

carrying and using a cell phone that regularly communicates with nearby cell towers, Andrews assumed the risk that the information transmitted to the cell towers would be revealed to the police.

According to Andrews, the third-party doctrine of *Smith v. Maryland*, is inapplicable because “a cell phone user takes no conscious, voluntary action to constantly share location information with a third party.” Andrews maintains that the Supreme Court in *Smith* reached its conclusion using a specific line of reasoning, recognizing that “telephone subscribers ‘realize’ that they send dialed numbers to the telephone company” and by virtue of those numbers appearing on their monthly bills “subscribers ‘realize’ that the dialed numbers are recorded by the telephone company.” Andrews contends that the same cannot be said in the instant case. As Andrews points out, the Court in *Smith* focused on the actual knowledge attributed to telephone users and stated:

All telephone users realize that they must “convey” phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.

Id. at 742. In that context, the court determined that because the “petitioner voluntarily conveyed to [the telephone company] information that it had facilities for recording and that it was free to record[,] . . . petitioner assumed the risk that the information would be divulged to police.” *Id.* at 745.

Although the Supreme Court’s decision in *Smith* has been applied broadly, *see, e.g., United States v. Bynum*, 604 F.3d 161, 162-64 (4th Cir. 2010) (upholding the government’s

use of a subpoena to obtain a website user’s name, email address, telephone number, and physical address—all information that the user entered on the website when he opened his account—from a website operator), it remains that a party must **voluntarily convey** information to a third-party, before there is no longer a reasonable expectation of privacy in that information. *Cf. Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (“This approach [in *Smith*] is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.” (citation omitted)). Recently, in *United States v. Graham, supra*, the Fourth Circuit addressed the application of the third-party doctrine to CSLI and stated:

[The precedents] simply hold that a person can claim no legitimate expectation of privacy in information she voluntarily conveys to a third party. It is that voluntary conveyance—not the mere fact that the information winds up in the third party’s records—that demonstrates an assumption of risk of disclosure and therefore the lack of any reasonable expectation of privacy. We decline to apply the third-party doctrine in the present case because a cell phone user does not “convey” CSLI to her service provider at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement.

796 F.3d at 354 (footnote omitted).

We agree, once again, with the *Graham* court and join in the view shared by other courts that, “[t]he fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by ‘choosing’ to carry a cell phone must be rejected.” *Graham*, 796 F.3d at 355-56 (quoting *In re United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809

F. Supp. 2d 113, 127 (E.D.N.Y. 2011)). Cell phone users do not actively submit their location information to their service provider.

In the present case, there was no affirmative act like “dialing.” This is made abundantly clear by Det. Haley’s testimony stating that “if they’re on the phone, then they’re already connected to . . . the [] network[, a]nd we’re not going to be able to pull them off of that until . . . they hang up the call.” Det. Haley’s testimony reveals that, in the event that an individual is actively using the cell phone to knowingly transmit signals to nearby cell towers, the cell site simulator will not be able to access the phone.

The pin-point location information that led to finding Andrews was obtained directly by law enforcement officers and not through a third-party. It is not the case that Andrews’s cell phone transmitted information to the service provider that was then recorded and shared with law enforcement. Thus, it cannot be said that Andrews “assumed the risk” that the information obtained through the use of the Hailstorm device would be shared by the service provider as in *Smith*. The function of the Hailstorm device foreclosed that possibility. When asked “how do you get information about where the phone is on the [Hailstorm] machine,” Det. Haley responded: “[W]hen [Hailstorm] captures that identifier that you put into the machine or the equipment, it then tells you . . . where the signal’s coming from[.]” Under the facts of this case, the ultimate location data relied on by the police was never transmitted to a third party voluntarily by Andrews. Because there was no third-party element to the use of the Hailstorm by the BPD to locate Andrews, *Smith* is inapposite. We conclude the Third Party Doctrine does not apply in this case.

II.

Standing

One of the State's primary arguments on appeal is that Andrews lacks standing to challenge the search of 5032 Clifton Avenue. The State argues that once it challenged Andrews's standing to protest the search of 5032 Clifton Avenue, the burden was on Andrews to put on evidence during the suppression hearing to establish Andrews's "basis for claiming he had a reasonable expectation of privacy in the contents of someone else's home." The State posits the suppression court erred in "finding that there was no need to prove standing."

Certainly, "[t]he burden is on the defendant to show standing; it is not on the State to show non-standing." *State v. Savage*, 170 Md. App. 149, 177 (2006). In *Savage*, however, this Court clarified that standing "[i]s exclusively a threshold question of applicability, concerned only with the coverage by the Fourth Amendment of the defendant who seeks to raise a Fourth Amendment challenge." *Id.* at 174. Thus, the burden on a proponent of a motion to suppress is to establish "*that his own Fourth Amendment rights were violated by the challenged search or seizure.*" *Id.* at 175 (emphasis in *Savage*) (quoting *Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978)).

Andrews points out that the State "failed to respond in any meaningful way" to his motion to suppress, and did not raise the issue of standing to challenge the search of 5032 Clifton Avenue until well into the June 4, 2015 suppression hearing. Andrews asserts that it was the State's suggestion that the parties stipulate that the issues before the court be decided based on the transcripts, the arrest warrant, the pen register\trap & trace

application, and the search warrant. Andrews contends the State did not raise the standing issue until after the fact-finding portion of the hearing had concluded. At that time, the court requested that Andrews address the issue, and defense counsel made a proffer that Andrews was an overnight guest at 5032 Clifton Avenue and offered to put him on the stand to provide supporting testimony.¹⁸ Andrews argues that the State waived any argument regarding standing, pointing to the State’s delay, its failure to challenge his proffer, and its concession that its trial theory was the fact “that [Andrews] has some interest [in 5032 Clifton Avenue] and that is why the gun from this crime, the murder weapon, was there with him.”

We need not pursue the nuances of the parties’ “standing” argument as they have framed the issue. We have already determined that Andrews had a reasonable expectation of privacy in his aggregate and real-time location information (CLSI) contained in his cell phone. *See Rakas*, 439 U.S. at 139-140 (stating that “the better analysis forthrightly focuses on the extent of a particular defendant’s rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing[.]” and

¹⁸ It is plain that an overnight guest has a legitimate expectation of privacy in his host’s home and “may claim the protection of the Fourth Amendment.” *Carter*, *supra*, 525 U.S. at 90; *Savage*, 170 Md. App. at 188-89. As Andrews points out, defense counsel made a proffer that Andrews was an overnight guest and offered to put testimony to that effect on the record. The State has not seriously challenged Andrews’s connection to the residence, but seeks merely to assert that his unopposed proffer was not sufficient to rebut their late challenge. We observe that—after the State sought to rely on earlier transcripts to provide necessary testimony, failed to challenge standing during the evidentiary portion of the suppression hearing, and left uncontroverted Andrews’s proffer that he was an overnight guest—Andrews’s proffer under the circumstances may have been sufficient to counter the State’s standing argument.

“[t]hat inquiry in turn requires a determination of whether the disputed search and seizure has infringed an interest of the defendant which the Fourth Amendment was designed to protect.”). The search warrant search for 5032 Clifton Avenue was based solely on constitutionally tainted information. As the suppression court explained, “I reviewed the warrant and it literally says the Defendant was in there so now we need a warrant. And information generated from the use of the Hailstorm [is to] be suppressed, that’s all that it is.” Because the Fourth Amendment violation of Andrews’s privacy in his real-time CSLI provided the only nexus to 5032 Clifton Avenue, Andrews was entitled to challenge that search. *See Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963) (stating that, in determining whether evidence is fruit of the poisonous tree, “the more apt question in such a case is whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.” (citation and internal quotation marks omitted)). For the foregoing reasons, Andrews had standing to challenge the “search” of 5032 Clifton Avenue.

III.

The Warrant Requirement

Having determined that the government’s use of a cell site simulator to obtain location information directly from an individual’s cell phone is a “search” under the Fourth Amendment, and, therefore, requires a warrant based on probable cause, we now examine the state’s reliance on the pen register\trap & trace order issued by the circuit court. First, we examine whether the Maryland pen register statute authorized the use of a cell site

simulator. Second, we examine whether the putative pen register\trap & trace order in this case operated as the equivalent of a warrant as the State contends.

a. The Maryland Pen Register Statute Does Not Authorize the Use of Cell Site Simulators Such as Hailstorm

The function of the Hailstorm device, as illuminated by testimony before the suppression court, places it outside the statutory framework of the Maryland pen register statute. The statute authorizes the use of the following surveillance methods defined in CJP §10-4B-0.1:

Pen register

(c)(1) “Pen register” means a device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.

(2) “Pen register” does not include any device or process used:

- (i) By a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by the provider or any device used by a provider or customer of a wire communication service for cost accounting or other similar purposes in the ordinary course of its business; or
- (ii) To obtain the content of a communication.

Trap and trace device

(d)(1) “Trap and trace device” means a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.

(2) “Trap and trace device” does not include a device or process used to obtain the content of a communication.

Wire communication, electronic communication, and electronic communication service

(e) “Wire communication”, “electronic communication”, and “electronic communication service” have the meanings stated in § 10-401 of this title.

The statute specifies that any order issued must identify, if known, “the person to whom is leased or in whose name is listed the **telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.**” CJP § 10-4B-04(b)(1) (emphasis added).

Construing the plain language of CJP § 10-4B-01, we determine that it does not, on its face, apply to the use of cell site simulators. A “pen register” is “a device or process that records . . . signaling information transmitted by an instrument . . . **from which a wire or electronic communication is transmitted.**” CJP § 10-4B-01(c)(1) (emphasis added). As discussed above, the Hailstorm device does not passively intercept an electronic communication that has been transmitted. Rather, it initiates contact with a cell phone and traces the signal received in response. A “trap and trace device” is a “device or process that captures the **incoming electronic or other impulses** that identify the originating number or other dialing, routing, addressing, and **signaling information reasonably likely to identify the source of a wire or electronic communication.**” CJP § 10-4B-01(d)(1) (emphasis added). The function of the Hailstorm device—to shower an electronic barrage of signals into a target area to actively engage the target cell phone—goes well beyond the bounds of the pen register statute which by its terms is limited to authorizing devices that record or identify the source of a communication or capture an originating number.

The Maryland pen register statute has been examined in only one reported opinion by a Maryland appellate court.¹⁹ *See Chan v. State*, 78 Md. App. 287, 293 (1989)

¹⁹ In the federal district court in *United States v. Wilford*, a defendant more recently argued that cell phone ping was not authorized by Maryland’s pen register statute. 961

(upholding the use of a trap and trace device pursuant to a court order to obtain data from over 5,000 calls over an eighty-day period). In *Chan*, although this Court determined that the newly enacted Maryland pen register statute was not applicable because it did not take effect until July 1, 1988, it stated that the new statute “unquestionably cover[ed]” the “trap and trace” of incoming calls and observed:

In response to the Electronic Communications Privacy Act of 1986 passed by the Federal Congress, the Maryland General Assembly moved for the first time to regulate “pen registers” and “trap and trace” devices by Chapter 607 of the Acts of 1988. The new regulation is not part of the “Wiretapping and Electronic Surveillance” subtitle but is a separate subtitle of its own, 4B, dealing with the distinct subject matter of “Pen Registers and Trap and Trace Devices.” **Its provisions and its wording are virtually verbatim with those of its Federal counterpart.**

Id. at 308 (emphasis added).

In 2001, Congress amended the definition of the term “pen register” in the federal counterpart as part of the USA PATRIOT Act. *See* PL 107–56, October 26, 2001, 115 Stat 272. Subsequently, in 2002, the Maryland pen register statute was also amended to the current versions, reproduced above. 2002 Md. Laws, ch. 100 (H.B. 1036). Notably, since

F. Supp. 2d 740, 768 (D. Md. 2013), *on reconsideration in part* (Nov. 27, 2013). In that case, the defendant maintained that the statutory language “is limited to providing law enforcement numbers that dialed into the target phone and numbers dialed out,” but does “not contemplate” the use of a cell phone as a “physical locator/tracking device.” *Id.* at 769. The district court noted that “[n]o judicial decision offers any guidance as to the scope of the Maryland statute with respect to ping[ing].” *Id.* However, rather than address whether the collection of CSLI was authorized by the pen register statute, the district court accepted that contention *arguendo* and, instead, based its holding on the unavailability of suppression as a remedy for violation of the statute. *Id.* at 770.

Chan was decided in 1989, the wording of the Maryland statute remains virtually verbatim with its federal counterpart. *See* 18 U.S.C. § 3127; 18 U.S.C. § 2510.

Looking then, at the federal statutory scheme, we note that the federal Communications Assistance for Law Enforcement Act (“CALEA”), which delineates a telecommunications carrier’s duty to cooperate in the interception of communications for law enforcement purposes, provides that “with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), **such call-identifying information shall not include any information that may disclose the physical location of the subscriber** (except to the extent that the location may be determined from the telephone number).” 47 U.S.C. § 1002 (2015) (emphasis added). Thus, federal law specifies that the federal equivalent to the Maryland pen register statute does not authorize location information. Rather, the federal scheme allows the government to use a mobile tracking device through warrant or other order as contemplated in 18 U.S.C. § 3117 and Federal Rule of Criminal Procedure 41.

Although there are no reported opinions that address whether the collection of real-time cell site location information (CSLI) is authorized under the Maryland’s pen register statute, numerous federal courts construing the virtually identical federal statutes have found no statutory authorization for obtaining such information without demonstrating probable cause. In 2005, the United States District Court for the Southern District of Texas held that the government must demonstrate probable cause and obtain a search warrant to obtain real-time CSLI. *In re Application for Pen Register & Trap/Trace Device with Cell*

Site Location Auth., 396 F. Supp. 2d 747, 759 (S.D. Tex. 2005). Construing the federal statutes, the district court stated:

Tracking device information such as cell site data is plainly not a form of electronic communication at all.

* * *

This type of surveillance is unquestionably available upon a traditional probable cause showing under Rule 41 [for a mobile tracking device]. On the other hand, permitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns, especially when the phone is monitored in the home or other places where privacy is reasonably expected.

Id. at 759, 765. See also *In re Application of the United States for an Order Authorizing Installation & Use of a Pen Register*, 415 F. Supp. 2d 211, 219 (W.D.N.Y. 2006) (holding that the government was not entitled to real-time CSLI by statute and thus, was required to make a “showing that there exists probable cause to believe that the data sought will yield evidence of a crime.”). Directly addressing the use of a cell site simulator (such as Stingray or Hailstorm) to obtain real-time CSLI for tracking purposes, the District Court for the Southern District of Texas determined that, rather than merely capturing signaling information as contemplated in the federal pen register statute, the use of a cell site simulator constituted a mobile tracking device. *In re the Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012).

We acknowledge that law enforcement has long relied on pen register\trap & trace orders for valid and vital investigative purposes. They will continue to do so. The pen register statute, however, is limited by its terms and is not intended to apply to other, newer

technologies. Thus we hold that a pen register\trap & trace order is not sufficient to authorize use of the Hailstorm.²⁰

Criminal Procedure § 1-203.1

Although at the time Andrews was arrested Maryland did not have a corollary to the provision in Federal Rule of Criminal Procedure 41 that specifically authorizes issuance of a warrant for a mobile tracking device, Maryland has since enacted a statute authorizing law enforcement to obtain real-time CSLI, effective October 1, 2014. Maryland Code (2001, 2008 Repl. Vol., 2014 Supp.) Criminal Procedure Article (“CP”) § 1-203.1. The statute provides that a court may issue an order allowing an officer to obtain real-time location information from an electronic device based on probable cause that:

- (i) a misdemeanor or felony has been, is being, or will be committed by the owner or user of the electronic device or by the individual about whom location information is being sought; and
- (ii) the location information being sought:

- 1. is evidence of, or will lead to evidence of, the misdemeanor or felony being investigated; or

²⁰ Federal law enforcement agencies have recognized that they need to obtain warrants rather than rely on less rigorous legal authorizations before utilizing cell site simulators. On September 3, 2015, the United States Justice Department of Justice announced a new policy setting forth required practices with respect to the treatment of information collected through the use of cell site simulators and stated:

While the department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, **law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator.**

Justice News, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators, DOJ 15-1084 (2015) (emphasis added).

2. will lead to the apprehension of an individual for whom an arrest warrant has been previously issued.

CP § 1-203.1(b)(1). The Fiscal and Policy Note prepared by the Department of Legislative Services for the General Assembly concerning this statute when it was first proposed, recognized that law enforcement officers were using the Maryland pen register statute to obtain cell phone-related information. It explained that the proposed statute would specifically authorize the capture of CSLI in accord with several recent federal court decisions finding that probable cause was needed to obtain such information. Fiscal and Policy Note (Revised), Senate Bill 698, Criminal Procedure – Electronic Device Location Information – Order (2014). The fiscal and policy note also contemplated the use of cell site simulators and stated:

While cell phone records are usually obtained from a cell phone provider, technology is making it possible for law enforcement to bypass these companies altogether. Certain devices allow law enforcement to obtain location data by imitating a cell phone tower, getting a phone to connect with it, and measuring signals from the phone to pinpoint its location. The device, which is being used by the Federal Bureau of Investigation, the military, and local law enforcement, is known by several trade names, including StingRay, KingFish, and LoggerHead.

Notably, CP § 1-203.1 contains safeguards and limitations not found in the Maryland pen register statute, including a thirty-day durational limit on the collection of location information unless an extension is sought on continuing probable cause, and a provision requiring notice to the user or owner of the monitored device within 10 days absent a showing of good cause to delay. CP § 1-203.1(c) & (d).

The parties have briefed extensively their view of the meaning and application of CP 1-203.1. Other than to provide context for the history of the Maryland pen register

statute and our conclusion that it was not intended to cover cell site simulators, we do not address the application of CP 1-203.1 and decline to opine as to whether an order under CP 1-203.1 will suffice to satisfy the requirements of a warrant based on probable cause.

In sum, we conclude that the purpose of Maryland's pen register statute is to capture information resulting from two-way, electronic or wire communications. Nothing in the plain language of CJP § 10-4B-01 *et seq.* suggests that it was ever intended to allow surveillance technology that can exploit the manner in which a cell phone transmits data to convert it into a mobile tracking device. Accordingly, an order issued pursuant to CJP § 10-4B-04 cannot authorize the use of a cell site simulator, such as Hailstorm. Because there was no statutory authorization for the BPD's use of the Hailstorm cell site simulator, we hold that the BPD should have sought a warrant or a specialized order upon a particularized showing of probable cause, and based on sufficient information about the technology involved to permit the court to contour reasonable limitations on the scope and manner of the BPD's use of the device.²¹ *See, e.g., In re Application of the United States for an Order Authorizing Installation & Use of a Pen Register*, 415 F. Supp. 2d at 219.

b. The Order Obtained by the State Was Not Equivalent to a Warrant

The State insists that its use of the Hailstorm device to track Andrews's cell phone was authorized by the court order. In the absence of a specific statute that would have

²¹ To the extent that the State makes a limited argument that there is no suppression remedy available for violation of the sections 10-4B-01 *et seq.*, we respond simply that the circuit court found, and we agree, that the use of the cell site simulator was a Fourth Amendment violation and, thereby, the exclusionary rule applies. The fact that there may have been a contemporaneous violation of sections 10-4B-01 *et seq.* does not limit the available remedy.

authorized the use of a cell site simulator at the time Andrews was arrested, the State presses that “the police erred on the side of caution and obtained a court order specifically authorizing the use of a cellular tracking device to find Andrews’s phone[,]” pursuant to the “nearest analog”—the Maryland pen register statute. The State acknowledges that the court order described in the Maryland pen register statute does not use the words “warrant” or “probable cause.” Nevertheless, the State argues that, in this case, the BPD’s application and the resulting order “went far beyond the requirements of the statute.”

The State points out that the BPD application was for an order allowing the police to employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of a Pen Register\Trap & Trace and Cellular Tracking Device [. . .] and shall initiate a signal to determine the location of the subject’s mobile device on the service provider’s network or with such other reference points as may be reasonabl[y] available . . .

The State also notes that the resultant order states that probable cause exists to authorize the use of a “Cellular Tracking Device.” Thus, the State contends that because the pen register\trap & trace order stated that it was based upon a finding of probable cause, it was, therefore, “the functional equivalent of a warrant.”

Andrews emphasizes that the order may issue on just a showing “that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation.” CJP § 10-4B-04(a)(1). In addition to the fact that a pen register\trap & trace order does not contemplate the use of a cell site simulator, Andrews points out that it also does not satisfy the requirements that a warrant based on probable cause be attached to a specific suspected crime, be confined in scope, or describe with

particularity the place to be searched or the person to be seized. Andrews contends that “[t]he moment BPD conducted surveillance with something other than a pen register, it exceeded the purview of the pen register order.” Further, Andrews contends that BPD’s application “For an Order Authorizing the Installation and Use of a Device Known as a Pen Register/Trap & Trace,” was intentionally captioned to ensure that the circuit court scrutinized it according to the statutory pen register factors. Andrews argues that BPD’s “disingenuous efforts” hid from the circuit court “the scope, intensity, [and] nature of the search,” and prevented the court from conducting a proper probable cause analysis.

We begin with our appraisal that an order issued under the pen register statute is not the equivalent of a warrant based on probable cause—a fact the State implicitly concedes in its argument that it “went beyond the requirement of the statute.” The applicable requirements of the statute are contained first in § 10-4B-03:

(b) *Contents.* — An application under subsection (a) of this section shall include:

- (1) The identity of the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
- (2) A statement under oath by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Additionally, 10-4B-04(a) states that an order may issue if the court finds the information likely to be obtained by the device is relevant to an ongoing criminal investigation, and the order must:

- (3) Specify the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace

device is to be attached or applied, and, in the case of a trap and trace device, the geographic limits of the trap and trace order;
(4) Contain a description of the offense to which the information likely to be obtained by the pen register or trap and trace device relates[.]

CJP § 10-4B-04(b)(3) & (4). Plainly, this limited showing falls short of the particularity required for the issuance of a search warrant. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983) (“The task of the issuing magistrate is simply to make a practical, common-sense decision whether . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.”); *Nero v. State*, 144 Md. App. 333, 345-46 (2002) (“General warrants, of course, are prohibited by the Fourth Amendment. . . . [T]he problem [posed by the general warrant] is not that of intrusion per se, but of a general, exploratory rummaging in a person’s belongings. . . . [The Fourth Amendment addresses the problem] by requiring a ‘particular description’ of the things to be seized.” (quoting *Andresen v. Maryland*, 427 U.S. 463, 480 (1976))).

Moving to the State’s argument that the order was sufficient because it went beyond the requirements of the statute, we start by rejecting the State’s contention that the words “probable cause” contained in the pen register application and order converted the overreaching order into a warrant. The “probable cause” articulated in the resulting order is merely that “**information likely to be obtained . . . is relevant to an ongoing criminal investigation.**” (Emphasis in original). Certainly, while this reflects the standard required for issuance of an order under CJP § 10-4B-04, it falls far short of the particularity required to support a search warrant. *See Gates*, 462 U.S. at 238; *Nero*, 144 Md. App. at 345-46.

In the information “offered in support of probable cause” the application states:

Your Applicant hereby certifies that the information likely to be obtained concerning [Andrews's] location will be obtained by learning the numbers, locations and subscribers of the telephone number(s) being dialed or pulsed from or to the aforesaid telephone and that such information is relevant to the ongoing criminal investigation.

Plainly, the State's use of the Hailstorm device extended far beyond this certification as to how information concerning Andrews's location would be obtained.

Here, the State inserted language into its application and proposed order attempting to, without being specific, obtain court authorization for more than a pen register\trap & trace order. Although the application does request authorization to use a "Cellular Tracking Device," it fails to name or describe any cell site simulator. In fact, there is absolutely nothing in the application or order that identifies the Hailstorm device, or provides even a rudimentary description of cell site simulator technology. The application also failed to identify any geographical limitation to the BPD's use of the undisclosed surveillance technology, and did not explain what was to be done with the information collected. Nor did the application disclose the possibility that the technology employed may capture the cell phone information (unique serial numbers) of innocent third parties in range of the target area. Finally, we are troubled that the application for a pen register\trap & trace order did not fully apprise the circuit court judge from whom it was sought of the information that it would yield. Based on the application that he received, the circuit judge was entitled to expect that the results would be a list of telephone numbers that Andrews called and that called Andrews—not a real-time fix on his location.

We determine that the pen register\trap & trace order in this case failed to meet the requirements of a warrant. To allow the government to collect real-time location

information on an unknown number of private cell phones, without any geographic boundaries, without any reporting requirements or requirements that any unrelated data be deleted, and without a showing of probable cause that contraband or evidence of a particular crime will be found through the particular manner in which the search is conducted would certainly run afoul of the Fourth Amendment. As stated in our holding above, unless a valid exception to the warrant requirement applies,²² the government may not use a cell phone simulator without a warrant or, alternatively, a specialized order that requires a particularized showing of probable cause, based on sufficient information about the technology involved to allow a court to contour reasonable limitations on the scope and manner of the search, and that provides adequate protections in case any third-party cell phone information might be unintentionally intercepted. To hold otherwise would be to

²² One of the exceptions more commonly relied upon applies when ‘the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.’” *Kentucky v. King*, 563 U.S. 452, 460 (2011) (some internal quotation marks omitted) (quoting *Mincey v. Arizona*, 437 U.S. 385, 394 (1978)). Maryland has recognized that “[e]xigent circumstances exist when a substantial risk of harm to the law enforcement officials involved, to the law enforcement process itself, or to others would arise if the police were to delay until a warrant could be issued.” *Williams v. State*, 372 Md. 386, 402 (2002) (citations omitted). It remains the State’s burden to establish exigent circumstances sufficient to justify a warrantless search. *Wengert v. State*, 364 Md. 76, 85 (2001) (citations omitted). We note that the Supreme Court in *Riley, supra*, rejected the argument that officer safety, in that case, presented an exigent circumstance that justified officer’s accessing content on a cell phone seized in a search incident to arrest. The Court observed that “[t]o the extent dangers to arresting officers may be implicated in a particular way in a particular case, they are better addressed through consideration of case-specific exceptions to the warrant requirement, such as the one for exigent circumstances.” 134 S. Ct. at 2486.

abandon the Fourth Amendment by assuming, without any foundation, that the citizens of Maryland have forfeited their reasonable expectation of privacy in their personal location.

IV.

The Exclusionary Rule

a. The Search Warrant Does Not Survive Removal of the Constitutionally Tainted Information.

The State contends that the search warrant that was obtained for 5032 Clifton Avenue was valid because probable cause existed once “Andrews was found in the home.” According to the State, Andrews was arrested pursuant to a valid arrest warrant and the police had “the consent of the apparent owner of the home to enter the home to take Andrews into custody.” Thus, the State argues, “[n]othing about the way in which Andrews was located negated the probable cause to believe that there could be evidence of the crimes at that address.”

In riposte, Andrews avers that without the location data provided by the cell site simulator, “the BPD possessed no nexus between the criminal activity at hand and 5032 Clifton Avenue.” Andrews asserts that, “[b]ecause the search warrant relied entirely on that nexus, it withers as fruit of the poisonous tree.”

First, we note that where entry into a protected space “was demanded under color of office” and “granted in submission to authority,” that submission does not equate to a waiver of a constitutional right. *Johnson, supra*, 333 U.S. at 13 (citing *Amos v. United States*, 255 U.S. 313 (1921)). Thus, the existence of an arrest warrant and the consent of

the owner of the residence do not, in themselves, diminish Andrews's protection under the Fourth Amendment. Nor do they render the later-acquired search warrant unassailable.

Second, the courts of Maryland have recognized that where a search warrant relies on information obtained in violation of the constitution, the question is "whether 'after the constitutionally tainted information is excised from the warrant, the remaining information is sufficient to support a finding of probable cause.'" *Redmond v. State*, 213 Md. App. 163, 191-92 (2013) (quoting *Williams v. State*, 372 Md. 386, 419 (2002)). *See also Karo*, 468 U.S. at 720-21 (stating that in determining whether evidence seized pursuant to a contested warrant remains admissible, one of the pertinent questions is whether "the warrant affidavit, after striking the [constitutionally tainted] facts . . . contained sufficient untainted information to furnish probable cause for the issuance of the search warrant.") Here, there can be no doubt that the only information linking Andrews and 5023 Clifton Avenue was the fruit of the Fourth Amendment violation. The State presents no credible argument that evidence of Andrew's presence in the home was obtained by independent lawful means.

In *Redmond v. State*, the BPD were investigating an armed robbery in which a cell phone was stolen. 213 Md. App. at 169. During their investigation, detectives contacted the victim's mobile service provider and, "by triangulating the signal from cell phone towers in the area, determined that the stolen cell phone was in the proximity of 3303 Round Road." *Id.* at 169. Thereafter, detectives began moving from house to house in the area, speaking to residents using a ruse that they were "looking for a pedophile named 'Leroy Smalls.'" *Id.* at 170. After obtaining consent to enter the appellant's residence

under those false pretenses, one of the detectives surreptitiously dialed the number of the stolen cell phone, heard it ringing upstairs, and then walked through the entire house conducting a “protective sweep” including opening closet doors and checking under beds. *Id.* at 171. Officers then sought a search warrant for the home on the basis of what they had discovered in the home. *Id.* at 171-72.

After a careful analysis, we determined that “[b]y dialing the number of the stolen cell phone and walking upstairs to locate it, the police exceeded the scope of any consent that was given to their presence inside 3303 Round Road.” *Id.* at 189-90. Applying the exclusionary rule, we noted that “all the information . . . attested to in applying for the search warrant (and on which the search warrant was granted) . . . was discovered during the initial illegal entry.” *Id.* at 192. We determined that the search warrant was not issued based on an independent lawful source and the unlawfully obtained evidence should be suppressed.²³ *Id.* And, we soundly rejected the argument that evidence in a warrant

²³ Although the warrant application in *Redmond* mentioned reliance on “sophisticated mobile and/or portable surveillance equipment” to locate the stolen cell phone, in that case we observed that:

Detective Jendrek did not testify that the ATT used *any* “sophisticated mobile and/or portable surveillance equipment” while in the 3300 block of Round Road. Rather, his testimony was that the ATT detectives confirmed the precise location of the cell phone by use of ordinary police investigatory tactics: speaking to the occupants of two houses, dialing the number of the stolen cell phone, listening for it to ring, and, ultimately, physically observing the stolen cell phone lying on a dresser.

Thus, to the extent that the averments in the search warrant application represent that the ATT detectives used “sophisticated” means to locate the

application was obtained by independent lawful means “(1) where the officer’s decision to seek the warrant was prompted by what they had seen during the initial entry; and (2) where information obtained during that entry was presented to the [judge] and affected his [or her] decision to issue the warrant.” *Id.* at 191 (internal quotation marks omitted) (alterations in *Redmond*) (quoting *Kamara v. State*, 205 Md. App. 607, 627-28 (2012)). *See also Murray v. United States*, 487 U.S. 533, 534 (1988) (“The ultimate question is whether the search pursuant to warrant was in fact a genuinely independent source of the information and tangible evidence at issue. This would not have been the case if the agents’ decision to seek the warrant was prompted by what they had seen during the initial entry or if information obtained during that entry was presented to the Magistrate and affected his decision to issue the warrant.”).

As in *Redmond*, here, the evidence that forms the only basis for probable cause in the State’s search warrant application—that Andrews was at 5032 Clifton Avenue—was that obtained through an unlawful search—in this case, the BPD’s use of the Hailstorm device. We agree with the circuit court’s determination that there was no independent lawful source to establish a nexus between Andrews and the residence. *Cf. Agurs v. State*, 415 Md. 62, 84 (2010) (stating that “police should have been aware that there must be a

stolen cell phone while at the scene on the afternoon of March 2, 2010, they are simply inaccurate.

213 Md. App. at 193. The defendant in *Redmond* did not challenge the use of any such device or the use of cell tower information. Accordingly, in *Redmond* we did not address the use of sophisticated mobile surveillance systems, as we must in the matter *sub judice*.

nexus between criminal activity and the place to be searched.”). Accordingly, once the constitutional taint is removed from the search warrant in this case, what remains is insufficient to establish probable cause for a search of 5032 Clifton Avenue and, as discussed further *infra*, the evidence seized in that search withers as the fruit of the poisoned tree. *Franks v. Delaware*, 438 U.S. 154, 156 (1978) (stating that if “the affidavit’s remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.”). Therefore, we affirm the suppression court’s exclusion of all evidence found at 5032 Clifton Avenue.

b. The State Cannot Rely on the Good Faith Exception

Finally, the State argues that BPD’s relied in good faith on the search warrant issued for 5032 Clifton Avenue after locating Andrews inside that address. The State asserts that police officers relied on, first, the pen register\trap & trace order, and, second, on the later issued search warrant for the premises. The State maintains that “[t]his is good faith squared[,]” and there is “simply no officer misconduct to deter in this case.” Thus, the State contends that the exclusionary rule should not apply in this case.

Andrews contends that without the location information provided by the cell site simulator the BPD possessed no nexus between him and 5032 Clifton Avenue, and, “[b]ecause the search warrant relied entirely on that nexus, it withers as the fruit of the poisonous tree.” Andrews asserts that where the information relied on to obtain a warrant is the product of a Fourth amendment violation, the fruit of the poisonous tree doctrine

trumps the good faith exception. Moreover, Andrews argues that good faith cannot apply where “law enforcement officers, from the outset, dealt dishonestly with the judiciary.”

In *United States v. Leon*, the Supreme Court held that, where officers have acted in good faith pursuant to a warrant that was later discovered to be invalid, exclusion is not warranted to deter police over-reach or misconduct. 468 U.S. 897, 924 (1984). The Supreme Court cautioned, however, that

[t]he good-faith exception for searches conducted pursuant to warrants is not intended to signal our unwillingness strictly to enforce the requirements of the Fourth Amendment, and we do not believe that it will have this effect. As we have already suggested, the good-faith exception, turning as it does on objective reasonableness, should not be difficult to apply in practice. When officers have acted pursuant to a warrant, the prosecution should ordinarily be able to establish objective good faith without a substantial expenditure of judicial time.

In *Fitzgerald v. State*, this Court aptly summarized the “good faith” exception:

Because the only purpose of the Exclusionary Rule of *Mapp v. Ohio*, 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961), is to deter unreasonable police behavior, *Leon* and [*Massachusetts v. Sheppard*, 468 U.S. 981 (1984)] held that a mistake made by a judge in issuing a warrant should not be attributed to the police officer who executes it. Because the officer has been reasonable in relying on the judge’s legal expertise, it would serve no deterrent purpose to exclude otherwise competent, material, and trustworthy evidence. See *Connelly v. State*, 322 Md. 719, 720–21, 589 A.2d 958 (1991).

153 Md. App. 601, 655-56 (2003) *aff’d*, 384 Md. 484 (2004). However, this Court observed that in *Karo, supra*, the Supreme Court instructed that, if the information obtained through a Fourth Amendment violation “proved critical to establishing probable cause for the issuance of the warrant,” it would invalidate the subsequent search warrant for the house. *Id.* at 656 (citing *Karo, supra*, 468 U.S. at 719). Accordingly, “the conclusion may readily be drawn that in the case of an antecedent Fourth Amendment violation which

contributes to a warrant application, the ‘fruit of the poisoned tree’ doctrine ‘trumps’ the officer’s ‘good faith’ reliance under *Leon* and *Sheppard*.” *Id.*

Here, as we noted above, the BPD submitted an overreaching pen register\trap & trace application that failed to clearly articulate the intended use, i.e., to track Andrews’s cell phone using an active cell site simulator. The ensuing order did not support the use of the Hailstorm device, nor did it, in any way, serve as a de facto warrant for the use of the Hailstorm device. As the State’s May 15, 2015 supplemental disclosure made clear, “WATF did not have the Clifton Ave address as a possible location until ATT provided that information.” Only after receiving that information through the use of the Hailstorm device and arresting Andrews at the premises did the same BPD officers who submitted the pen register\trap & trace application then apply for a search warrant.

As Andrews points out, without the antecedent Fourth Amendment violation the nexus between the residence to be searched and the alleged criminal activity could not have been established. *Cf. Agurs*, 415 Md. at 84 (stating that “police should have been aware that there must be a nexus between criminal activity and the place to be searched.”). In the present case, the antecedent Fourth Amendment violation was the only basis upon which the search warrant application stood, and the fruit of the poisoned tree doctrine does, indeed, trump alleged good faith reliance on the part of BPD. *See Fitzgerald*, 153 Md. App. at 656.

The Supreme Court in *Leon*, was clear that “the officer’s reliance on the magistrate’s probable-cause determination and on the technical sufficiency of the warrant he issues must be objectively reasonable.” 468 U.S. at 922. *See, e.g., Spence v. State*, 444 Md. 1, 12-13

(2015) (wherein the police officer, in searching a cell phone and reading text messages during a search incident to arrest, was acting in good faith reliance on then-controlling authority in Maryland); *Agurs*, 415 Md. at 83 (concluding that the good faith exception did not apply where “no reasonably well-trained police officer could have relied on the warrant that authorized the search of Agurs’ home.”). We cannot say the BPD officers in this case reasonably relied on the warrant obtained through their own misleading order application and unconstitutionally intrusive conduct. To do so would allow law enforcement to insulate its own errors merely by presenting limited information to a magistrate, obtaining a warrant post-intrusion, and then re-entering the place to be searched. The good faith exception to the exclusionary rule seeks to avoid “[p]enalizing the officer for the magistrate’s error, rather than his own.” *Leon*, 468 U.S at 921. That is, however, not that case here. *See id.* at 919 (“The deterrent purpose of the exclusionary rule necessarily assumes that the police have engaged in willful, or at the very least negligent, conduct which has deprived the defendant of some right. By refusing to admit evidence gained as a result of such conduct, the courts hope to instill in those particular investigating officers, or in their future counterparts, a greater degree of care toward the rights of an accused.” (quoting *United States v. Peltier*, 442 U.S. 531, 539 (1975))).

It is for all of these reasons that we hold that the evidence obtained in the search of 5032 Clifton Avenue is inadmissible as fruit of the poisoned tree and was properly excluded by the suppression court.

**JUDGMENTS OF THE CIRCUIT
COURT FOR BALTIMORE CITY
AFFIRMED.**

**COSTS TO BE PAID BY MAYOR AND
CITY COUNCIL OF BALTIMORE.**

From: (b)(6); (b)(7)(C)
Sent: 28 Aug 2018 20:51:00 +0000
To: (b)(6); (b)(7)(C)
Subject: (b)(7)(E) PPT
Attachments: Cell-site Simulator PP (2nd).ppt, GPS Maritime - Final to (b)(6); (b)(7)(C) docx, GPS Hypotheticals.docx

(b)(7)(E)

Start at slide 137.

(b)(6); (b)(7)(C)

Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) (office)
202-500-(b)(6) (mobile)

(b)(6); (b)(7)(C)

***** WARNING *** ATTORNEY/CLIENT PRIVILEGE *** ATTORNEY WORK PRODUCT *****

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~



U.S. Immigration and Customs Enforcement

(b)(6); (b)(7)(C)

Associate Legal Advisor

Homeland Security Investigations Law Division

Criminal Law Section

Office of the Principal Legal Advisor

August 2016

Overview

- OPLA
 - CLS
 - HSI Embed Program
- Introduction to Cell-Site Simulators
- Reintroduction to Fourth Amendment Search and Seizure
 - The Pen Register Statute and the Electronic Communications Privacy Act of 1986
- Cell-Site Simulator Policy



Overview: OPLA

- ICE Office of the Principal Legal Advisor
 - Headquarters
 - Overview of Divisions
 - Homeland Security Investigations Law Division
 - Criminal Law Section
- Offices of the Chief Counsel
 - HSI Embedded Attorney



What are Cell-Site Simulators?

- Purpose?

- (b)(5); (b)(7)(E)
-
-

- How do they work?

- (b)(5); (b)(7)(E)
-
-



Use of Cell-Site Simulators

ICE must use cell-site simulators in a manner consistent with the protections of the U.S. Constitution, specifically the Fourth Amendment, and applicable statutory authorities, notably the Pen Register Statute.



Fourth Amendment and How it Protects

The right of the people to be secure in their persons, houses, papers, and effects, against **unreasonable searches and seizures**, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.



ICE

Fourth Amendment: Exclusionary Rule

(b)(5); (b)(7)(E)



U.S. Immigration
and Customs
Enforcement

ICE

Fourth Amendment Exclusionary Rule: Exception

(b)(5); (b)(7)(E)



U.S. Immigration
and Customs
Enforcement

Searches

- Government participation
- Intrusion (physical, visual, auditory)
- Reasonable Expectation of Privacy (“REP”)
 - Subjective expectation of privacy
 - Objectively reasonable



ICE

No REP

- Open fields
- Open view
- Overheard conversations
- Abandoned Property
- Trash
- Odors
- Items previously and lawfully searched
- Movement of vehicles and containers in public



U.S. v. Jones

- Warrantless Installation of GPS Tracker
 - Intent to obtain information + Trespass
 - Short duration monitoring permissible
- 48-hour rule (DOJ policy)
- Inapplicable situations
 - Exceptions to warrant requirement
 - Commercial vehicles, aircraft, vessels
 - Border searches
 - Per se reasonable
 - Extended border search
 - Extraterritorial application



General Rule - Warrants

- Warrantless searches & seizures generally are presumed to be unreasonable unless a reasonable exception applies
- Requirements:
 - Probable Cause
 - Particularity



Warrants & Electronic Devices

- Scope
- Particularity
- Retention
- Time limits



Exceptions to Warrants But PC Still Needed

- Arrest in a Public Place
- Plain View
 - Lawful presence/access
 - Probable cause to seize is immediately apparent
- Mobile Conveyances
- **Exigent Circumstances**



Exceptions – Warrant & PC

- Protective Sweep
- Stop/Frisk
- Inventory
- Regulatory
- Administrative
- Search Incident to Arrest
- Consent
- Border Search



The Pen Register Statute and ECPA

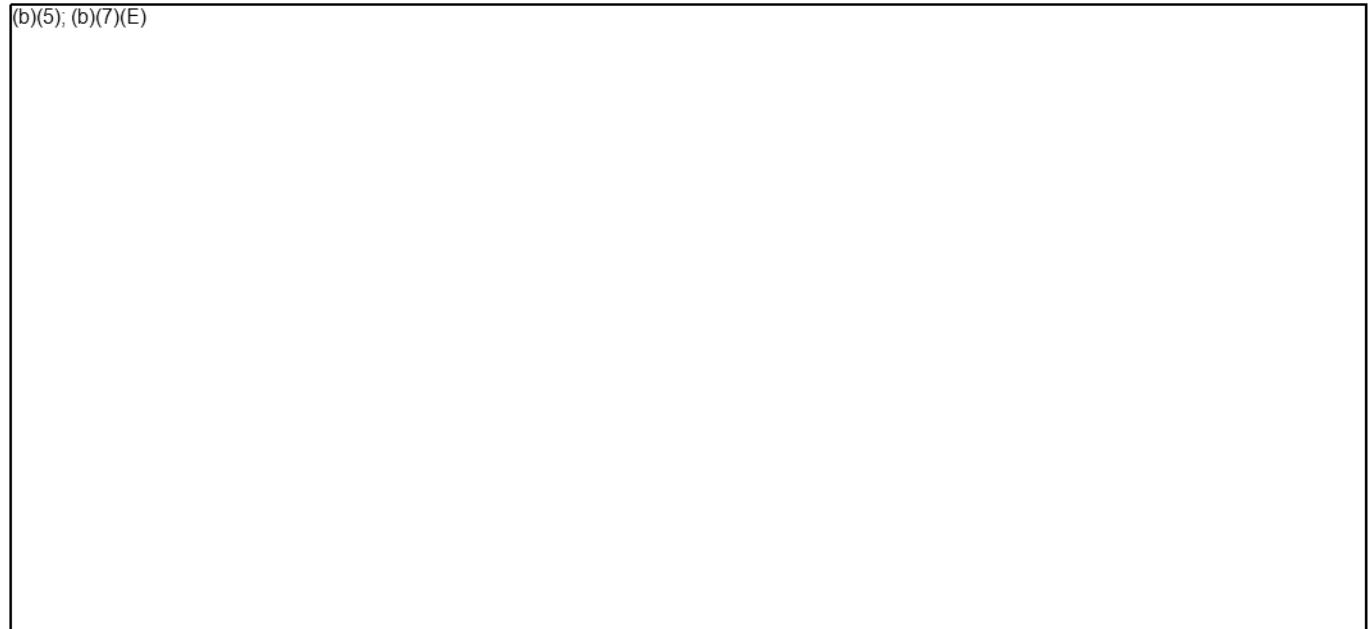
- The Pen Register Statute is a component of the Electronic Communications Privacy Act of 1986 (“ECPA”), which is also comprised of the Stored Communications Act and amendments to the Wiretap Act.
 - § ECPA Controls the collection and disclosure of content and non-content information related to electronic communications, as well as content that has been stored remotely.
 - w Title I of ECPA – Wiretap Act
 - w Title II of ECPA – Stored Communications Act
 - w **Title III of ECPA – Pen register and trap and trace devices**
- As noted above, a cell-site simulator must be configured as a pen register.



ICE

Pen Register and Trap and Trace Devices

(b)(5); (b)(7)(E)



U.S. Immigration
and Customs
Enforcement

ICE

Cell-Site Simulator Policy

Must obtain a search warrant supported by **probable cause** and issued pursuant to rule 41 of the Federal Rules of Criminal Procedure, **unless** there is an exigent circumstance under the Fourth Amendment or an exceptional circumstance.



U.S. Immigration
and Customs
Enforcement

Cell-Site Simulator Policy

Exigent Circumstances

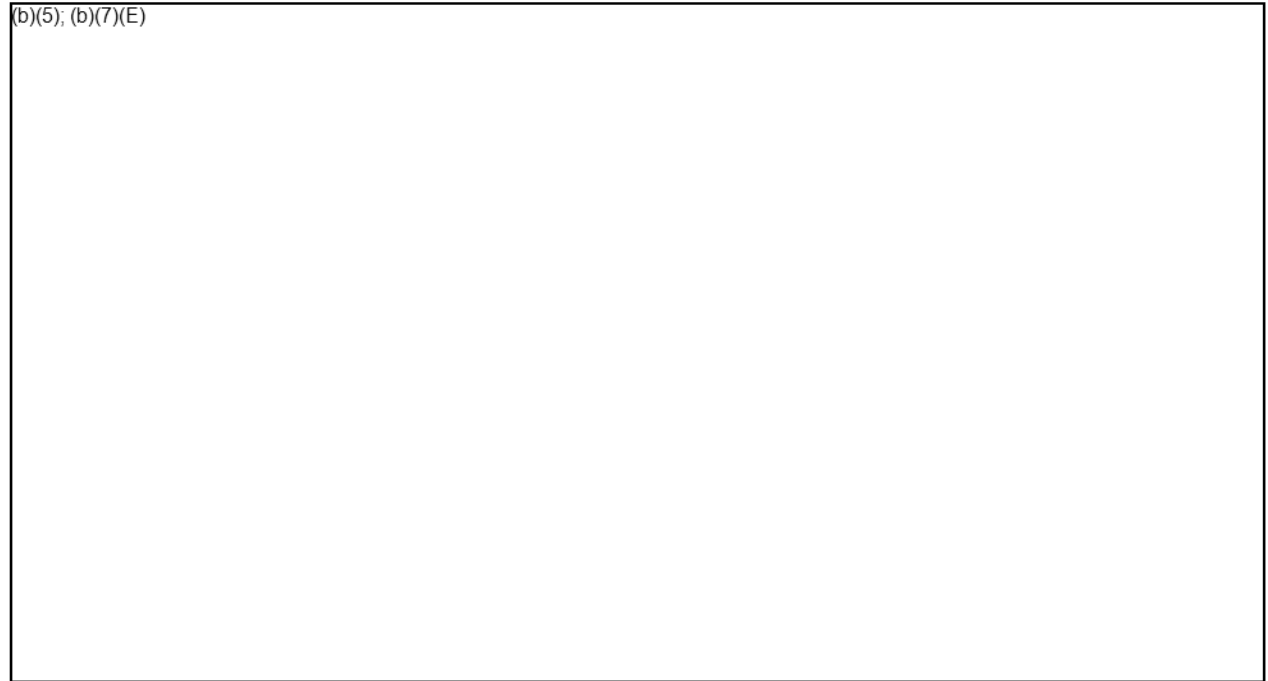
May nullify the Fourth Amendment warrant requirement when the needs of law enforcement are so compelling that it renders a warrantless search objectively reasonable.



Cell-Site Simulator Policy

Exigent Circumstances (cont.)

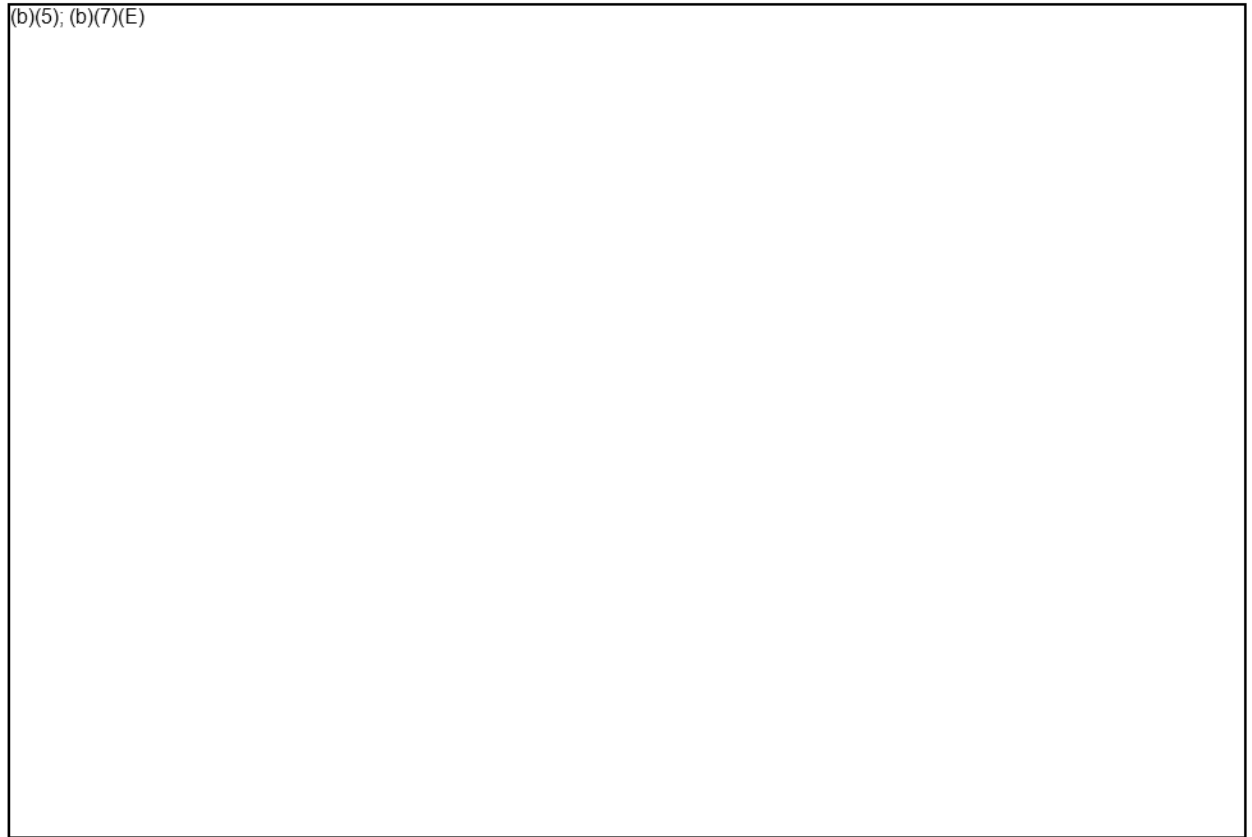
(b)(5); (b)(7)(E)



Cell-Site Simulator Policy

Exigent Circumstances (cont.)

(b)(5); (b)(7)(E)



Cell-Site Simulator Policy

Exceptional Circumstances

(b)(5); (b)(7)(E)



Cell-Site Simulator Review

Always need a warrant with requisite probable cause!

§ *Unless an **exigent circumstance** exists; or*

§ *Unless an **exceptional circumstance** exists.*



Applications for Use of Cell-Site Simulators

(b)(5); (b)(7)(E)

-

-

-



Information to be included in Application

- Application or supporting affidavit for use of cell-site simulator should:

(b)(5); (b)(7)(E)

§

§

§



Data Collection and Disposal

- Data collected through the use of a cell cite simulator must be handled in the same manner, consistent with applicable existing laws and requirements, including duty to preserve exculpatory evidence.

(b)(5); (b)(7)(E)

§

§

§

§



Additional Notes

- State and Local Partners

(b)(5); (b)(7)(E)

- Improper Use of Cell-Site Simulators
- This policy is guidance and is not intended to and does not create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law or equity, by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial or any other proceeding.



Quiz

- (b)(5); (b)(7)(E)



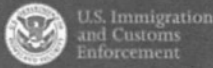
Questions?

OPLA-CLS@ice.dhs.gov

ICE

Electronic Communications Privacy Act

- **Title I of ECPA** – Wiretap Act
- **Title II of ECPA** – Stored Communications Act
- **Title III of ECPA** – Pen register and trap and trace devices



ECPA is made up of three titles. We will discuss these in more detail in the next. CALIFORNIA RECENTLY PASSED ITS OWN VERSION THAT HAS SOME UNIQUE DIFFERENCES. WE'VE ASKED (b)(6); (b)(7)(C) TO DISCUSS THESE AFTER WE FINISH ADDRESSING CURRENT FEDERAL LAW.

Title I - prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title I also prohibits the use of illegally obtained communications as evidence. 18 U.S.C. § 2515.

Title II – Stored Communications Act protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses. 18 U.S.C. §§ 2701-12.

Title III - Addresses pen register and trap and trace devices, requires government entities to obtain a court order authorizing the installation and use of a pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap

and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated). No actual communications are intercepted by a pen register or trap and trace. The authorization order can be issued on the basis of certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the applicant's agency.

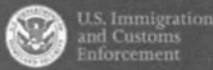
The Communications Assistance to Law Enforcement Act (CALEA) amended ECPA in 2004. CALEA sets out obligations of telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization. The FBI is responsible for implementing CALEA.

- Note – there is some discussion of amending CALEA to address recent cell phone encryption concerns.

ICE

Title III – Pen Register and Trap and Trace Devices

- Obtain the pen register records from the appropriate phone company to identify which numbers are being called by the target telephone, how often they are called, and for what duration.
- Under the USA Patriot Act, the legal threshold for obtaining these records was lowered to a demonstration that the records are relevant to an ongoing criminal investigation.



This is found in USA Patriot Act sections 214-216.

Pen register = device or process that records or decodes dialing, routing, addressing or signaling information transmitted by a communication instrument or facility; does not include content, which is governed by Title III. 18 USC 3127(3)

Trap and trace device = device or process that captures the incoming electronic impulses, which identify the source of the communication (originating number or other dialing, routing, addressing or signaling information); does not include content, which is governed by Title III. 18 USC 3127(4).

ICE requests installation or use of pen registers or trap and trace devices through a court order; the standard for obtaining the order is that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency. 18 USC 3122.

ICE

Cell Phone Location Data

- Historical Cell-Site Information
- Prospective Cell Phone Location Information
 - Cell-Site
 - E911
- Stingray/Trigger Fish Devices/
International Mobile Subscriber Identity
(IMSI) Catchers



U.S. Immigration
and Customs
Enforcement

- Historical Cell-Site Location Information
 - 18 USC 1703(d) orders generally can be used to obtain cell-site records, however there is much litigation surrounding this (especially bulk historical data collection in light of *Jones*).
 - The Fourth Circuit now joins the Fifth, Sixth, and Eleventh Circuits in holding that no Fourth Amendment protection exists for cell site records under the third party doctrine.

***U.S. v. Graham*, No. 12-4659 (4th Cir. May 31, 2016) (en banc)**

The Fourth Circuit issued an en banc decision on the U.S. government's petition, finding that no warrant is required for law enforcement to obtain historical cell-site location information (CSLI) from carriers. This decision eliminates the circuit split created in the initial Fourth Circuit panel decision. *U.S. v. Graham*, 796 F.3d 332 (4th Cir. 2015). In the panel decision, the Fourth Circuit held that the government had violated defendants' rights when it obtained historical CSLI for an extended period of time without a warrant. The panel cited to the Justice Sotomayor concurrence in *U.S. v. Jones* for the conclusion that long-term location information disclosed in cell phone records can reveal a significant

comprehensive view of an individual's daily life. 132 S.Ct. 945, 955 (2012). Although the court refused to declare a bright line rule for what is too long a time period, it determined that the 14 days of CSLI in this case was too long. The court nevertheless determined that the government acted in good faith in obtaining the historical CSLI without a warrant and affirmed the convictions of Defendants Aaron Graham and Eric Jordan arising from their participation in a series of armed robberies.

The en banc opinion disagreed with the 2015 panel decision, concluding that the government's acquisition of historical CSLI from defendants' cell phone provider did not violate the Fourth Amendment.

Supreme Court precedent mandates this conclusion. For the Court has long held that an individual enjoys no Fourth Amendment protection "in information he voluntarily turns over to [a] third part[y]." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). This rule -- the third-party doctrine -- applies even when "the information is revealed" to a third party, as it assertedly was here, "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976). All of our sister circuits to have considered the question have held, as we do today, that the government does not violate the Fourth Amendment when it obtains historical CSLI from a service provider without a warrant. In addition to disregarding precedent, Defendants' contrary arguments misunderstand the nature of CSLI, improperly attempt to redefine the third-party doctrine, and blur the critical distinction between content and non-content information.

The Supreme Court may in the future limit, or even eliminate, the third-party doctrine. Congress may act to require a warrant for CSLI. But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case.

Although the en banc opinion acknowledges the defendants' analogy to government location tracking, it determines that "it is premature to equate CSLI with the surveillance information obtained in...*Jones*" because CSLI can only determine a four-square-mile area within which a person used his or her cell phone, and CSLI does not allow the government to "place an individual" at home or other private locations. (n. 3)

- Prospective Cell Phone Location Information
 - Prospective cell-site information identifies the tower (and in most cases the sector of the cell tower) used to route communications to or from the target phone. Taken together with the location of the relevant cell towers, these

records permit investigators to determine the general area in which the target phone is located at the time that a communication occurs.

- DOJ believes that prospective cell-site information can be properly obtained with a hybrid order, which is based on the combined authority of Section 2703(d) of the Stored Communications Act and the Pen/Trap Statute. Some judges, however, have refused to sign hybrid orders for prospective cell-site information and have required the use of a search warrant.
- E911 data provides more precise information, in the form of geographic coordinates, about the location of a target phone. Significantly, while all providers can supply prospective cell-phone location information, some providers (e.g. Verizon) lack the ability to produce prospective E911 location information to law enforcement even when served with a search warrant.
 - DOJ recommends that law enforcement always utilize a search warrant when seeking to compel a provider to produce E911 location information.

•Stingray/Trigger Fish/IMSI Catchers

(b) (7)(E)



Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

December 27, 2018

December 21, 2018-December 27, 2018

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

December 31, 2018

December 28, 2018-December 31, 2018

Target Located

Arrests

(b)(7)(E)

U.S. Department of Homeland Security
500 12th Street, SW
Washington, D.C. 20536



U.S. Immigration
and Customs
Enforcement

AUG 31 2017

MEMORANDUM FOR: Assistant Directors
Deputy Assistant Directors
Special Agents in Charge
Attachés

FROM:

 Derek N. Benner 
Acting Executive Associate Director

SUBJECT:

Use of Cell-Site Simulator Technology

Purpose:

(b)(7)(E)

Background:

(b)(7)(E)



Management Controls and Accountability

(b)(7)(E)



(b)(7)(E)



Legal Process and Court Orders

(b)(7)(E)



(b)(7)(E)



(b)(7)(E)



~~LAW ENFORCEMENT SENSITIVE~~

Applications for Use of Cell-Site Simulators

(b)(7)(E)



(b)(7)(E)



~~LAW ENFORCEMENT SENSITIVE~~

Data Collection, Recordkeeping, and Disposal

(b)(7)(E)



State and Local Partners

(b)(7)(E)



Coordination and Ongoing Management

(b)(7)(E)

Improper Use of Cell-Site Simulators

Accountability is an essential element in maintaining the integrity of HSI. Allegations of violations of any orders that implement this policy, as with other allegations of misconduct, will be referred to the Joint Intake Center and/or the ICE Office of Professional Responsibility.

No Private Right

This policy guidance is not intended to and does not create any right, benefit, trust or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial, or any other proceeding.

(b)(7)(E)



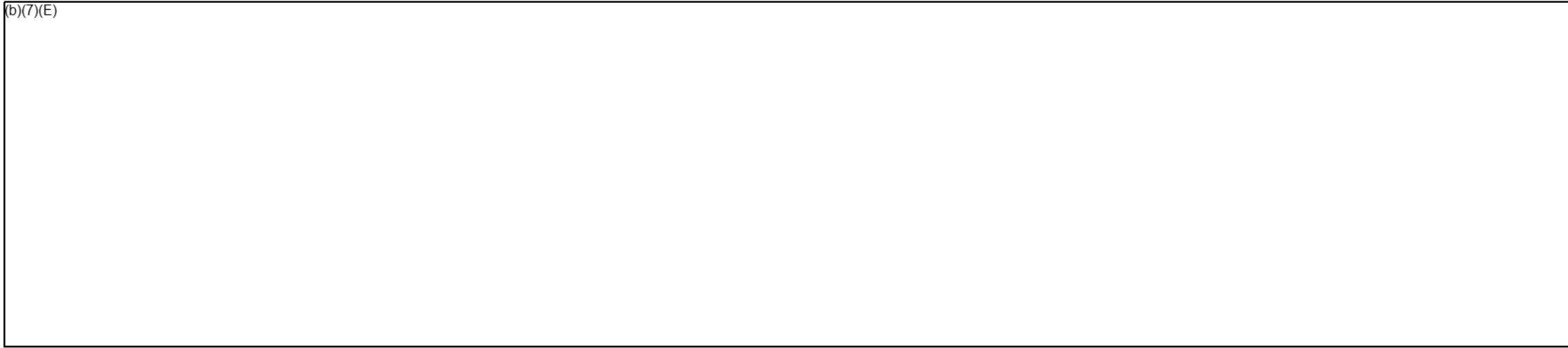
HSI

POLICY GUIDANCE REGARDING THE USE OF CELL-SITE SIMULATOR TECHNOLOGY



Basic Uses

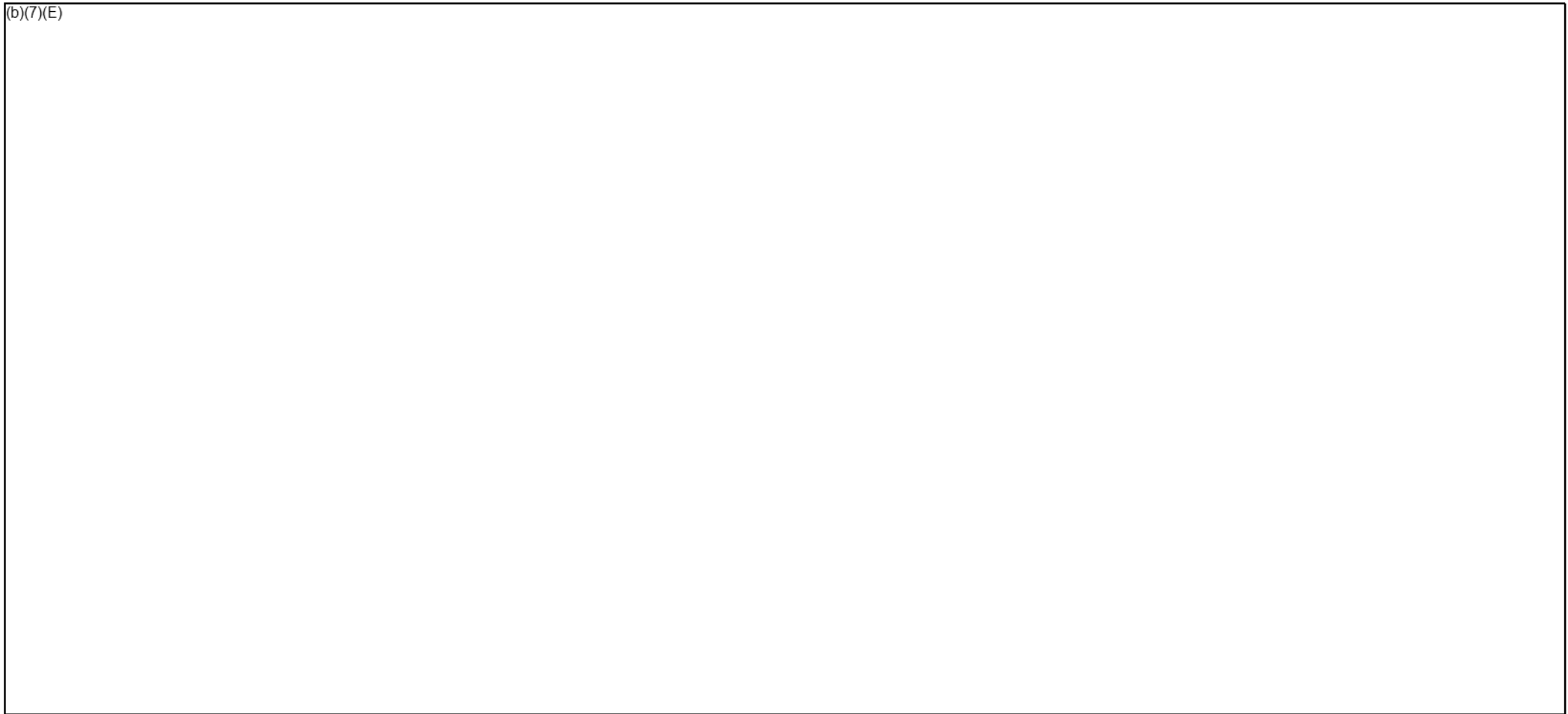
(b)(7)(E)





How They Function

(b)(7)(E)





How They Function

(b)(7)(E)



How They Function

(b)(7)(E)





HSI Cell-Site Simulators Obtain...

(b)(7)(E)



HSI Cell-Site Simulators DO NOT....

(b)(7)(E)



PEN Register Configuration

(b)(7)(E)



Management and Accountability

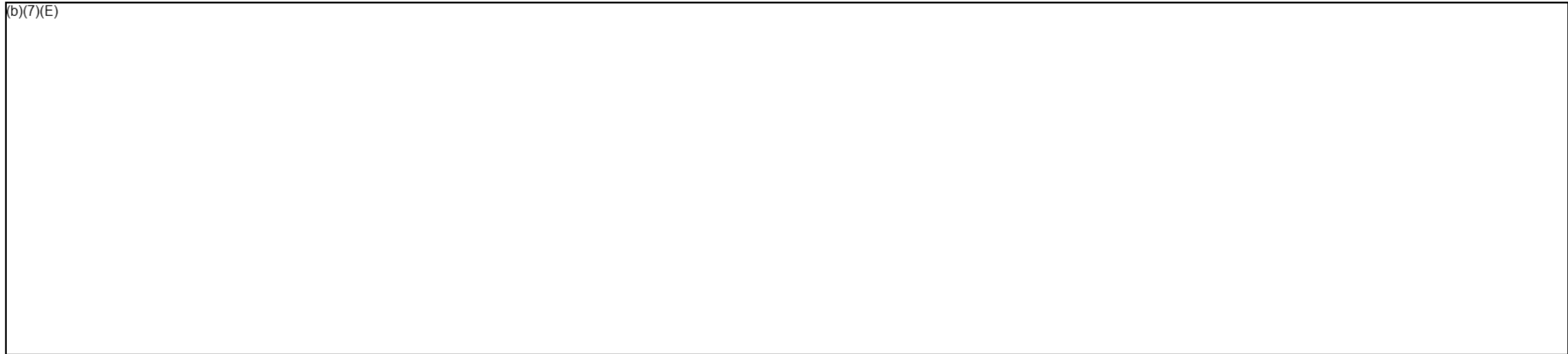
(b)(7)(E)





Legal Process

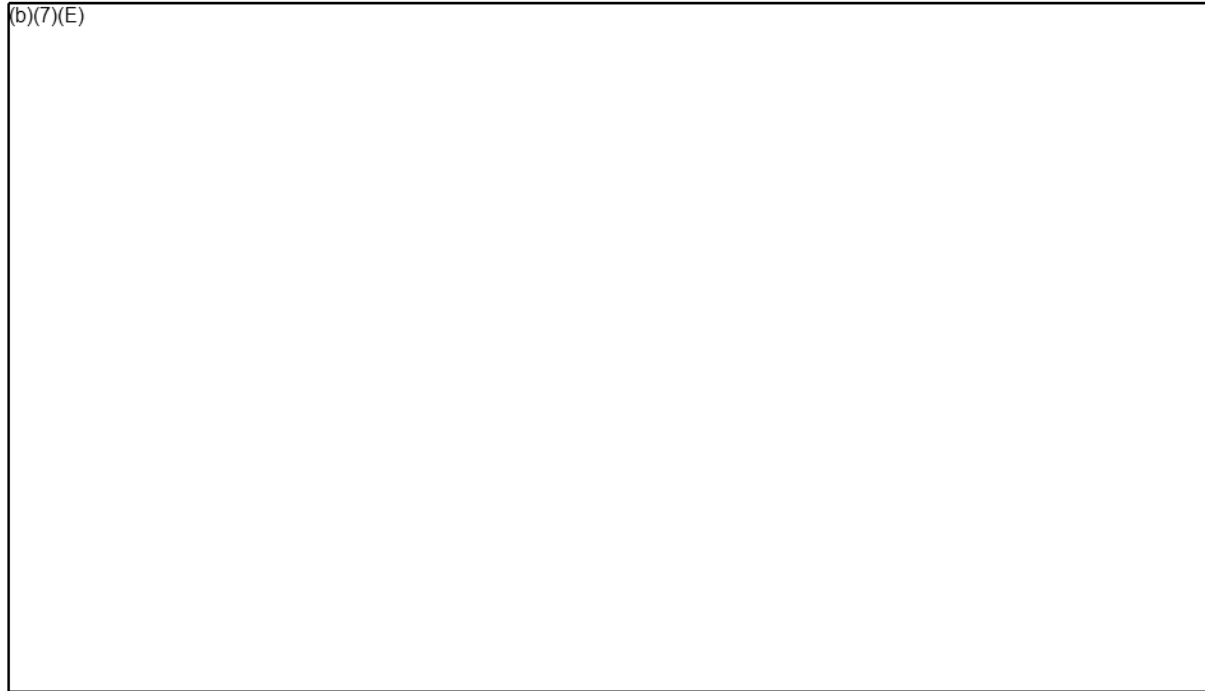
(b)(7)(E)





Legal Process

(b)(7)(E)



4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.



Legal Process

(b)(7)(E)



Exigent Circumstances under the Fourth Amendment

(b)(7)(E)



Exigent Circumstances under the Fourth Amendment

(b)(7)(E)



Applications for Use of Cell-Site Simulators

(b)(7)(E)



Applications for Use of Cell-Site Simulators

(b)(7)(E)



Applications for Use of Cell-Site Simulators

(b)(7)(E)



Applications for Use of Cell-Site Simulators

(b)(7)(E)



Data Collection & Disposal

(b)(7)(E)



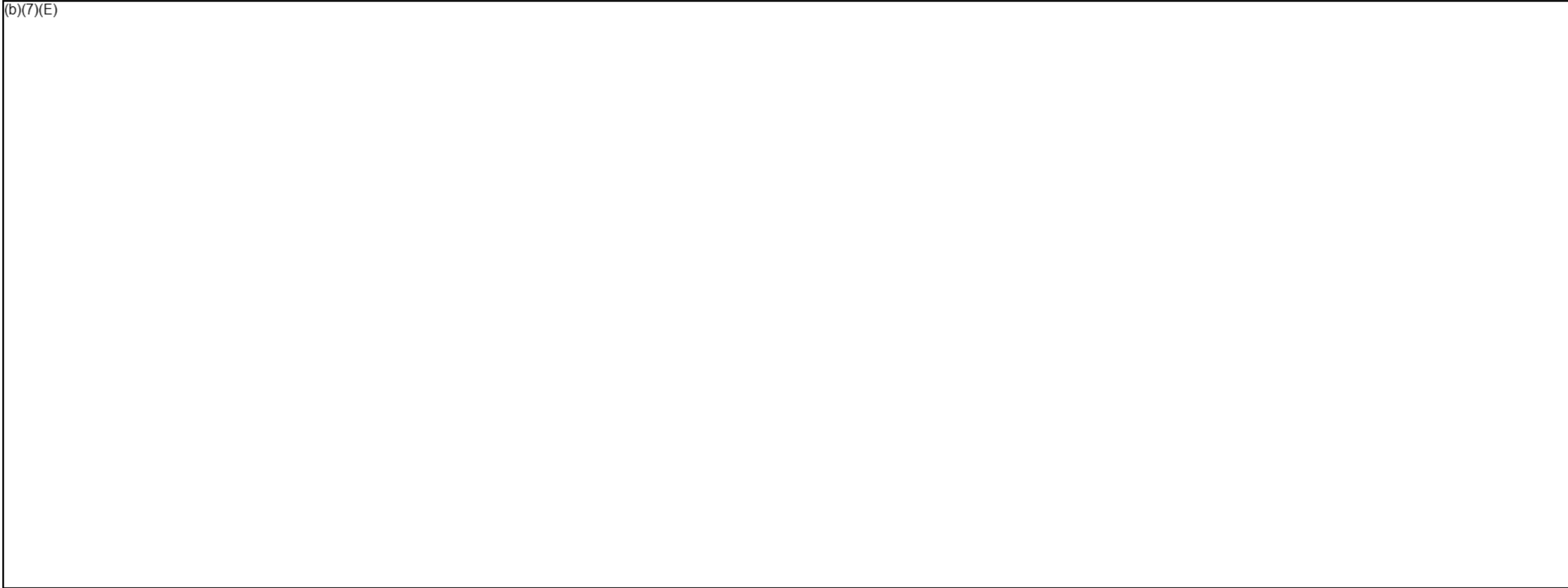
Auditing

(b)(7)(E)



Auditing

(b)(7)(E)





State and Local Partners

(b)(7)(E)



Training and Coordination

(b)(7)(E)



Improper Use of Cell-Site Simulators

Accountability is an essential element in maintaining the integrity of HSI. Allegations of violations of any orders that implement this policy, as with other allegations of misconduct, will be referred to the Joint Intake Center and/or the ICE Office of Professional Responsibility.



Questions

For questions pertaining to the HSI Cell-Site Simulator Program, Please contact the Technical Operations Unit (TechOps)

(b)(7)(E)



Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

January 3, 2019

January 1, 2019 -January 3, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

January 10, 2019

January 4, 2019 - January 10, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

January 15, 2019

January 11, 2019 -January 15, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

January 24, 2019

January 16, 2019 -January 24, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

January 31, 2019

January 24, 2019 -January 31, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

February 7, 2019

February 1, 2019, -February 7, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

February 14, 2019

February 8, 2019, -February 14, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

February 21, 2019

February 15, 2019, -February 21, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

February 28, 2019

February 22, 2019, -February 28, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

March 7, 2019

March 1, -March 7, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
March 14, 2019

March 8, -March 14, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
March 21, 2019

March 15, -March 21, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

March 28, 2019

March 22, -March 28, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -April

4, 2019

March 29, -April 4, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -April

11, 2019

April 5, -April 11, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -April
17, 2019

April 12, -April 17, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -April
25, 2019

April 18, -April 25, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 - May
2, 2019

April 26, -May 2, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -May
9, 2019

May 3, -May 9, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -May
15, 2019

May 10, -May 15, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -May
23, 2019

May 16, -May 23, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -May
30, 2019

May 24, -May 30, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -June

6, 2019

May 31, -June 6, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 - June
12, 2019

June 7, -June 12, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -June
20, 2019

June 13, -June 20, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -June

26, 2019

June 21, -June 26, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 - July
5, 2019

June 27, -July 5, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -July
11, 2019

July 6, -July 11, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -July
18, 2019

July 12, -July 18, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -July
25, 2019

July 19, -July 25, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
August 1, 2019

July 26, -August 1, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

August 7, 2019

August 2, -August 7, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
August 15, 2019

August 8, -August 15, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
August 22, 2019

August 16, -August 22, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

August 28, 2019

August 23, -August 28, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
September 5, 2019

August 29, -September 5, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
September 12, 2019

September 6, -September 12, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -
September 20, 2019

September 13, -September 20, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

September 26, 2019

September 21, -September 26, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

October 3, 2019

September 27, -October 3, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: January 1, 2019 -

October 4, 2019

October 4, -October 7, 2019

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

November 1, 2018

October 26, 2018-November 1, 2018

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

November 15, 2018

November 9, 2018-November 15, 2018

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

November 15, 2018

November 9, 2018-November 15, 2018

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

November 21, 2018

November 16, 2018-November 21, 2018

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

November 29, 2018

November 22, 2018-November 29, 2018

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

December 6, 2018

November 30, 2018-December 6, 2018

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

December 13, 2018

December 7, 2018-December 13, 2018

Target Located

Arrests

(b)(7)(E)

Technical Operations CSS Weekly Report

CSS Activity: March 1, 2018 -

December 20, 2018

December 14, 2018-December 20, 2018

Target Located

Arrests

(b)(7)(E)

From:

(b)(6); (b)(7)(C)

Sent:

2 Apr 2013 11:47:54 -0400

To:

(b)(6); (b)(7)(C)

Cc:

(b)(6); (b)(7)(C)

Subject:

RE: Stingray/Portable Cell Tower Technology

(b)(6);
(b)(7)(C)

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(5); (b)(7)(E)

Regards

(b)(6); (b)(7)(C)

*Unit Chief
Technical Operations
Homeland Security Investigations
Immigration & Customs Enforcement
Department of Homeland Security
Desk: (703) 551-(b)(6);
Cell: (571) 245-(b)(7)(C)*
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)

Sent: Tuesday, April 02, 2013 10:54 AM

To: (b)(6); (b)(7)(C)

Cc:

Subject: RE: Stingray/Portable Cell Tower Technology

Thanks (b)(6). If I could get a briefing sometime in the next couple of weeks on this, I would appreciate it. Happy to head down to TechOps if that's easier. Just let me know.

(b)(6):

Privacy Officer
Assistant Director for Privacy & Records
U.S. Immigration & Customs Enforcement
Direct: (202) 732-(b)(6);
Main: (202) 732-(b)(7)(C)

Questions? Please visit the Privacy & Records Office website at <http://intranet.ice.dhs.gov/sites/ooop/>.

From: (b)(6); (b)(7)(C)

Sent: Monday, April 01, 2013 5:57 PM

To: (b)(6); (b)(7)(C)

Cc:

Subject: RE: Stingray/Portable Cell Tower Technology

(b)(6);

I have copied in TechOps Unit Chief (b)(6); (b)(7)(C) as the Stingray program for HSI is under his shop with devices dispersed throughout the US (b)(6); can provide you with a briefing and information on the HSI program managed by TechOps.

(b)(5); (b)(7)(E)

Thanks

(b)(6); (b)(7)(C)

Deputy Assistant Director
Law Enforcement Support & Information Management (LESIM)
Homeland Security Investigations (HSI)
Immigration and Customs Enforcement (ICE)
Department of Homeland Security (DHS)
(202) 732-(b)(6);

(b)(6); (b)(7)(C)

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

From: (b)(6); (b)(7)(C)

Sent: Monday, April 01, 2013 5:42 PM

To: (b)(6); (b)(7)(C)

Subject: FW: Stingray/Portable Cell Tower Technology

Importance: High

Let's talk...

(b)(6);

Privacy Officer

Assistant Director for Privacy & Records

U.S. Immigration & Customs Enforcement

Direct: (202) 732-(b)(6);

Main: (202) 732-(b)(7)(C)

Questions? Please visit the Privacy & Records Office website at <http://intranet.ice.dhs.gov/sites/ooop/>.

From: (b)(6); (b)(7)(C)

Sent: Monday, April 01, 2013 2:42 PM

To: (b)(6); (b)(7)(C)

Cc:

Subject: Stingray/Portable Cell Tower Technology

Importance: High

(b)(6);
(b)(7)(C)

(b)(5); (b)(7)(E)

- 1) **Slate: FBI Files Unlock History Behind Clandestine Cellphone Tracking Tool**
http://www.slate.com/blogs/future_tense/2013/02/15/stingray_imsi_catcher_fbi_files_unlock_history_behind_cellphone_tracking.html
- 2) **Wall Street Journal: 'Stingray' Phone Tracker Fuels Constitutional Clash**
<http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html>
- 3) **The Washington Post: Little-known surveillance tool raises concerns by judges, privacy activists**
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

(b)(5); (b)(7)(E)

I'm out on Tuesday, April 2, 2013, but am free this afternoon and much of the remainder of this week if you need to chat.

Best wishes,

(b)(6);
(b)(7)(C)

(b)(6); (b)(7)(C)

M.S., J.D., CIPP/US/G
Directorate Privacy Officer | Science & Technology Directorate | Department of Homeland Security
202-254-(b)(6) Office | 202-527-(b)(6) Blackberry (b)(6); (b)(7)(C) @hq.dhs.gov

From: (b)(6); (b)(7)(C)
To:
Cc:
Subject: HSI Policy-Use of Over-The-Air Wireless (cellular) Tracking Equipment
Date: Monday, January 12, 2015 1:23:29 PM

(b)(6);
(b)(7)(C)

(b)(6);
(b)(7)(C) advised you were requesting HSI policy information. See below HSI policy for the use of Use of Over-The-Air Wireless (Cellular) Tracking Equipment. HSI HB14-04 Technical Operations Handbook dated 07/21/2014.

16.1 Use of Over-The-Air Wireless (Cellular) Tracking Equipment

(b)(5); (b)(7)(E)

Please let me know if you require additional information.

(b)(6); (b)(7)(C)

Section Chief
Investigative Intercept Section
Technical Operations
ICE-Homeland Security Investigations
U.S. Department of Homeland Security
Lorton, VA
703-551-(b)(6); Desk
703-599-(b)(7)(C) Cell

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

From: (b)(6); (b)(7)(C) (CTR)
Sent: 12 Jan 2015 14:23:31 -0500
To: (b)(6); (b)(7)(C)
Subject: RE: HSI Policy-Use of Over-The-Air Wireless (cellular) Tracking Equipment

(b)(5); (b)(7)(E)

(b)(6); (b)(7)(C) (CTR)
AGS, Inc.
Privacy Compliance Specialist
In support of the ICE Privacy Office
U.S. Immigration and Customs Enforcement

Direct: 202-732-(b)(6);
Main: 202-732-(b)(7)(C)

For help with privacy questions, please visit the ICE Intranet at

<https://insight.ice.dhs.gov/mgt/oop/>

From: (b)(6); (b)(7)(C)
Sent: Monday, January 12, 2015 2:21 PM
To: (b)(6); (b)(7)(C) (CTR); (b)(6); (b)(7)(C)
Subject: RE: HSI Policy-Use of Over-The-Air Wireless (cellular) Tracking Equipment

Get the language from them on this too: are required to submit reports in accordance with Section 19.4 of this Handbook

(b)(6);
Privacy Officer
Assistant Director for Privacy & Records
U.S. Immigration & Customs Enforcement
Direct: (202) 732-(b)(6);
Main: (202) 732-(b)(7)(C)

Questions? Please visit the Privacy & Records Office website at <https://insight.ice.dhs.gov/mgt/oop/Pages/index.aspx>.

From: (b)(6); (b)(7)(C) (CTR)
Sent: Monday, January 12, 2015 1:35 PM
To: (b)(6); (b)(7)(C)
Subject: FW: HSI Policy-Use of Over-The-Air Wireless (cellular) Tracking Equipment

FYI

(b)(6); (b)(7)(C) (CTR)
AGS, Inc.
Privacy Compliance Specialist
In support of the ICE Privacy Office
U.S. Immigration and Customs Enforcement

Direct: 202-732-(b)(6);
Main: 202-732-(b)(7)(C)

For help with privacy questions, please visit the ICE Intranet at <https://insight.ice.dhs.gov/mgt/oop/>

From: (b)(6);
Sent: Monday, January 12, 2015 1:23 PM
To: (b)(6); (b)(7)(C) (CTR)
Cc: (b)(6); (b)(7)(C)
Subject: HSI Policy-Use of Over-The-Air Wireless (cellular) Tracking Equipment

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) advised you were requesting HSI policy information. See below HSI policy for the use of Use of Over-The-Air Wireless (Cellular) Tracking Equipment. HSI HB14-04 Technical Operations Handbook dated 07/21/2014.

(b)(5); (b)(7)(E)

Please let me know if you require additional information.

(b)(6); (b)(7)(C)

Section Chief
Investigative Intercept Section
Technical Operations
ICE-Homeland Security Investigations
U.S. Department of Homeland Security
Lorton, VA
703-551-(b)(6) Desk
703-599-(b)(7) Cell

~~Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.~~

From: (b)(6); (b)(7)(C) (CTR)
Sent: 31 Jan 2019 17:32:00 +0000
To: (b)(6); (b)(7)(C)
Subject: Surveillance Technologies PIA
Attachments: HSI Surveillance Technologies PIA TechOps Draft (01 31 19).docx

H (b)(6);

Attached please find a draft of the Surveillance Technologies PIA for your review.

Please let me know if I can provide any additional information.

Best,

(b)(6);
(b)(7)(C)

(b)(6);
(b)(7)(C)

Supporting the Office of Information Governance & Privacy
U.S. Immigration and Customs Enforcement

(b)(6); @associates.ice.dhs.gov

(Mobile) (b)(6); (b)(7)(C)



Privacy Impact Assessment
for the

Homeland Security Investigation (HSI) Surveillance Technologies

DHS/ICE/PIA-048

January 31, 2019

Contact Point

Derek N. Benner

Executive Associate Director

Homeland Security Investigations

U.S. Immigration and Customs Enforcement

**(202) 732-(b)(6);
(b)(7)(C)**

Reviewing Official

Philip S. Kaplan

Chief Privacy Officer

Department of Homeland Security

**(202)343-(b)(6);
(b)(7)(C)**

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



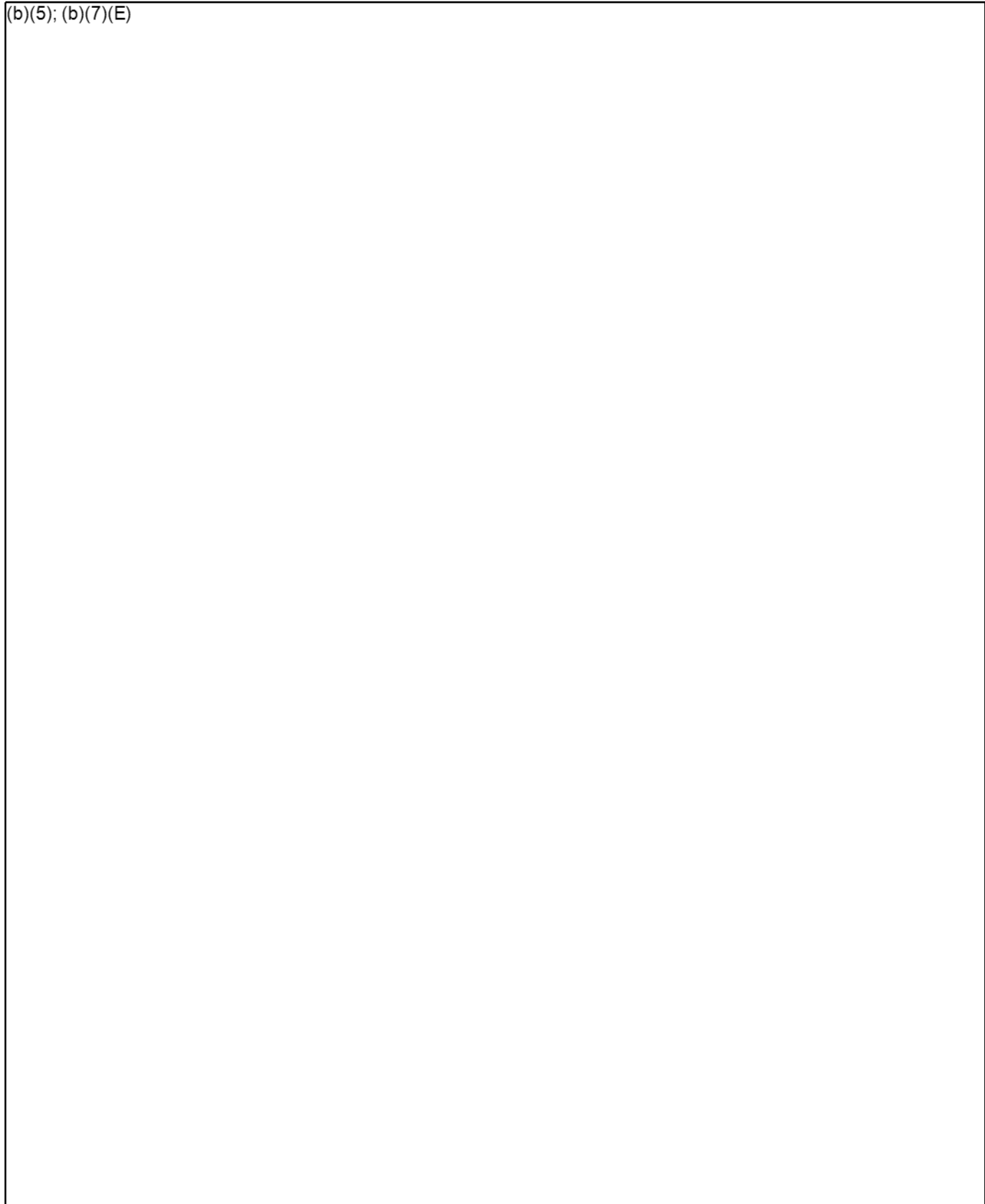
(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

FOR OFFICIAL USE ONLY (FOUO)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

Responsible Officials

Program Manager:

Approval Signature Page

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

(b)(5); (b)(7)(E)



U.S. Immigration
and Customs
Enforcement

February 16, 2017

MEMORANDUM FOR Derek Benner
 Deputy Executive Associate Director
 Homeland Security Investigations

FROM: Lyn Rahilly
 Assistant Director

SUBJECT: Comments on HSI Policy Use of Cell-Site Simulator Technology

Thank you for the opportunity to review this draft policy. As use of this technology has been the focus of much attention in the media and from Congress, I recommend (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

Training Requirements

I recommend (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

I also recommend (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

Recordkeeping

I recommend (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

When responding to a letter on cell-site simulators from several (b)(7)(E)
DHS provided information about how the surveillance outcomes are documented within HSI.
The DHS response is below:

Q. How long is the collected information retained? How is this information disposed of, and what timeframe is your agency using to dispose of information collected by such devices?

(b)(5); (b)(7)(E)

See (b)(7)(E) final, p.9.

Assuming it is still accurate, I recommend (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

cc: Scott Lanum, Assistant Director, ODCR
Debbie Seguin, Assistant Director, Policy

¹ This recommendation (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

From: (b)(6); (b)(7)(C) (CTR)
Sent: 8 Nov 2018 14:15:30 +0000
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C) (CTR)
Subject: RE: ICE HSI Cell Site Simulator Log PTA

Thanks (b)(6);

I will work with (b)(6); to update the (b)(7)(E) to include the information regarding the Cell Site Simulators. We are currently waiting for an updated Draft from the Program Office.

Thanks,
(b)(6);

From: (b)(6);
Sent: Thursday, November 8, 2018 8:41 AM
To: (b)(6); (b)(7)(C) @ice.dhs.gov > (b)(6); (b)(7)(C) (CTR)
<(b)(6); (b)(7)(C) @associates.ice.dhs.gov >
Cc: (b)(6); (b)(7)(C) @ice.dhs.gov >; (b)(6); (b)(7)(C) (CTR)
(b)(6); @associates.ice.dhs.gov >
Subject: RE: ICE HSI Cell Site Simulator Log PTA

Thanks (b)(6);
(b)(7)(C)

If possible I would rather keep everything in one PTA than to write separate ones.

(b)(6) - would you be able to work with (b)(6); to update the (b)(7)(E) to include information regarding Cell Site Simulators?

Regarding PIA coverage, I know that (b)(6); is currently working on updating the (b)(7)(E) PIA, so this might be something we need to address. I've also copied (b)(6); since he'll be writing a PIA on (b)(7)(E) (b)(7)(E) generally, which might be a better fit.

Let's get the bulk of the PTA done first, and then we can determine where PIA coverage should fall.

(b)(6); (b)(7)(C)
Deputy Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732-(b)(6);
Mobile: 202-70-(b)(6);
Main: 202-732-(b)(6);

Questions? Please visit our website at <https://insight.ice.dhs.gov/mgt/igp/privacy/Pages/index.aspx>

From: (b)(6); (b)(7)(C)
Sent: Thursday, November 8, 2018 8:35 AM

To: (b)(6); (b)(7)(C) @ice.dhs.gov; (b)(6); (b)(7)(C) (CTR)
(b)(6); (b)(7)(C) @associates.ice.dhs.gov>

Subject: FW: ICE HSI Cell Site Simulator Log PTA

Importance: High

H (b)(6);

I received the email below (and a screen shot attached) from the PM, (b)(6); for the Cell Site Simulator Log – he says that their program was told by someone here in ICE Privacy that because this is just the log of what action was taken (in a SharePoint site) ICE Privacy was going to include this log where the Cell Site Simulator is discussed in the existing (b)(7)(E) and a new PTA for the log is not needed.

From the shared drive, I see the (b)(7)(E) is currently under review for renewal by (b)(6); copied here.

(b)(5); (b)(6); (b)(7)(C)

From: (b)(6);

Sent: Wednesday, November 7, 2018 4:45 PM

To: (b)(6); (b)(7)(C) @ice.dhs.gov>

Subject: RE: ICE HSI Cell Site Simulator Log PTA

(b)(6);

I was under the impression that this was not required. My DA [redacted] spoke with someone in the privacy office several months ago and it was determined that we would either not need a PTA or it would be added under the [redacted]

Thanks,

[redacted]
[redacted]
Homeland Security Investigations
National Program Manager
Technical Enforcement Officer
703-551-[redacted] Desk
571-839-[redacted] Mobile
[redacted]@ICE.DHS.GOV

Technical Support: ICE Service Desk: (888) 34-[redacted]
VECADS Support: VECADS 24/7 Support Desk: (888) [redacted] or
[redacted]@ice.dhs.gov
CVN Support: Spectrum Support Desk: (703) 551-[redacted]@ice.dhs.gov

Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

From: [redacted]@ice.dhs.gov>
Date: Wednesday, Nov 07, 2018, 16:12
To: [redacted]@ice.dhs.gov>
Subject: ICE HSI Cell Site Simulator Log PTA

Hi [redacted]
I've recently joined ICE Privacy as a detailee from CBP Privacy to support them while they back-fill some of the vacancies left in their office. I know you were working with both [redacted] and [redacted] on this PTA, but neither are in this office at this time. I believe [redacted] has left, and [redacted] is out on training, returning in a month or so. I'm here until the end of the year, and was hoping to assist in closing out some of the backlog of PTAs. For this reason, [redacted], Acting Privacy Officer for [redacted] has assigned this PTA to me to see if we can move it up to DHS HQ Privacy (PRIV).

Attached is the latest email between you and [redacted] with the most recent version of the PTA. I'm not sure if you've had an opportunity to respond to [redacted] questions/comments, but before I dove too deep into this, I wanted to check with you to be sure we're working on the most recent version. Can

you please let me know where you are on this PTA, and send me the updated/edited version so I can review and assist you in getting this cleared through PRIV?

Thanks,

(b)(6);

(b)(6); (b)(7)(C)

Sr. Privacy Analyst (detailed to)
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement

202-394-(b)(6); Mobile

(b)(6); (b)(7)(C)@ice.dhs.gov

Questions? Please visit our website at <https://insight.ice.dhs.gov/mgt/igp/privacy/Pages/index.aspx>

From: (b)(6); (b)(7)(C)
Sent: 30 Dec 2014 15:43:05 -0500
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: PTA for Stingray

(b)(6); (b)(7)(C)

Understood and will do.

Please note that I have also copied (b)(6); (b)(7)(C) and (b)(6); (b)(7)(C) on your email so that they are aware of this request.

Have a Happy New year!

Regards.

(b)(6); (b)(7)(C)

Section Chief
Information Systems Security Office
Law Enforcement Support & Information Sharing (LESIM)
ICE/Homeland Security Investigations (HSI)
Department of Homeland Security (DHS)
Office: 202-732-(b)(6);
Mobile: 202-421-(b)(7)(C)
(b)(6); (b)(7)(C) @ice.dhs.gov

ISSO Support: HSI-LESIM-ISSO@ice.dhs.gov

~~Warning: This email and any attachments are UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. No portion of this email should be furnished to the media, either in written or verbal form. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.~~

From: (b)(6); (b)(7)(C)
Sent: Tuesday, December 30, 2014 3:36 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: PTA for Stingray

Hi (b)(6);

We received a letter from the Senate inquiring on privacy compliance for HSI's Stingray surveillance technology. We worked on the response last week with an agent named (b)(6); (b)(7)(C) down in (b)(7)(E) who was very helpful. It's clear the Senators were very interested in whether my office had conducted a privacy review of this technology, and we have not as it is not required under the law or DHS policy. In light of their concerns, however, we promised to do one.

What I suggest is (b)(5)
(b)(5); (b)(6); (b)(7)(C)

If you could have them send the PTA to my new deputy, (b)(6); (b)(7)(C) when it's done, that would be great.

(b)(6);
Privacy Officer
Assistant Director for Privacy & Records
U.S. Immigration & Customs Enforcement
Direct: (202) 732-(b)(6)
Main: (202) 732-(b)(6);

Questions? Please visit the Privacy & Records Office website at <https://insight.ice.dhs.gov/mgt/ooop/Pages/index.aspx>.

From: (b)(6); (b)(7)(C)
Sent: 17 Nov 2014 15:32:17 -0500
To: (b)(6); (b)(7)(C)
(ICE-HSI) (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: Stingrays Fox News

Many thanks!

From: (b)(6); (b)(7)(C)
Sent: Monday, November 17, 2014 3:32 PM
To: Edge, Peter T (b)(6); (b)(7)(C) (ICE-HSI);
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: Re: Stingrays Fox News

I agree.

(b)(6); (b)(7)(C)
Deputy Principal Legal Advisor
(305) 970 (b)(6) (cell)
(202) 732 (b)(6) (desk)

*** Warning *** Attorney/Client Privilege *** Attorney Work Product ***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

Sent from my BlackBerry Wireless Handheld

From: Edge, Peter T
Sent: Monday, November 17, 2014 03:27 PM
To: (b)(6); (b)(7)(C) (ICE-HSI);
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: Stingrays Fox News

(b)(5) is appropriate.

Peter T. Edge
Executive Associate Director
Homeland Security Investigations- ICE
202-732-(b)(6) office

From: (b)(6); (b)(7)(C)
Sent: Monday, November 17, 2014 3:24:03 PM
To: (b)(6); (b)(7)(C) Edge, Peter T.; (b)(6); (b)(7)(C) (ICE-HSI); (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: FW: Stingrays Fox News

Folks –

Fox News is asking us if we have a response to a FOIA'd document tweeted out by a senior ACLU member (see below) about the fact that ICE uses the "Harris Stingray II" system to listen in on phone conversations. The FOIA'd docs (which you'll have to look up on a non-work computer or mobile device since our system blocks the link below), is a redacted purchase order showing a contract from the ICE Office of Investigations dated Sept. 2010 for some of the related technology and devices. It looks like it was the ICE attaché office in Amman.

I've discussed with (b)(6) and our sense is (b)(5)

(b)(5)

HSI/OPLA/Privacy – do you feel differently?

Many thanks!

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) [mailto:(b)(6); (b)(7)(C)@FOXNEWS.COM]
Sent: Monday, November 17, 2014 2:42 PM
To: (b)(6); (b)(7)(C)
Subject: Stingrays

Hey (b)(6),

Can you look at p. 44 (see link below) and comment on ICE using Harris Stingray II system similar system US Marshalls story from WSJ Friday to listen in to phone conversations?

Thank you,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

tweeted at 6:11 PM on Thu, Nov 13, 2014:

The US Marshals aren't the only feds with phone spying gear strapped to airplanes. ICE does it too. <https://t.co/u07ySUqsUz>
(<https://twitter.com/csoghoian/status/533034551472586752?s=03>)

Stingray tracking system---

http://en.wikipedia.org/wiki/Stingray_phone_tracker

Homeland Security Investigations (HSI)

Basic Uses



(b)(7)(E)



U.S. Immigration
and Customs
Enforcement

How Cell-Site Simulators Function



(b)(7)(E)

•

•



Homeland Security Investigations (HSI)

How Cell-Site Simulators Function



(b)(7)(E)

•

•



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

HSI Cell-Site Simulators Usage



HSI Cell-Site Simulators may obtain:

- (b)(7)(E)
-



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

HSI Cell-Site Simulators Usage



HSI Cell-Site Simulators Do Not:

(b)(7)(E)

-
-
-



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

HSI Cell-Site Simulators Usage



(b)(7)(E)



U.S. Immigration
and Customs
Enforcement

~~Law Enforcement Sensitive~~

2020 ICL 00013-980

Management And Accountability



(b)(7)(E)

•

•



Homeland Security Investigations (HSI)

Management And Accountability



(b)(7)(E)

-
-



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

Legal Process



(b)(7)(E)



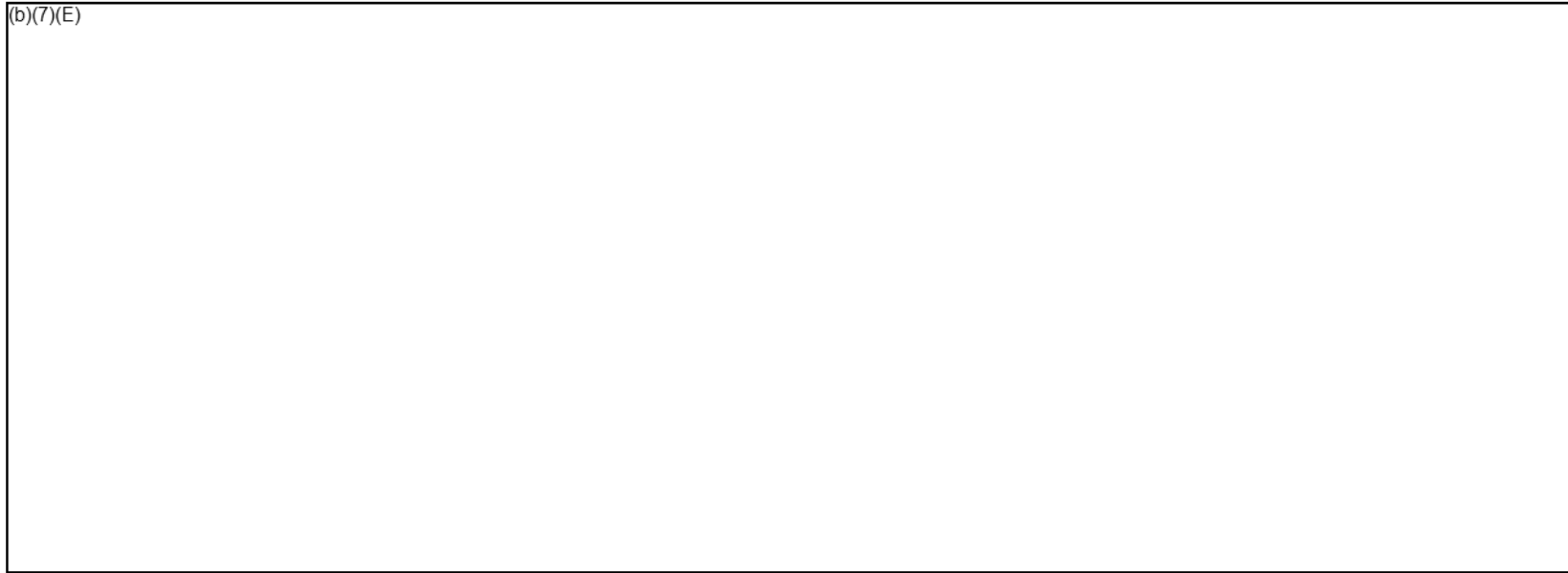
U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

Legal Process



(b)(7)(E)



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

Exigent Circumstances under the Fourth Amendment



(b)(7)(E)

-
-
-
-
-
-



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

Exigent Circumstances under the Fourth Amendment



(b)(7)(E)



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

Exigent Circumstances under the Fourth Amendment



(b)(7)(E)



U.S. Immigration
and Customs
Enforcement

~~Law Enforcement Sensitive~~

2020-ICL-00013-987

Homeland Security Investigations (HSI)



Applications for Use of Cell-Site Simulators

(b)(7)(E)

-
-
-
-



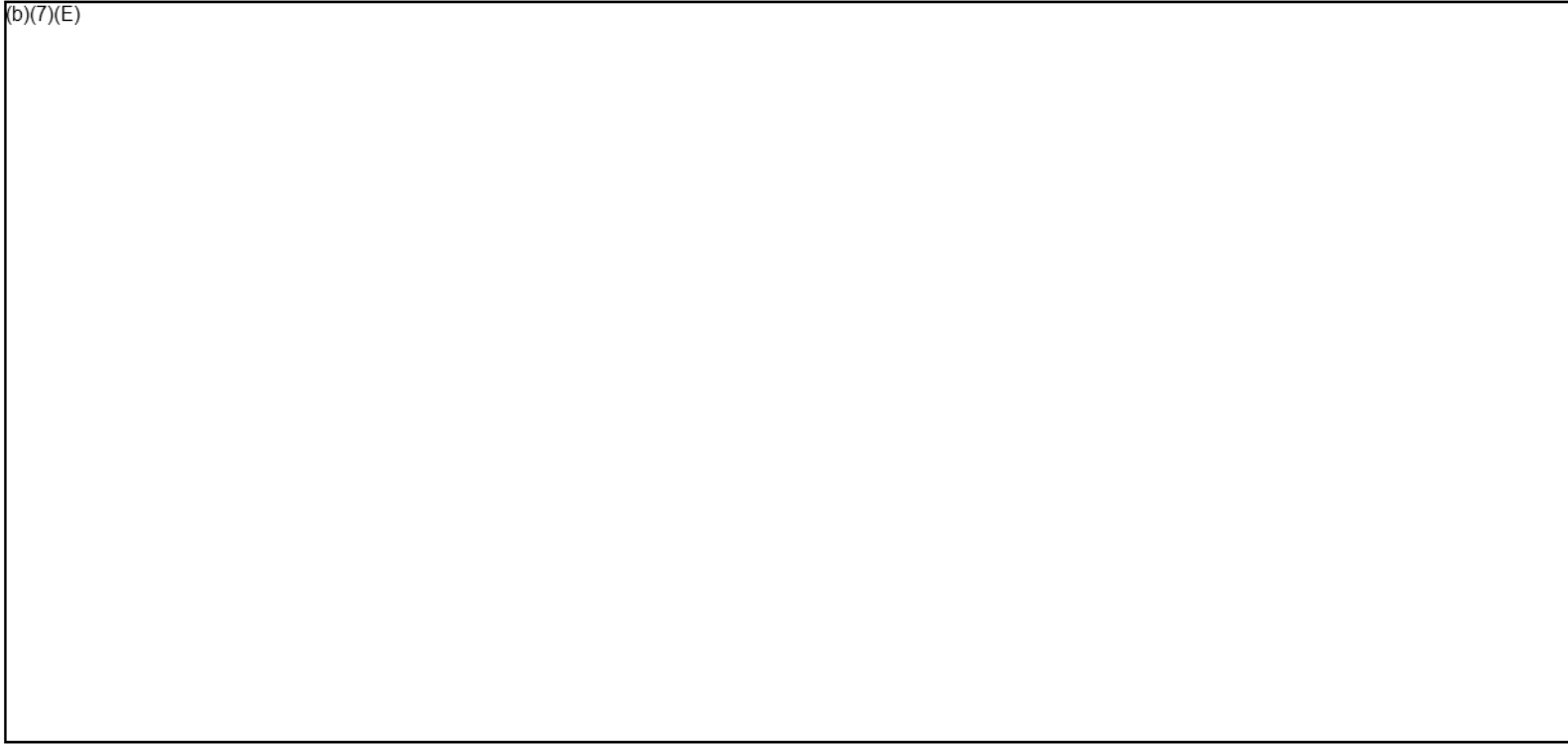
U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)



Applications for Use of Cell-Site Simulators

(b)(7)(E)



U.S. Immigration
and Customs
Enforcement

— Law Enforcement Sensitive —

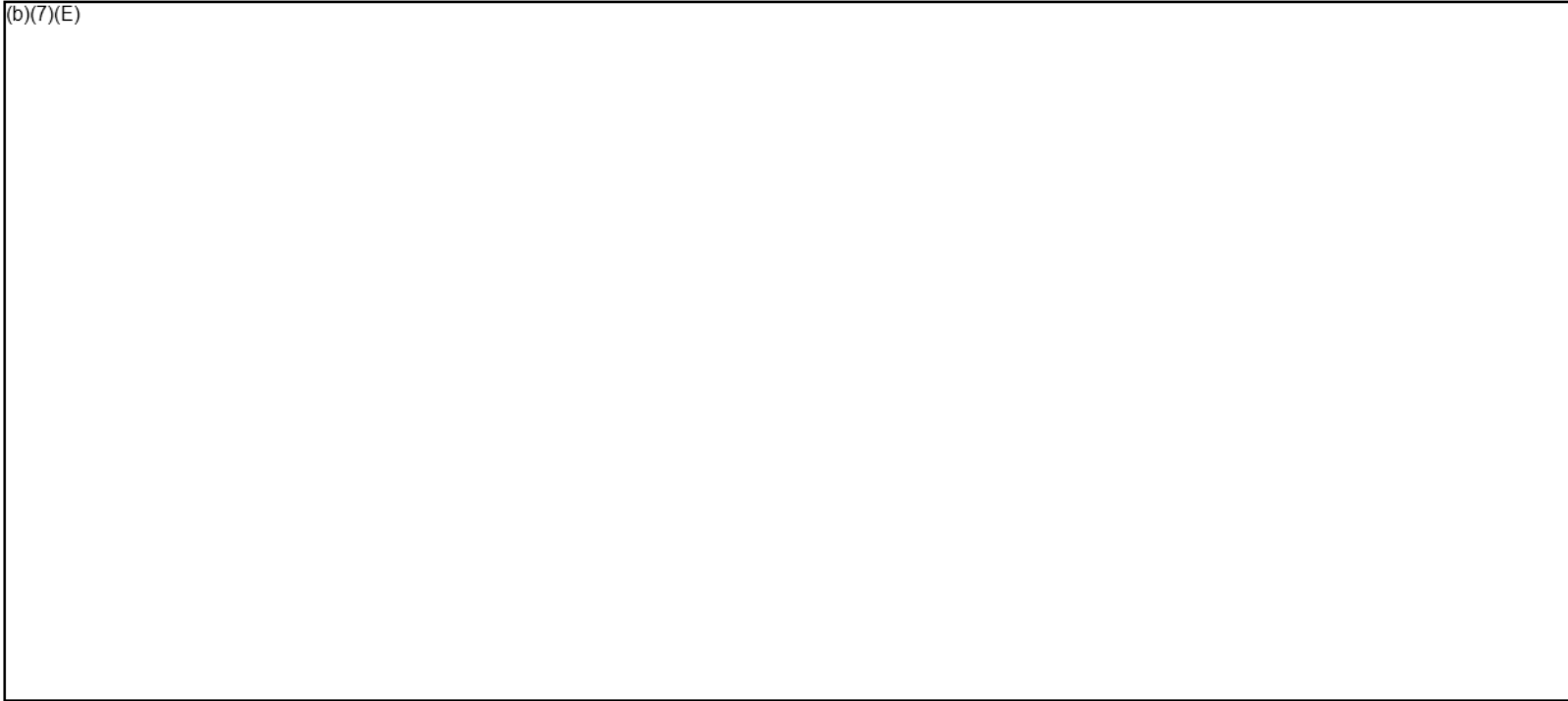
2020-ICL-00013-989

Homeland Security Investigations (HSI)



Applications for Use of Cell-Site Simulators

(b)(7)(E)



U.S. Immigration
and Customs
Enforcement

~~Law Enforcement Sensitive~~

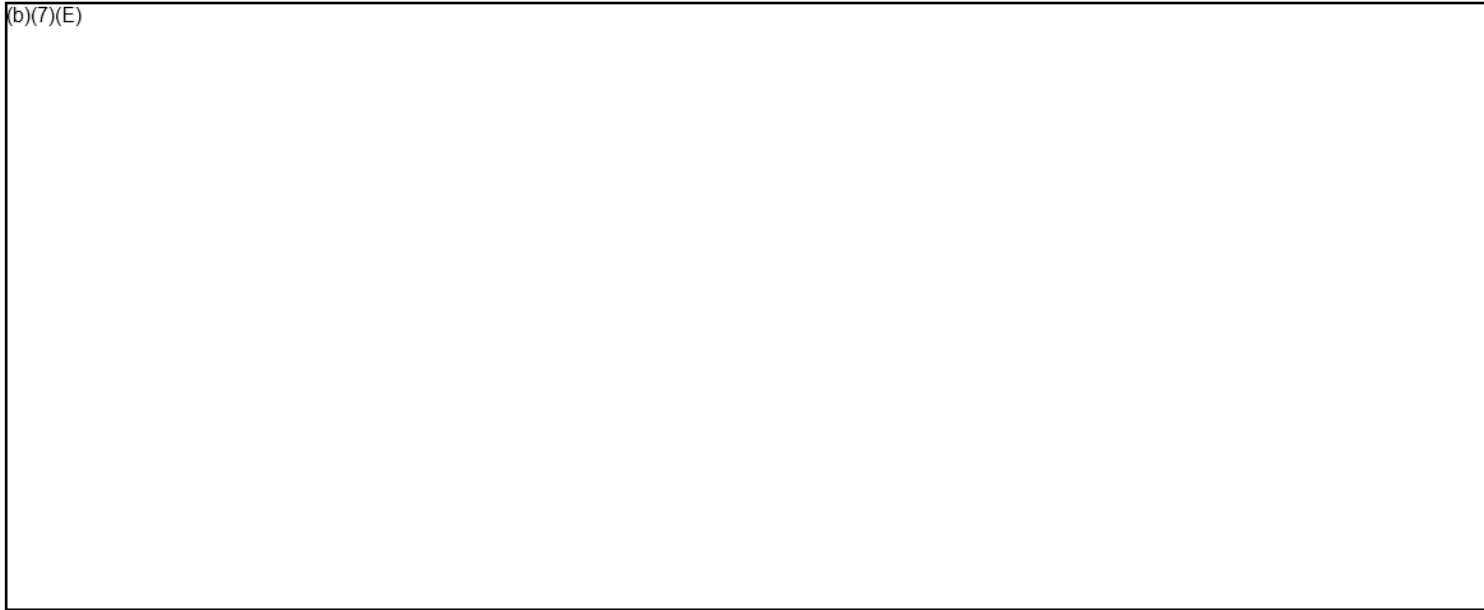
~~2020-ICL-00013-990~~

Homeland Security Investigations (HSI)

Data Collection & Disposal



(b)(7)(E)



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

Data Collection & Disposal



(b)(7)(E)



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

Training and Coordination



(b)(7)(E)

-
-
-



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

Improper Use of Cell-Site Simulators



Accountability is an essential element in maintaining the integrity of HSI. Activities involving the improper use of cell-site simulators, which are in contrast to the policies and procedures established by HSI in regard to these devices, as with other allegations of misconduct, will be reported to the ICE Office of Professional Responsibility or the Joint Intake Center.



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)



Frequently Asked Questions

Q: (b)(7)(E)

A:

Q:

A:



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)



Frequently Asked Questions

(b)(7)(E)

Q:

A:

Q:

A:



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)



Frequently Asked Questions

Q: (b)(7)(E)

A:

Q:

A:



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)



Frequently Asked Questions

Q: (b)(7)(E)

A:

Q:

A:



U.S. Immigration
and Customs
Enforcement

Homeland Security Investigations (HSI)

For Questions Pertaining to the
HSI Cell-Site Simulator Program,
Please Contact:



Technical Operations Unit
Cell-Site Simulator Program Manager

703-551-(b)(6); (b)(7)(C)



U.S. Immigration
and Customs
Enforcement



CNET News

FBI prepares to defend 'Stingray' cell phone tracking

Privacy groups plan to tell a judge tomorrow that controversial cell phone tracking technology, used by federal police since at least the mid-1990s, violates Americans' Fourth Amendment rights.

by [Declan McCullagh](#) March 27, 2013 4:57 PM PDT



Follow [@declanm](#)



The FBI has used "stingray" cell-tracking technology since at least the mid-1990s. Now it's the focus of a constitutional challenge.

The Federal Bureau of Investigation's secretive "Stingray" surveillance technology that allows police to surreptitiously track the locations of cell phones and other mobile devices will itself go on trial in an Arizona courtroom tomorrow afternoon.

Attorneys representing the U.S. Department of Justice are expected to defend warrantless use of stingray devices, which trick mobile devices into connecting to them by impersonating legitimate cell towers. Prosecutors yesterday filed court documents saying stingrays were used in investigations in Arizona and Wisconsin going back to 2008.

In the legal skirmishing leading up to tomorrow's three-hour hearing, federal attorneys have told U.S. District Judge David Campbell that the defendant in this case, Daniel Rigmaiden, did not have reasonable "privacy expectations" in the whereabouts of his Verizon mobile broadband card and "thus the agents in this case were not required to obtain a warrant."



One of the so-called stingray cell phone tracking devices, which impersonates a cell tower.

Civil libertarians are hoping the Rigmaiden case will be the first in the nation to impose privacy limits on how police use stingrays, in much the same way that previous legal challenges have resulted in curbs on warrantless use of thermal imaging devices and GPS tracking of vehicles through physical bugs.

To the American Civil Liberties Union and the Electronic Frontier Foundation, it's a clear case of surveillance technology outpacing the law. They say that "the government's use of the stingray violated the Fourth Amendment." Because stingrays represent a dragnet surveillance technique, capturing not only the target's electronic identifier but that of anyone else in the vicinity, the technique amounts to precisely the type of general search warrant outlawed by the Fourth Amendment, they say.

Another objection they have lodged is that federal agents did ask a judge to permit them to obtain telephone records from Verizon -- but, crucially, did not divulge that a stingray device was going to be used against Rigmaiden.

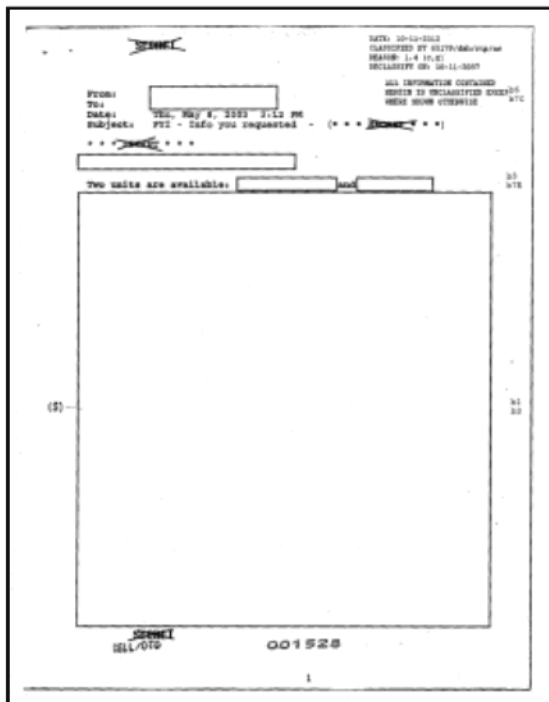
"Had the government candidly told the judge that it intended to use a stingray, he may have denied the application without prejudice to a subsequent application providing further details about the technology," the ACLU and EFF say. That's what happened last summer in Texas, when a federal magistrate judge rejected an effort by the Drug Enforcement Administration to deploy stingrays without obtaining a search warrant backed by probable cause.

Linda Lye, a staff attorney at the ACLU of Northern California who will be arguing in court in Arizona tomorrow, said this morning that there appears to be a pattern of concealment when police use stingray devices.

A newly disclosed email ([PDF](#)) from Miranda Kane, the head of the criminal division for the U.S. Attorney's office in the northern district of California, says (WIT refers to stingray devices):

It has recently come to my attention that many agents are still using WIT technology in the field although the pen register application does not make that explicit. While we continue work on a long term fix for this problem, it is important that we are consistent and forthright in our pen register requests to the magistrates...

Tomorrow's hearing in the case against Rigmaiden, who faces charges including conspiracy, wire fraud, mail fraud, and aggravated identity theft for allegedly filing more than 1,000 bogus tax returns, will center on his request to "suppress" data he contends the government acquired in violation of the Fourth Amendment. If he wins that argument, the so-called exclusionary rule would make evidence derived from unconstitutional surveillance inadmissible in court, but prosecutors could still win a conviction if the remainder of the evidence is sufficient.



The FBI has not disclosed details about its stingray devices. In response to an open records request from the Electronic Privacy Information Center, the bureau declassified this previously SECRET document but completely redacted it. [Click for larger image.](#)

(Credit: FBI)

The Justice Department has taken the unusual position of agreeing in January that the "the aircard location operation was a Fourth Amendment search and seizure." But, prosecutors say, they nevertheless intend to argue that the "defendant has no standing to complain" about any possible Fourth Amendment violations because, in part, he used a pseudonym to obtain the wireless device and rent the apartment: "Defendant's wide-ranging fraudulent and deceptive conduct should not merit an expectation of privacy that society is prepared to recognize as reasonable."

A ruling that the Fourth Amendment requires a warrant before deploying a stingray device would, if upheld on appeal, end the FBI's practice of attempting to obtain them using less privacy-protective procedures intended for recording what numbers were called on an analog telephone line. But it wouldn't halt the use of the devices: Agents could still deploy them using a warrant based on probable cause that a crime is being committed.

Stingrays aren't exactly new technology. A 1996 [Wired article](#) described how an FBI surveillance team from Quantico, Va., used one to track Kevin Mitnick: "It could also be used to page Mitnick's cell phone without ringing it, as long as he had the phone turned on but not in use. The phone would then act as a transmitter that they could home in on with a Triggerfish cellular radio direction-finding system that they were using."

Their use has spread far beyond the FBI and the military, which has long employed direction-finding gear. [LA Weekly reported](#) in January that the [First Amendment Coalition](#) obtained documents showing stingrays were used during routine "criminal investigations 21 times in a four-month period during 2012" by the Los Angeles Police Department. Those included burglary, drug, and murder investigations.


Last month, the Electronic Privacy Information Center obtained stingray documents ([PDF](#)) from the FBI describing procedures for the "loan" of stingray cell site simulators to state and local agencies. A 2009 [government procurement document](#) shows that the U.S. Secret Service paid Harris Corp., which makes stingray devices, over \$25,000 for training. (Harris secured [another](#) Secret Service contract last year.)

A trial in Rigmaiden's criminal case is scheduled to start in Phoenix on May 15.



Declan McCullagh

[Declan McCullagh](#) is the chief political correspondent for CNET. Declan previously was a reporter for Time and the Washington bureau chief for Wired and wrote the Taking Liberties section and Other People's Money column for CBS News' Web site.

 [Follow @declanm](#)

890 F.Supp.2d 747
(Cite as: 890 F.Supp.2d 747)

C

United States District Court,
 S.D. Texas,
 Corpus Christi Division.

In the Matter of THE APPLICATION OF THE
 UNITED STATES of America for AN ORDER
 AUTHORIZING THE INSTALLATION AND USE
 OF A PEN REGISTER AND TRAP AND TRACE
 DEVICE.

C.A. No. C-12-534M.
 June 2, 2012.

Background: Assistant United States Attorney applied for issuance of an order authorizing installation and use of pen register and trap and trace device to detect radio signals emitted from cellular telephones in vicinity of subject.

Holding: The District Court, Brian L. Owsley, United States Magistrate Judge, held that equipment required authorization pursuant to a warrant, rather than under pen register statute.

Denied.

West Headnotes

[1] Telecommunications 372  1475

372 Telecommunications

372X Interception or Disclosure of Electronic Communications; Electronic Surveillance

372X(B) Authorization by Courts or Public Officers

372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

The pen register and trap and trace device statute mandates that a court have a telephone number or some similar identifier before issuing an order authorizing such devices. 18 U.S.C.A. § 3123.

[2] Telecommunications 372  1475

372 Telecommunications

372X Interception or Disclosure of Electronic Communications; Electronic Surveillance

372X(B) Authorization by Courts or Public Officers

372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Equipment designed to capture cell phone numbers of phones within vicinity of subject of criminal investigation required authorization pursuant to a warrant, warranting denial of application pursuant to pen register statute; pen register applications required telephone number or some similar identifier and application did not explain the technology or process by which it would be used to gather subject's cell phone number. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 3123.

****748 OPINION DENYING THE APPLICATION FOR A PEN REGISTER AND TRAP AND TRACE DEVICE***

BRIAN L. OWSLEY, United States Magistrate Judge.

This matter comes before the Court pursuant to a written and sworn application pursuant to 18 U.S.C. §§ 3122(a)(1), 3127(5), and 2703(c)(1) by an Assistant United States Attorney who is an attorney for the government as defined by Rule 1(b)(1)(B) of the Federal Rules of Criminal Procedure and an accompanying affidavit of a special agent with the United States Drug Enforcement Agency.

BACKGROUND

In the application, the Assistant United States Attorney "certifies that the Drug Enforcement Administration (DEA) is conducting an ongoing criminal investigation regarding violations of federal criminal statutes." Specifically, the investigation focuses on a Subject alleged to be engaged in narcotics trafficking. The application details the investigation spanning several years of the Subject's alleged involvement and notes that at one point the Subject's cell phone number was known, but that the Subject apparently is no longer using that cell phone. Based on information provided by individuals cooperating with the investigation, it is believed that the Subject is using a new cellular telephone.

890 F.Supp.2d 747
 (Cite as: 890 F.Supp.2d 747)

In the pending application, the Assistant United States Attorney “requests the Court issue an order authorizing the installation and use of a pen register and trap and trace device for a period of sixty (60) days to 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.” The applicant further explains 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.”

After reviewing the application, an *ex parte* hearing was conducted with the special agent leading the investigation. He indicated that this equipment designed to capture these cell phone numbers was known as a “**stingray**.” Moreover, the Assistant*749 United States Attorney explained that the application was based on a standard application model and proposed order approved by the United States Department of Justice. During this hearing, a number of the decisions addressed below were discussed with the Assistant United States Attorney. He was not familiar with these cases, but indicated that he would be able to provide case law to support this application the next day.^{FNI}

^{FNI}. This memorandum was never provided to the Court.

The application has a number of shortcomings. It does 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. For example, there was no discussion as to 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.

While these various issues were discussed at the

hearing, the government did not have specific answers to these questions. Moreover, neither the special agent nor the Assistant United States Attorney appeared to understand the technology very well. At a minimum, they seemed to have some discomfort in trying to explain it.

ANALYSIS

Historically, a pen register was viewed as a device recording the outgoing numbers dialed from a specific telephone number. United States v. Giordano, 416 U.S. 505, 512 n. 2, 94 S.Ct. 1820, 40 L.Ed.2d 341 (1974) (noting that a pen register is “a device that records telephone numbers dialed from a particular phone”) (emphasis added); United States v. New York Telephone Co., 434 U.S. 159, 161 n. 1, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977) (“A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.”).

In 2001, Congress amended the definition of the term “pen register” as part of the USA PATRIOT Act. See In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F.Supp.2d 448, 455 (S.D.N.Y.2006). In that statute, Congress redefined a “pen register” as

a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

18 U.S.C. § 3127(3); accord *750In re United States, 622 F.Supp.2d 411, 414 (S.D.Tex.2007) . Additionally, a trap and trace device is defined as

890 F.Supp.2d 747
(Cite as: 890 F.Supp.2d 747)

a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

18 U.S.C. § 3127(4); accord *In re United States*, 622 F.Supp.2d at 414. Congress further mandated the information that a court needs to grant such an application based on what is required to be in the court order authorizing the pen register and trap and trace device

(b) Contents of order—an order issued under this section—

(1) shall specify—

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, *including the number or other identifier* and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied,....

18 U.S.C. § 3123(b)(1) (emphasis added).

With the PATRIOT Act, the definition of a pen register was broadened. *In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F.Supp.2d at 455. Nonetheless, courts still have determined that pen register applications seek information about a particular telephone. See, e.g., *United States v. Jadowe*, 628 F.3d 1, 6 n. 4 (1st Cir.2010) (“A ‘pen register’ is a device used, inter alia, to record the dialing and other information transmitted by a targeted phone.”); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F.Supp.2d 747, 752

(S.D.Tex.2005) (“A ‘pen register’ is a device that records the numbers dialed for outgoing calls made from the target phone.”); *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers*, 402 F.Supp.2d 597, 602 (D.Md.2005) (“pen register records telephone numbers dialed for outgoing calls from the target phone”); *In re Application of the United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F.Supp.2d 435, 438 (S.D.N.Y.2005) (“Pen Register Statute is the statute used to obtain information on an ongoing or prospective basis regarding outgoing calls from a particular telephone”); *In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Information*, 515 F.Supp.2d 325, 328 (E.D.N.Y.2007) (“In layman's terms, a pen register is a device capable of recording all digits dialed from a particular phone.”); *United States v. Bermudez*, No. 05-43-CR, 2006 WL 3197181, at *8 (S.D.Ind. June 30, 2006) (unpublished) (“A ‘pen register’ records telephone numbers dialed for outgoing calls made from the target phone.”). Similarly, a trap and trace device after the Patriot Act still seeks information about a particular phone. See, e.g., *751 *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers*, 402 F.Supp.2d at 602 (“trap/trace device ... records the telephone numbers of those calling the target phone”); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F.Supp.2d at 752 (“A trap and trace device captures the numbers of calls made to the target phone.”); *Bermudez*, 2006 WL 3197181, at *8 (“a trap/trace device records the telephone numbers of those calling the target phone”).

This approach is consistent with the current version of § 3123. Thus, a court is required to list in any order the identity of the person who is the cell phone subscriber, but only if that identity is known. See 18 U.S.C. § 3123(b)(1)(A). Additionally, the court is also required to include the name of the criminal investigation's subject, but again only if that identity is known. See 18 U.S.C. § 3123(b)(1)(B). However, regarding the telephone number or other

890 F.Supp.2d 747

(Cite as: 890 F.Supp.2d 747)

such identifier, Congress mandated explicitly that information be included within the court order. See 18 U.S.C. § 3123(b)(1)(C).^{FN2} The Patriot Act's revised definition of a pen register and trap and trace device in § 3127 simply amplifies the various types of information that are available such as routing and signaling information. See *Jadowe*, 628 F.3d at 6 n. 4; *In re Application of the United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F.Supp.2d at 438–39; see also *In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F.Supp.2d at 454 (noting that pen registers and trap and trace devices apply to particular cell phones and provide additional information such as cell site information); *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register Device*, 497 F.Supp.2d 301, 306 (D.P.R.2007) (“the term ‘signaling information’ under 18 U.S.C. § 3127(3) and (4) encompasses cell site information”).

^{FN2}. These specific identifiers include, *inter alia*, the Electronic Serial Number, the International Mobile Equipment Identity, the Mobile Equipment Identifier, or the Urban Fleet Mobile Identifier, which are addressed in both the application and the proposed order.

[1] The language of § 3123(b)(1) is straightforward in that a telephone number or similar identifier is necessary for a pen register. The Supreme Court has explained that “in all statutory construction cases, we begin with ‘the language itself [and] the specific context in which that language is used.’” *McNeill v. United States*, — U.S. —, 131 S.Ct. 2218, 2221, 180 L.Ed.2d 35 (2011) (quoting *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341, 117 S.Ct. 843, 136 L.Ed.2d 808 (1997)). Moreover, courts are to “look first to the word's ordinary meaning” when interpreting a statute. *Schindler Elevator Corp. v. United States ex rel. Kirk*, — U.S. —, 131 S.Ct. 1885, 1891, 179 L.Ed.2d 825 (2011) (citing *Gross v. FBL Fin. Servs., Inc.*, 557 U.S. 167, 175, 129 S.Ct. 2343, 174 L.Ed.2d 119 (2009)); accord *Wall v. Kholi*, — U.S. —, 131 S.Ct. 1278, 179 L.Ed.2d 252 (2011) (citing *Williams v. Taylor*, 529 U.S. 420, 431, 120 S.Ct. 1479, 146 L.Ed.2d 435

(2000)). Here, the plain language of the statute mandates that this Court have a telephone number or some similar identifier before issuing an order authorizing a pen register. The government has not provided any support to the contrary that the pen register statute should be interpreted in this manner.

The special agent leading the investigation referred to the equipment that the government proposes to use as a **stingray**. Other names for this equipment include *752 triggerfish, cell site simulator, and digital analyzer. Regardless of what it is called, there is scant case law addressing the equipment.

In a decision issued prior to the Patriot Act, one court defined a “digital analyzer” as “a portable device that can detect signals emitted by a cellular telephone ... [including] the electronic serial number (“ESN”) assigned to a particular cellular telephone, the telephone of the cellular telephone itself, and the telephone numbers called by the cellular telephone.” *In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, 885 F.Supp. 197, 198 (C.D.Cal.1995); see also *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F.Supp.2d 747, 755 (S.D.Tex.2005) (defining a triggerfish as equipment that “enables law enforcement to gather cell site data directly, without the assistance of the service provider”).

[2] In *United States v. Rigmaiden*, 844 F.Supp.2d 982 (D.Ariz.2012), the defendant was a fugitive who was charged with identity theft and mail and wire fraud. *Id.* at 987–88. “The government located and arrested Defendant, in part, by tracking the location of an aircard connected to a laptop computer that allegedly was used to perpetuate the fraudulent scheme.” *Id.* The defendant was seeking extensive discovery based on his allegations “that the technology and methods used to locate the aircard violated his Fourth Amendment rights.” *Id.* In that investigation, the law enforcement officers had both a pen register and trap and trace device as well as a warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a mobile tracking device. That court found that “[t]he mobile tracking device used by the FBI to locate the aircard functions as a cell site simulator. The mobile tracking device

890 F.Supp.2d 747
(Cite as: 890 F.Supp.2d 747)

mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard.” *Id.* at 995; *see also* 18 U.S.C. § 3117 (addressing mobile tracking devices). Moreover, that “mobile tracking device used to simulate a Verizon cell tower is physically separate from the pen register trap and trace device used to collect information from Verizon.” *Rigmaiden*, 844 F.Supp.2d at 995. Finally, the government asserted that “for purposes of Defendant’s motion to suppress, ... the Court may assume that the aircard tracking operation was a Fourth Amendment search and seizure.” *Id.*

Thus, *Rigmaiden* provides several salient points for the analysis here. The use of what was termed a cell site simulator was deemed a mobile tracking device. The government indicated that this cell site simulator was authorized pursuant to the warrant for the mobile tracking device as opposed to any pen register and trap and trace device. Finally, in that case, the government acknowledged that the proper analysis had to be pursuant to Fourth Amendment search and seizure jurisprudence.

Here, the application seeks an order authorizing the use of this equipment as a pen register as opposed to seeking a warrant. The government has not provided any support that the pen register statute applies to **stingray** equipment. Based on the statutory language and the limited case law analyzing this issue, a pen register does not apply to this type of electronic surveillance.

CONCLUSION

Accordingly, the government’s application for a pen register and trap and trace device is hereby denied without prejudice.

S.D.Tex.,2012.

In re the Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device
890 F.Supp.2d 747

END OF DOCUMENT



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSCconnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	Cell Site Simulator Technology and Log
(b)(6); (b)(7)(C); (b)(7)(E)	

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

SPECIFIC PTA QUESTIONS

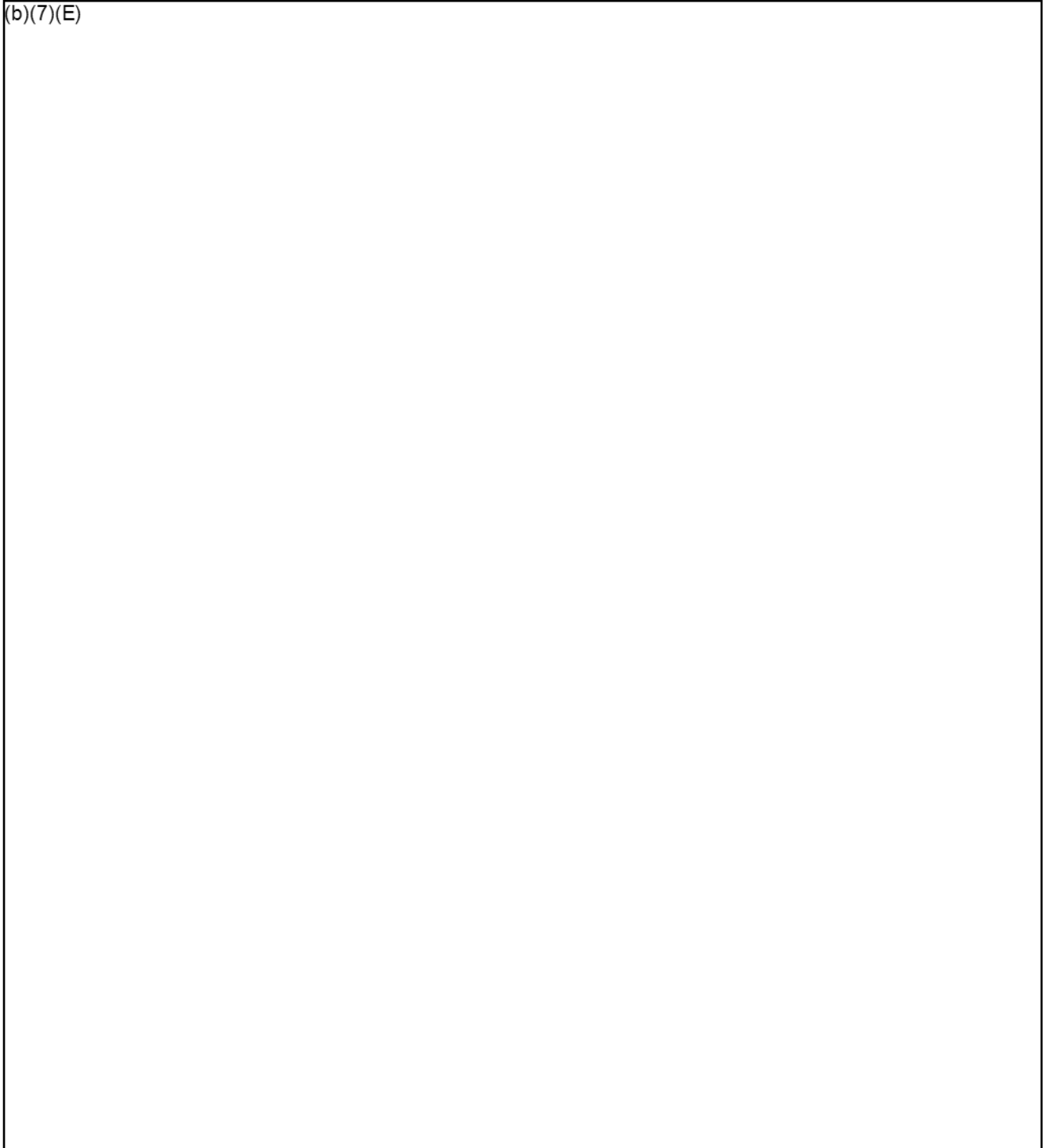
(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

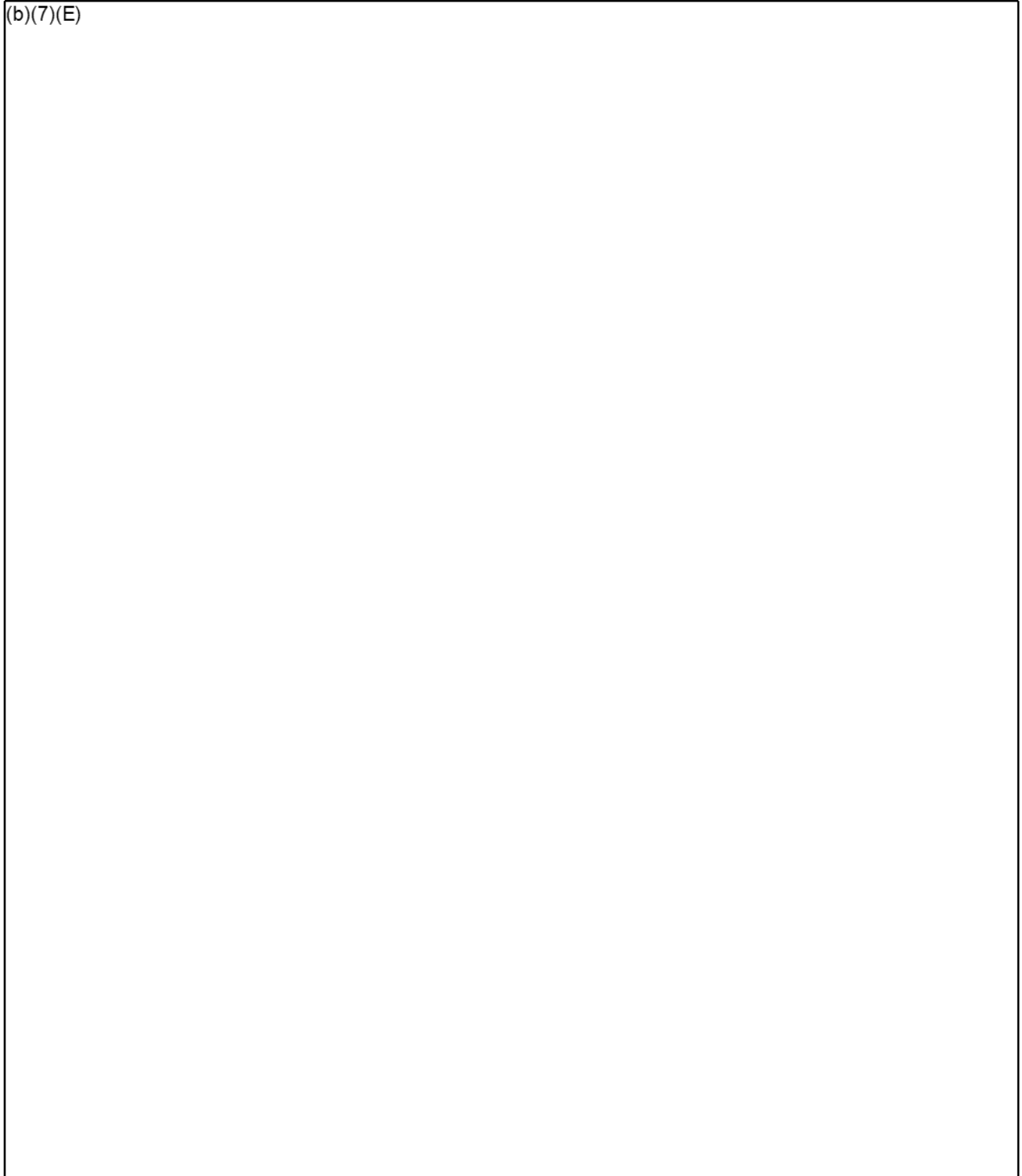
(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

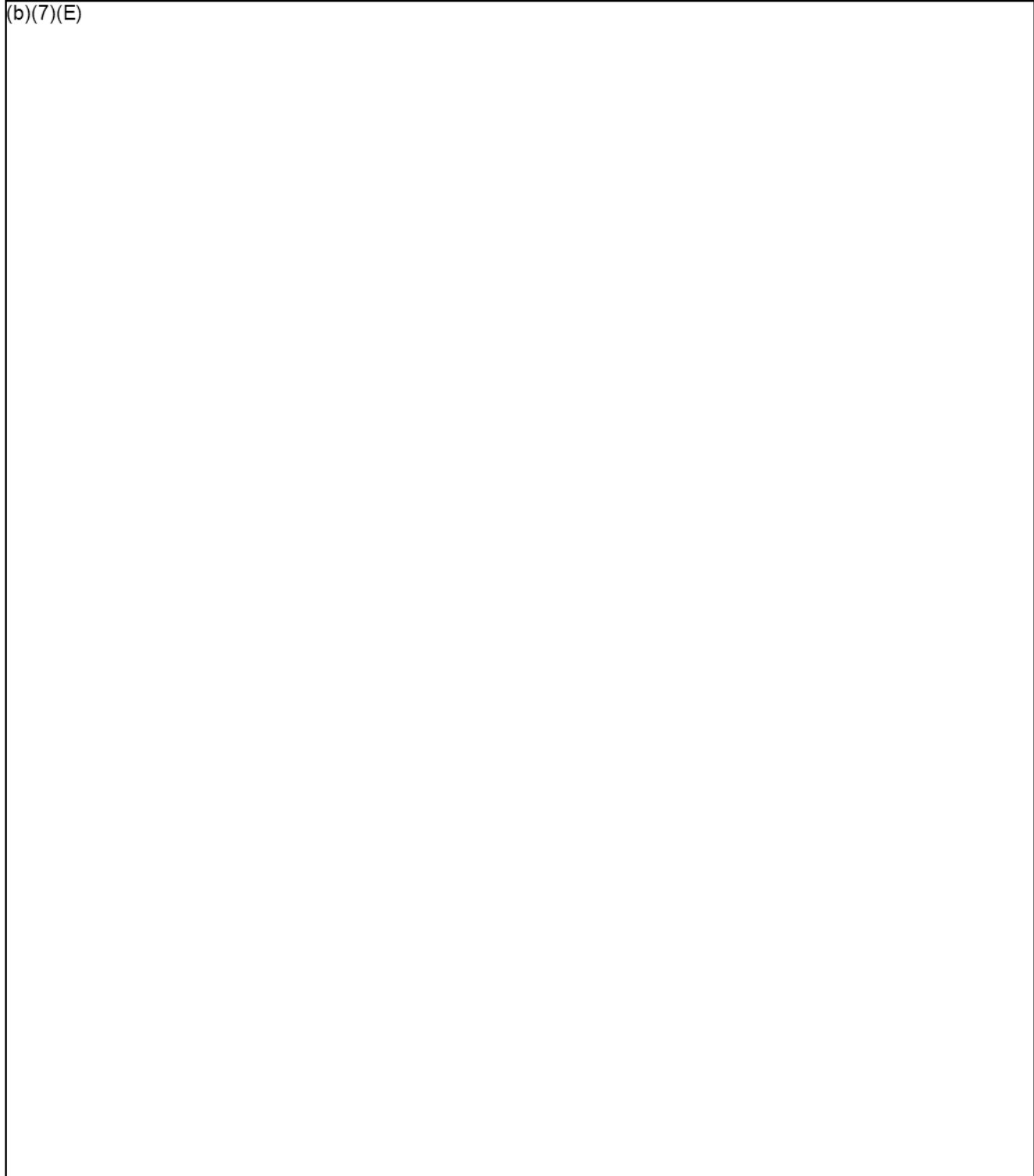


LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE



LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE

(b)(6); (b)(7)(C); (b)(7)(E)

LAW ENFORCEMENT SENSITIVE LAW ENFORCEMENT SENSITIVE