

IN THE FLORIDA SECOND JUDICIAL CIRCUIT
IN AND FOR LEON COUNTY, FLORIDA

STATE OF FLORIDA,

Plaintiff

v.

JAMES THOMAS,

Defendant

Case No.: 37 2008 CF 003350

Judge: Hankinson

Div. A

SPN 175470

v.

AMERICAN CIVIL LIBERTIES UNION
OF FLORIDA, INC.,

Intervenor

/

ACLU'S REPLY IN SUPPORT OF
MOTION FOR PUBLIC ACCESS TO SEALED JUDICIAL RECORDS

Intervenor ACLU of Florida ("ACLU") replies to the State's Response to the Court's Order to Show Cause ("Response") (filed May 12, 2014) in further support of the its motion for public access to the sealed portions (Christopher Corbitt's examination, pages 11-24) of the August 23, 2010, hearing transcript in this case:

The State points to two statutes—without any explanation of how they are applicable—for why the Court should continue to seal portions of Officer Corbitt's examination during the suppression hearing. Neither citation justifies excluding the public from a full and robust discussion about the "allegations of misconduct by

police and prosecution that raise constitutional issues” often at issue in a suppression hearing. *Miami Herald Pub. Co. v. Lewis*, 426 So. 2d 1, 8 (Fla. 1982). The State fails to attach any “documents or records upon which the Response is based,” as required by this Court’s March 6, 2014 Order to Show Cause. The State therefore fails to carry its “burden of producing evidence and proving by a greater weight of the evidence that closure is necessary, the presumption being that a pretrial hearing should be an open one.” *Lewis*, 426 So. 2d at 8; *see also* Fla. R. Jud. Admin. 2.420(e)(1) (setting forth the showing required of the party seeking to seal court records). *See State Farm Mut. Auto. Ins. Co. v. LaForet*, 591 So. 2d 1143, 1144 (Fla. 4th DCA 1992) (“A ‘showing’ is more than a bare assertion; it consists of specific explanations and reasons.”).

The Court should reject the State’s unsubstantiated assertions of secrecy and grant public access to the entire transcript of the suppression hearing.

I. Section 119.071(2)(d), Florida Statutes, Does Not Justify Continued Sealing of the Transcript

The State’s unsupported citation to “Section 110.071(2)(d), Florida Statutes”¹ does not provide the Court with a basis to continue sealing the transcript.

¹ The ACLU assumes that the intended citation is to § 119.071(2)(d), Fla. Stat. (exempting from disclosure under the Florida Public Records Act “information revealing surveillance techniques or procedures or personnel”), as § 110.071, Fla. Stat., was repealed in 1979.

In exempting from disclosure “[a]ny information revealing surveillance techniques or procedures or personnel,” § 119.071(2)(d), Fla. Stat., must be narrowly construed to further a public necessity. Fla. Const. Art. I, § 24(c).² Accordingly, to qualify for exemption, the specific information must (a) be both publically unknown—otherwise disclosing it would not “*reveal*[]” anything, § 119.071(2)(d), Fla. Stat.—and (b) substantially hinder, once known, the collection of criminal intelligence information—otherwise there would be no “public necessity.” Here, the State fails to explain how public access to the entire transcript would reveal TPD’s surveillance secrets and disrupt its ability to collect further criminal intelligence information. The State’s silence suggests it cannot satisfy the public necessity for the exemption because the transcript does not reveal anything new and important.

Extensive information about cell site simulators is already public, including information released by the Tallahassee Police Department (“TPD”) and the Florida Department of Law Enforcement (“FDLE”). *See infra* Part IV. Once

² The Florida Constitution requires that exemptions to the public access to records be supported by a specific “public necessity justifying the exemption and . . . no broader than necessary to accomplish the stated purpose of the law.” Fla. Const. Art. I, § 24(c). Although the 1979 law creating § 119.071(2)(d), Fla. Stat., did not include a statement of public necessity (as it was enacted before § 24(c)), the current exemption nonetheless is properly limited to information for which there is a public necessity. *In re Amendments to Florida Rule of Judicial Admin. 2.420-Sealing of Court Records & Dockets*, 954 So. 2d 16, 17 (Fla. 2007) (observing that Florida Supreme Court rules, including Fla. R. Jud. Admin. 2.420, “strongly disfavor court records that are hidden from public scrutiny”); *see also Marino v. Univ. of Fla.*, 107 So. 3d 1231, 1233 (Fla. 1st DCA 2013) (“public records exemptions are to be narrowly construed”).

information is in the public domain, “there remains little to be hidden from disclosure, and given [Florida law’s] overwhelming preference for complete public access to documents,” continued sealing should not be allowed. *Downs v. Austin*, 522 So. 2d 931, 935 (Fla. 1st DCA 1988); *see also Staton v. McMillan*, 597 So. 2d 940, 941 (Fla. 1st DCA 1992) (“[T]he statutory exemptions [to disclosure] do not apply if the information has already been made public.”). Thus, even if the State had made a serious attempt to carry its burden that continued sealing is justified—which it has not—any application of the exemption has been waived.

Furthermore, the information is unlikely the kind of detailed, secretive protocols that would actually thwart TPD’s investigations. In contrast, information about, for example, whether law enforcement obtained a warrant or court order permitting it to use the cell site simulator, whether it was relying on a nondisclosure agreement with a private corporation or a state or federal agency to avoid disclosing use of the cell site simulator to judges or defense attorneys, and whether it has policies in place to regulate cell site simulator use, would not reveal “surveillance techniques or procedures.” This is the information likely discussed in Officer Corbitt’s examination.

Accordingly, § 119.071(2)(d), Fla. Stat., presents no basis for the continued sealing of the transcript.

II. The Homeland Security Act Does Not Apply to the Information at Issue

The State also cites to the federal Homeland Security Act, 6 U.S.C. § 482, but again fails to explain how it has any bearing on the propriety of public access to the sealed portions of August 23, 2010, transcript. *See* Response at 1.

The Act provides that “information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information.” 6 U.S.C. § 482(e). “Homeland security information” is defined as

- any information possessed by a Federal, State, or local agency that--
 - (A) relates to the threat of terrorist activity;
 - (B) relates to the ability to prevent, interdict, or disrupt terrorist activity;
 - (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or
 - (D) would improve the response to a terrorist act.

Id. § 482(f)(1).

The information contained in the redacted portions of the transcript is not covered by this provision for at least four reasons.

First, the information was not “obtained . . . from a Federal agency.” Investigator Corbitt’s testimony concerns use of a cell site simulator by the Tallahassee Police Department in a local criminal investigation. Details of the use

of the device, information about whether the government obtained a warrant or court order authorizing use of the device, and facts concerning the potential violation of the Defendant's and third parties' privacy rights cannot be construed as having been "obtained" from a federal agency.

Second, for § 482(e) to apply the information must have been obtained "from a Federal agency *under this section*." (Emphasis added). That means that a federal agency must have provided the information to state or local personnel "through information sharing systems," *id.* § 482(b)(1), including "the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation," *id.* § 482(b)(4). The State has made no representation or showing that information contained in the transcript was obtained from a federal agency, much less that it was obtained through an "information sharing system" as statutorily defined.

Third, the Act provides that "*a State or local law* authorizing or requiring [a state or local] government to disclose information shall not apply to such information." 6 U.S.C. § 482(e) (emphasis added). But unsealing of the transcript is required by federal, in addition to state, law. Because the public's right of access to judicial records is secured by the First Amendment to the U.S. Constitution and

by federal common law, § 482 does not apply. *See Press-Enterprise Co. v. Superior Court*, 478 U.S. 1 (1986) (public has a First Amendment right of access to the transcript of a preliminary hearing in a criminal case).

Fourth, the transcript cannot plausibly contain “homeland security information” because the redacted information does not relate to terrorist activity. The investigation in this case involved allegations of sexual assault and theft, and there has been no suggestion by the government that the Defendant was suspected of any terrorism-related offense. Moreover, *none* of the TPD’s 277 uses of cell site simulators since 2007 have involved terrorism investigations. The Police Department has used cell site simulators in a range of criminal and missing persons investigations, but never in a terrorism case. *See* Wessler Decl. Ex. A (list produced by TPD in response to ACLU public records request showing all uses of cell site simulators since 2007 and identifying each incident or offence under investigation).

Further, the use of cell site simulators only “relates to the ability to prevent, interdict, or disrupt terrorist activity,” 6 U.S.C. § 482(f)(1)(B), to the same extent that every other law enforcement investigative tool or technique does. Fingerprint kits, binoculars, squad cars, helicopters, handguns, and Title III wiretap authority are all possible to use in investigations of both ordinary crimes and terrorism

threats. But the mere possibility of using a device, authority, or technique in a terrorism investigation does not mean that every mention of it should be stricken from court records in run-of-the-mill criminal cases. Having allowed state and local police departments around the country to obtain and use cell site simulators in the full range of criminal cases,³ the government cannot now try to invoke vague and inapplicable counterterrorism concerns to shield normal law enforcement activities from public view.

III. The Federal Caselaw and Statutes Cited by the State Have No Bearing On This Case

All but one of the grounds for continued sealing asserted in the Response sound in federal law. Yet this is a state-court proceeding governed by state law. *See generally* ACLU's Mot. for Public Access to Judicial Records. The State itself acknowledges as much, writing that federal law is "not . . . strictly applicable" to this case. Response at 2. Nonetheless, it throws up a smokescreen of inapplicable federal court opinions and statutes in apparent hope of distracting the Court. The Court need not pay this tactic any heed.

³ See John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA Today (Dec. 8, 2013), <http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsapolice/3902809/> (finding that at least 25 of 125 police departments investigated by USA Today own cell site simulators).

A. The Federal Freedom of Information Act Is Irrelevant

The State's citation to an exemption to the federal Freedom of Information Act, *see* Response at 2 (citing 5 U.S.C. § 552(b)(7)(E)), is clearly irrelevant:

“Whatever the federal act may provide as to documents in the possession of federal agencies, the Act is not applicable to state agencies.” *Wallace v. Guzman*, 687 So. 2d 1351, 1353 (Fla. 3d DCA 1997).

B. The Federal “Law Enforcement Privilege” Does Not Apply Here

Citations to federal cases concerning the so-called “law enforcement privilege” are similarly unavailing. *See* Response at 2. Although Florida courts recognize a narrow privilege against compelled disclosure of a confidential informant's identity to a defendant in a criminal case, *Treverrow v. State*, 194 So. 2d 250 (Fla. 1967), the State cites no case, and the ACLU is aware of none, recognizing a broader law enforcement privilege as a matter of state law, nor applying any such privilege to motions for public access to judicial records. Thus, the State's citations are patently inapposite.

Even if such privilege existed under state law, it would be inapplicable here. First, the law enforcement privilege applies to government “investigatory files.” *White v. City of Fort Lauderdale*, No. 08-60771-CIV, 2009 WL 1298353, at *4 (S.D. Fla. May 8, 2009). The only document at issue here, however, is a transcript of a judicial hearing in which a government agent provided testimony in the

presence of counsel for both parties and the Court. The claimed privilege does not apply. *Cf. id.* (holding that the law enforcement privilege does not apply to the plaintiff's interrogatories directed at individual defendants); *JTR Enters., LLC v. An Unknown Quantity of Colombian Emeralds, Amethysts & Quartz Crystals*, 297 F.R.D. 522, 529 (S.D. Fla. 2013) (“[Plaintiff] did not request any governmental or law enforcement agency to produce their investigatory files or communications. . . . [W]e find that the privilege does not apply . . .”).

Second, the law enforcement privilege is “a qualified privilege protecting investigative files in an *ongoing* criminal investigation.” *In re U.S. Dep't of Homeland Sec.*, 459 F.3d 565, 572 (5th Cir. 2006) (Dennis, J., concurring) (emphasis added) (internal quotation marks omitted); *accord Sirmans v. City of S. Miami*, 86 F.R.D. 492, 495 (S.D. Fla. 1980) (“The applicable federal privilege for criminal investigative files provides for the protection of files relating to ongoing criminal investigations.”). Therefore, “the privilege lapses either at the close of an investigation or at a reasonable time thereafter based on a particularized assessment of the document.” *In re U.S. Dep't of Homeland Sec.*, 459 F.3d at 571 (majority opinion). Here, the investigation concluded in 2008 and trial was held in 2011. Even if a description of the investigation in this case might once have been privileged, any privilege lapsed during the nearly six years since the investigation closed. *See JTR Enters., LLC*, 297 F.R.D. at 529 (citing failure to “provide[] an

affidavit or any supporting documentation to confirm that there is, in fact, an ongoing criminal investigation” as reason to deny application of the privilege).

Third, the federal law enforcement privilege must be formally invoked by “the head of the department having control over the documents,” and that invocation must be accompanied by “a detailed specification of the information for which the privilege is claimed, with an explanation why this information properly falls within the scope of the privilege.” *In re Polypropylene Carpet Antitrust Litig.*, 181 F.R.D. 680, 687 (N.D. Ga. 1998) (citing *Tuite v. Henry*, 98 F.3d 1411, 1417 (D.C. Cir. 1996)); *accord JTR Enters., LLC*, 297 F.R.D. at 529. The State provides no such invocation or explanation here.

Fourth, “in determining whether the privilege should apply, a court must balance the government’s interest in confidentiality against the litigant’s need for information.” *White*, 2009 WL 1298353, at *3; *see also United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir. 1986) (“We stress that the necessity determination requires a case by case balancing process, and that we have established no fixed rules about the discoverability of electronic surveillance techniques in criminal cases.”). As explained in the ACLU’s motion for public access, Florida courts recognize the strength of the public’s right of access to judicial records, and

“‘strongly disfavor court records that are hidden from public scrutiny.’” ACLU Mot. at 20 (quoting *In re Amendments*, 954 So. 2d at 17).

Finally, “the law enforcement investigatory privilege ‘can be waived, and, once waived, is lost.’” *In re Polypropylene Carpet Antitrust Litig.*, 181 F.R.D. at 689 (quoting *Dellwood Farms, Inc. v. Cargill, Inc.*, 128 F.3d 1122, 1126 (7th Cir. 1997)). As detailed below, *see infra* Part IV, the TPD and the State of Florida have waived their interest in preserving the secrecy of their use of a cell site simulator in this investigation by publicly disclosing facts about their possession and use of cell site simulators, including that they used a cell site simulator in this and other cases. Application of the privilege is also waived by the large volume of other publicly available information about cell site simulator devices and law enforcement use of them.

IV. Extensive Information About Cell Site Simulators Is In the Public Domain

The State’s attempt to permanently seal portions of the hearing transcript must be reconciled with the large amount of information about cell site simulators already in the public domain. In light of this public information there is no valid basis for maintaining any portion of the August 23, 2010, transcript under seal.

A. Information Released by the TPD and FDLE

The ACLU sent public records requests to the TPD and FDLE concerning their possession and use of cell site simulators on February 27, 2014 and March 13, 2014, respectively. In response, the TPD released a list of 277 separate instances since 2007 where it contended it used cell site simulators to track the locations of cell phones in investigations. Wessler Decl. Ex. A.⁴ The investigation at issue in this case is included on that list (in the entry dated 9/13/2008). The entry discloses the telephone number of the target phone and a location, “Pensacola/White,”⁵ where the tracking apparently commenced. Also public is the address to which the TPD tracked the phone: 2060 Continental Avenue, Apartment 251. Suppression Hr’g Tr. 27:9–14, 106:6–7, August 23, 2010. The public therefore already knows where the cell site simulator was used. The public also knows how precisely the cell site simulator can track a phone: to a particular apartment within a large apartment complex. *See id.* at 27:9–14;⁶ *Thomas v. State*, 127 So. 3d 658, 659–60

⁴ The version of the spreadsheet provided by the TPD includes the phone number tracked in each investigation. In recognition of the privacy interest of individual phone users whose phones were tracked, the ACLU has redacted the last four digits of each number in the copy of the spreadsheet filed with the Court. *See* Fla. R. Jud. Admin. 2.425(a)(4).

⁵ Likely the corner of West Pensacola Street and White Drive in Tallahassee.

⁶ “Q: What was your level of certainty that phone that you were seeking to obtain or recover was within the apartment at Apartment 251, there at Berkshire Manor Apartments.

A: My level of certainty was enough to swear in a probable cause affidavit that I believe that property was in there.”

(Fla. 1st DCA 2013) (“[P]olice were able to track her cell phone to the apartment Mr. Thomas shared with his girlfriend. The investigators settled on a specific apartment ‘shortly after midnight’ . . .”).

The TPD has also provided information about its use of cell site simulators to the press. TPD Chief Michael DeLeo and spokesperson David Northway have discussed the technology on camera and in print, providing information about whether and when the Department obtains court authorization to use a cell site simulators, whether it relies on information obtained using cell site simulators to apply for search warrants at later stages of an investigation, what types of investigations the devices are used in, and what policies govern their use.⁷ The TPD has even described the types of information that it does and does not collect while using cell site simulators.⁸

⁷ See Video: *TPD Chief Talks ‘Stingray’ Use* (Tallahassee Democrat Mar. 16, 2014), <http://archive.tallahassee.com/article/20140317/NEWS01/303170020>; Jennifer Portman, *Is Cellphone Stingray Invasive or Essential?*, Tallahassee Democrat, Mar. 16, 2014, *available at* <http://archive.tallahassee.com/article/20140317/NEWS01/303170020>, attached as Exhibit B to the Wessler Declaration; Jennifer Portman, *TPD Changes Tracking Policy*, Tallahassee Democrat, Apr. 13, 2014, *available at* <http://www.tallahassee.com/article/20140413/NEWS01/304130018>, attached as Exhibit D to the Wessler Declaration.

⁸ See *TPD Chief Talks ‘Stingray’ Use*, *supra* (“I do want to . . . reassure people that we are not using the technology indiscriminately, that we’re not tracking people’s whereabouts, we’re not eavesdropping on conversations or reading text messages or emails or anything like that.”).

The FDLE has also released relevant information, including about its purchase and use of cell site simulators. In response to the ACLU's public records request, the FDLE released a copy of the Electronic Surveillance Support Team Multi-Agency Voluntary Cooperation Mutual Aid Agreement between the FDLE and TPD through which the FDLE loans its cell site simulators to the TPD for use in investigations. *See* Wessler Decl. Ex. E.⁹ The FDLE also released purchase records detailing more than three million dollars of expenditures on cell site simulators and related equipment from the Harris Corporation, *see* Wessler Decl. Ex. G,¹⁰ as well as a copy of the non-disclosure agreement the FDLE signed with the Harris Corporation concerning its purchase and use of that equipment. *See* Wessler Decl. Ex. H.¹¹ The FDLE has identified 1,835 uses of cell site simulators

⁹ Although the copy of the Mutual Aid Agreement signed by the TPD includes two redactions, a copy of an identical agreement signed by another police department in the state includes no redactions. *See* Wessler Decl. Ex. F.

¹⁰ *See also* Wessler Decl. Ex. B (“Since 2008, purchase records show FDLE has placed about 15 orders with the Melbourne-based company, for equipment, software and support services totaling more than \$3 million. Purchase requests show a single unit, along with various software packages, cost nearly \$300,000.”).

¹¹ *See also* Jennifer Portman, *FDLE Signed Stingray Non-Disclosure Deal*, Tallahassee Democrat, Mar. 30, 2014, *available at* <http://www.tallahassee.com/apps/pbcs.dll/article?AID=2014303300011>, attached as Exhibit C to the Wessler Declaration. Although the copy of the non-disclosure agreement released by the FDLE includes several small redactions, a nearly identical non-disclosure agreement released by the Tucson, Arizona, Police Department is unredacted. *See* Wessler Decl. Ex. I.

in its files, *see* Wessler Decl. Ex. J, and has described to the press how and when it uses the devices, and what information it collects when using them.¹²

B. Information in Judicial Opinions and Records

Judicial opinions and court documents from around the country reveal details about how cell site simulators are used in particular investigations. The U.S. District Court for the District of Utah, for example, detailed testimony by an FBI agent describing, step-by-step, how he used a cell site simulator “to determine, with a reasonable degree of certainty, a fairly narrow geographical location where an individual is located while a cell call is being placed.” *United States v. Allums*, No. 2:08–CR–30 TS, 2009 WL 806748, at *1 (D. Utah Mar. 24, 2009), Wessler Decl. Ex. K. In a Wisconsin case, police officers testified in a suppression hearing in open court about their use of a cell site simulator to track a cell phone signal to a particular apartment building. Motion Hearing Transcript at 13–16, *State v. Tate*, No. 09CF002842 (Wis. Cir. Ct., Milwaukee Cnty. Apr. 22, 2011), Wessler Decl. Ex. L, *appeal pending*, No. 2012AP000336-CR (Wis. Argued Oct. 3, 2013). In a federal case in California, the court docketed a copy of the government’s application for an order authorizing use of a cell site simulator, which included a detailed description of how the device would be used:

¹² Wessler Decl. Ex. B (quoting FDLE Commissioner Gerald Bailey and spokesperson Gretl Plessinger).

A cell site simulator is a mobile device that captures the signaling information—the phone number, serial number, etc.—of cell phones within the vicinity. The cell site simulator mimics a cell site tower in that it reads signaling information broadcast in public by cell phones turned on in the area. After locating [the suspect] through physical surveillance, agents will position the cell site simulator nearby. Any cell phone that [the suspect] possesses (if turned on), as well as other cell phones nearby, will transmit their signaling information to the cell site simulator. Agents will repeat the process multiple times at different locations and times. By identifying the signaling data common to each capture—i.e., the signaling information that comes up each time—agents can determine the signaling information for a phone used by [the suspect].

Motion to Suppress Cell Site & Simulated Cell Site Evidence, Ex. B-1 at 2 n.2, *United States v. Espudo* (No. 12CR0236-IEG) 954 F. Supp. 2d 1029 (S.D. Cal. filed Apr. 8, 2013), Wessler Decl. Ex. M. An opinion from the U.S. District Court for the District of Arizona includes a list of factual admissions by the government concerning its use of a cell site simulator in the case. *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012). A 2012 indictment filed in the Northern District of Illinois describes use of a cell site simulator (called a “digital analyzer device”) to identify a suspect’s cell phone number. Criminal Complaint at 8 n.1, *United States v. Arguijo* (N.D. Ill. Feb. 13, 2012), *available at* http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222_01d.pdf, Wessler Decl. Ex. N. A 2006 opinion from the Southern District of Indiana describes law enforcement’s use of a cell site simulator “to pinpoint the multi-unit residence located at 5352 West Deming Place as the precise location of a particular cell

phone believed to be used by or otherwise connected with [the suspect].” *United States v. Bermudez*, No. IP05-0043-CR05-BF, 2006 WL 3197181, at *1 (S.D. Ind. June 30, 2006), Wessler Decl. Ex. O, *aff’d sub nom. United States v. Amaral-Estrada*, 509 F.3d 820 (7th Cir. 2007). These and other descriptions of cell site simulator use in public judicial records belie the State’s claim that the transcript must remain partially sealed.

C. Public Information About Harris Corporation’s Cell Site Simulator Devices

Detailed information about the technical specifications and capabilities of cell site simulators is also publicly available from numerous sources, including patent applications submitted by the Harris Corporation. *See, e.g.*, U.S. Patent No. 7,592,956 (filed Feb. 12, 2008), Wessler Decl. Ex. P. Harris has even publicly filed photos of its devices with the U.S. Patent and Trademark Office. *See* Wessler Decl. Exs. Q–S.¹³ Harris Corporation’s own promotional materials also describe the capabilities and features of its cell site simulators. *See, e.g.*, Wessler Decl. Ex. T¹⁴

¹³ Available at <http://tsdr.uspto.gov/documentviewer?caseId=sn76303503&docId=SPE20130404144554#docIndex=2&page=1>;

<http://tsdr.uspto.gov/documentviewer?caseId=sn77316689&docId=SPE20140514151847#docIndex=1&page=1>;

<http://tsdr.uspto.gov/documentviewer?caseId=sn76303814&docId=SPE20140213150610#docIndex=2&page=1>.

¹⁴ Available at <http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf>.

(Harris product information sheets for StingRay and AmberJack); Wessler Decl. Ex. U¹⁵ (Harris product information sheet for KingFish); *see also* Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, Ars Technica, Sept. 25, 2013¹⁶ (describing Harris Corporation's line of cell site simulators).

Documents made public by state and local governments as part of their cell site simulator procurement processes reveal similar details. For example, the Anchorage, Alaska, Police Department's purchase request for a Kingfish cell site simulator describes its capabilities as including the ability to:

- Identify location of an active cellular device to within 25 feet of actual location anywhere in the United States
- Track the route of any active cellular device and record tracking information for evidentiary purposes
- Mimic the functional appearance of an active cellular service tower
- Interrupt service to active cellular connection
- Prevent connection to identified cellular device ("No Service")

Wessler Decl. Ex. V. Likewise, letters from Harris Corporation to the Miami Police Department describe technical details of the StingRay and KingFish,

¹⁵ Available at <http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf>.

¹⁶ <http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/>.

including the radio frequencies over which they broadcast. Wessler Decl. Ex. W–X.¹⁷

D. Information Released by the Federal Government

Finally, the federal government has released significant information about use and regulation of cell site simulators. In response to a Freedom of Information Act request from the Electronic Privacy Information Center, the U.S. Department of Justice has released thousands of pages of documents about the use of cell site simulators in criminal investigations.¹⁸ Likewise, the Department of Justice Electronic Surveillance Manual describes the capabilities of cell site simulators:

Law enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones by the electronic signals that they broadcast. This equipment includes an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information. Working together, these devices allow the agent to identify the direction (on a 360 degree display) and signal strength of a particular cell phone while the user is making a call. By shifting the location of the device, the operator can determine the phone's location more precisely using triangulation.

¹⁷ Available at <http://egov.ci.miami.fl.us/Legistarweb/Attachments/34768.pdf> and <http://egov.ci.miami.fl.us/Legistarweb/Attachments/48003.pdf>.

¹⁸ See *EPIC v. FBI – Stingray/Cell Site Simulator*, Electronic Privacy Information Center, <https://epic.org/foia/fbi/stingray/>.

Wessler Decl. Ex. Y.¹⁹ The Manual also explains the legal process that federal agents are required to obtain in order to use cell site simulators. *Id.* at 45–48.²⁰

The Federal Communications Commission has also released information about regulation of cell site simulators, including letters from local police departments seeking permission to use the devices on the public radio spectrum. *See* Wessler Decl. Ex. Z.

* * *

The publicly available information about cell site simulators, including information about TPD’s use of them, fatally undermines the State’s claim that information in the hearing transcript must remain sealed. This Court should reject the State’s attempt to shield important information about the legality and constitutionality of government conduct from public view. The government has already spoken publicly about cell site simulators to defend their use. *See, e.g.,* Wessler Decl. Exs. B–D. It should not be able to wield the sword of its statements to favorably influence public opinion, but then use the sealing process as a shield against release of complete and accurate information to the public when such

¹⁹ Dep’t of Justice, *Electronic Surveillance Manual* 44 (June 2005), available at <http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf>.

²⁰ *See also Electronic Investigative Techniques*, U.S. Atty’s Bull., Sept. 1997, at 13–14 (discussing use of digital analyzers and cell site simulators), available at http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf.

information might reveal violations of law. *Cf. Downs*, 522 So. 2d at 935 (once the government has disclosed information “to its advantage, there remains little to be hidden from disclosure”).

CONCLUSION

For the foregoing reasons, and for the reasons stated in the ACLU’s opening brief, this Court should reject the State’s proposal to permanently seal selected portions of the August 23, 2010, transcript. The public’s right of access attaches to that judicial record, and it should be unsealed in full.

CERTIFICATE OF SERVICE

I certify that the foregoing document has been furnished to the following by filing the document today through the e-Service system (Fla.R.Jud.Admin. 2.516(b)(1):

Kathryn Ray (State Attorney), RayKa@leoncountyfl.gov
Daren Shippy (Def. Thomas), daren.shippy@rc1.myflorida.com
Rick Courtemanche (Tallahassee Police), Rick.Courtemanche@talgov.com
Lewis Shelley (Tallahassee Police) Lewis.Shelley@talgov.com,
paula.burn@talgov.com

Dated: May 27, 2014

Respectfully Submitted,

s/Benjamin James Stevenson

Benjamin James Stevenson

Fla. Bar. No. 598909

ACLU Found. of Fla.

Post Office Box 12723

Pensacola, FL 32591-2723

T. 786.363.2738

F. 786.363.1985

bstevenson@aclufl.org

Nathan Freed Wessler

N.Y. Ba No. 4878880 (Admitted *Pro Hac Vice*)

American Civil Liberties Union Foundation

125 Broad Street, 18th Floor

New York, NY 10004

T. 212.549.2500

F. 212.549.2654

nwessler@aclu.org

Counsel for Intervenor ACLU