninth Circuit in *Rettig* explicitly faulted the government for failing to disclose not only the purpose of the search but also its intended scope. *See* 589 F.2d at 422 ("By failing to advise the judge of all the material facts, including the purpose of the search *and its intended scope*, the officers deprived him of the opportunity to exercise meaningful supervision over their conduct and to define the proper limits of the warrant.") (emphasis added). Moreover, it is difficult to reconcile core Fourth Amendment prohibitions on searches lacking in probable cause with the *Rigmaiden*'s court's characterization of this issue as a mere "detail of execution."

[79] In *Rigmaiden,* the court found that the *Leon* good faith doctrine applied because the "'agents were using a relatively new technology, and they faced a lack of legal precedent regarding the proper form of a warrant to obtain the location information they sought.'" 2013 WL 1932800 at *31. "There is no precedent," the court stated, "suggesting that the agent was required to include in his warrant application technical details about the operation of the mobile tracking device." *Id.* at *32. But it is precisely the lack of legal precedent about IMSI catcher technology and its intrusive effect on third parties that imposes a duty on the officers to seek guidance from the judicial officer. *See Ctr. Art Galleries-Haw.,* 875 F.2d at 753 ("When the officer seeking a warrant is aware of an overbreadth problem, . . . we can reasonably expect the officer to bring the problem to an impartial magistrate's or judge's attention and to seek specific assurances that the possible defects will not invalidate the warrant."); *see also CDT,* 621 F.3d at 1178 (Kozinski, C.J., concurring) (discussing "the government's duty of candor in presenting a warrant application").

[80] *See* City's Verified Answer, *Hodai v. City of Tucson*, No. C20141225 (Ariz. Super. Ct. filed Mar. 4, 2014) (aff. of Bradley S. Morrison at 2), *available at* http://bloximages.chicago2.vip.townnews.com/azstarnet.com/content/tncms/assets/v3/editorial/6/7f/67fb460f-c2f6-51b9-8639-a36371622133/537d2509b468c.pdf.pdf. ("[T]he FBI has, as a matter of policy, for over 10 years, protected this specific electronic surveillance equipment and techniques from disclosure, directing its agents that while the product of the identification or location operation can be disclosed, neither details on the equipment's operation nor the tradecraft involved in use of the equipment may be disclosed.").

[81] The May 23, 2011 email chain was obtained by the ACLU of Northern California through a FOIA request and is available at https://www.aclu.org/technology-and-liberty/us-v-rigmaiden-doj-emails-stingray-applications; *see also* Linda Lye, DOJ Emails Show Feds Were Less Than 'Explicit' With Judges On Cell Phone Tracking Tool, ACLU of Northern California Blog (Mar. 27, 2013), https://www.aclu.org/blog/national-security-technology-and-liberty/doj-emails-show-feds-were-less-explicit-judges-cell.

[82] First Submission of Consolidated Exhibits Relating to Discovery and Suppression Issues, Exhibit 34 at 51, *United States v. Rigmaiden,* No. 08-cr-00814-DGC (D. Ariz. Jan 4, 2012), ECF No. 587-2, (Email from Denise L Medrano, Special Agent, Phoenix Field Office, to Albert A. Childress (July 17, 2008 6:01 AM)) (emphasis added), *available at* https://www.aclunc.org/sr06.

[83] Email from Kenneth Castro, *supra* note 63.

[84] *Id.*

[85] As DOJ explains, an IMSI catcher intercepts "necessary signaling data" consisting of a target device's unique numeric identifier and location whenever the phone is on, and even if it is not being used; when the phone makes or receives a call, an IMSI catcher captures not only the device's unique numeric identifier and location, but also "the call's incoming or outgoing status,

the telephone number dialed, [and] the date, time, and duration of the call." USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1.

[86] *See also Bravo,* 665 F.3d at 1084-85 (reversing grant of summary judgment for government defendants in civil challenge to lawfulness of search warrant where officer obtained warrant to search home where suspect had previously resided but officer had no evidence that current residents were involved in crime); *Liston,* 120 F.3d at 973-74 (officer not entitled to qualified immunity where he obtained warrant to search home and "for sale" and "sold" signs in front yard indicated third parties other than suspect occupied home).

[87]While the government is likely to argue that criminal defendants do not have standing to raise third party issues, the argument could be made that information about the IMSI catcher's the impact on third parties bears on questions of overbreadth and severability.

[88] In *Rigmaiden*, references to "StingRays" appeared in documents pertaining to the investigation. *See* Response to Government's Memorandum Regarding Law Enforcement Privilege, Exhibit 39 at 62, *United States v. Rigmaiden,* No. 08-cr-00814-DGC (D. Ariz. Jan 4, 2012), ECF No. 536-4 (rough notes prepared by IRS-CI Agent Denise L. Medrano) (handwritten checklist: "utility search[,]…tax return search[,] Post office – verifying forwarding info[,] Run plates[,] Review Video[,] Accurint[,] StingRay"), *available at* https://www.aclunc.org/sr08; First Submission of Consolidated Exhibits Relating to Discovery and Suppression Issues, Exhibit 26 at 32, *United States v. Rigmaiden,* No. 08-cr-00814-DGC (D. Ariz. Jan 4, 2012), ECF No. 587-2 (United States Postal Inspection Service Investigation Details Report) ("During the course of this investigation and conferring with TSD agents with the FBI and USPIS, we determined that doing a normal 'Trap and Trace' on the aircard would suffice. [redacted] Essentially we would ping the number associated to the card instead of collecting data from the aircard's connection. . . . On 7/16/08, we were informed that they were able to track a signal and were using a 'Stingray' to pinpoint the location of the aircard."), *available at* https://www.aclunc.org/sr09.

[89] A Pen/Trap device would capture the following types of data: phone numbers/IP addresses, location area code (which identifies a group of cell sites and is not related to a phone number area code), cell site ID, cell site sector, and possibly signal strength, singal angle of arrival, and signal time difference of arrival (also called signal time of flight). An IMSI catcher would also capture the foregoing types of data, *except* cell site IDs and location area codes being accessed by the target phone. When a phone connects with and accesses the carrier's network, it accesses cell site IDs and location area codes. When it instead connects with an IMSI catcher, it is no longer accessing the carrier's network and hence is no longer accessing cell site IDs and location area codes. If the data produced by the government in response to this request includes cell site IDs and location area codes – and those cell site IDs and location area codes match those of the carrier – the device used was a Pen/Trap.

[90] A Pen/Trap device collects cell site IDs and location area codes but would not have its own cell site ID and location area code. An IMSI catcher, however, has its own cell site ID and location area code – and this cell site ID and location area code would not typically match any in the wireless carrier's network infrastructure. If the government provides data in response to this request, the device used was an IMSI catcher. This assumes, however, that the prosecution correctly understood the request and did not mistakenly provide cell site IDs and location area codes *collected* by the surveillance device, rather than the cell site ID and location area code *of* the surveillance device. It would be prudent to couple discovery on this issue with a subpoena to the carrier for all location area codes, active cell sites, locations of active cell sites, and the

approximate coverage areas of each active cell site within range of where the defendant's phone was located or identified at the time it was monitored. This would allow comparison between any cell site ID/location area code provided in response to this request with that of the actual carrier.

[91] *See supra* n. 90.

[92] A typical Pen/Trap device will not log its own GPS coordinates, but an IMSI catcher would. It may not however be programmed to retain its GPS coordinates. If the government provides GPS coordinates of the device used to monitor the target phone – and those coordinates reflect multiple geographical locations, or a single geographical location that is not the location of an actual cell site – the device is an IMSI catcher.

[93] It may be prudent to propose that identifying information pertaining to third parties be redacted and replaced with unique numeric identifiers.

[94] *See United States v. Cedano-Arellano,* 332 F.3d 568, 571 (9th Cir. 2003) (narcotics dog's training logs and certification discoverable under Rule 16). Training materials and reports signed by individuals participating in the investigation (requests 10 and 11) would facilitate the identification of the individuals involved in deploying the IMSI catcher.

[95] If the investigation were led by a local police department but the FBI or United States Marshals Service participated in tracking the phone, this might be an indication that a federal agency provided its IMSI catcher.

[96] Law enforcement may use an IMSI catcher to collect information on the carrier's network. An IMSI catcher can be used to conduct a base station survey. A Pen/Trap device would not. If a base station survey is produced in response to this request, an IMSI catcher was used.

[97] To prevent an interference with service to the defendant's phone, the government would have had to make some kind of arrangement with the carrier that would allow the IMSI catcher to become part of its network or develop a mechanism to forward data from the phone to the carrier's network. If one of these arrangements occurred, some documentation should exist.

[98] *See Florida v. Thomas,* Hearing on Motion to Suppress, *supra* note 10, at 17 ("[O]nce the equipment comes into play and we *capture* that handset, to make locating it easier, the equipment *forces that handset to transmit at full power.*") (emphasis added.)

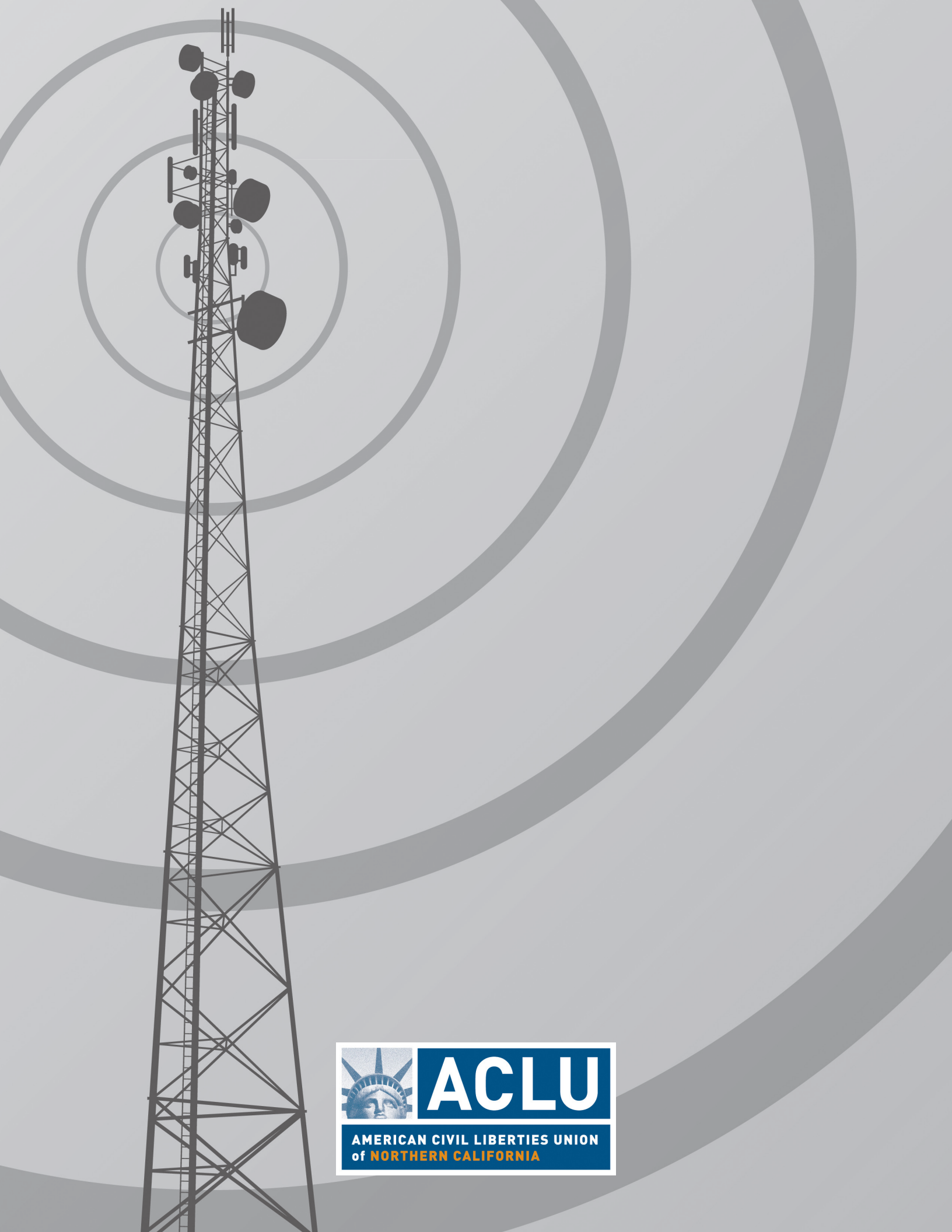
[99] *See Cedano-Arellano,* 332 F.3d at 571 (narcotics dog's training logs and certification discoverable under Rule 16). Training materials may provide information regarding the operation of the device, which might in turn shed light on forced registration and increased power output.

[100] While the government will likely argue that a defendant has no standing to raise third party issues, there is an argument that the impact on third parties is relevant to overbreadth and severability. *See supra* at Section VI-D-2.

[101] This may shed light on whether any omission about IMSI catchers from a warrant affidavit is intentional.

This publication can be found online at:

https://www.aclunc.org/publications/stingrays-most-common-surveillance-tool-government-wont-tell-you-about



ACLU

AMERICAN CIVIL LIBERTIES UNION
of NORTHERN CALIFORNIA