EFiled: May 09 2016 03:32PM EDT
Transaction ID 58977958
Case No. N16A-02-006 RRC

IN THE SUPERIOR COURT OF THE STATE OF DELAWARE

JONATHAN RUDENBERG, Petitioner Below, Appellant v. DELAWARE DEPARTMENT OF JUSTICE, THE CHIEF DEPUTY ATTORNEY GENERAL & DELAWARE DEPARTMENT OF SAFETY AND HOMELAND SECURITY, DIVISION OF STATE POLICE, Respondents Below, Appellees	C.A. No. N16A-02-006 RRC

Compendium to Appellant's Opening Brief

Ryan Tack-Hooper (No. 6209)
Richard H. Morse (No. 531)
American Civil Liberties Union Foundation of Delaware
100 West 10th Street, Suite 706
Wilmington, DE 19801
(302) 654-5326 x 105
Attorneys for Petitioner Below, Appellant

May 9, 2016

TABLE OF CONTENTS

Tab

A

ACLU of N. Cal. v. DOJ

United States District Court for the Northern District of California

June 17, 2015, Decided; June 17, 2015, Filed

Case No. 13-cv-03127-MEJ

Reporter
2015 U.S. Dist. LEXIS 79340; 2015 WL 3793496

AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA, Plaintiff, v. DEPARTMENT OF JUSTICE, Defendant.

Subsequent History: Summary judgment granted by, Judgment entered by *ACLU v. DOJ, 2015 U.S. Dist. LEXIS 90672 (N.D. Cal., July 13, 2015)*

Prior History: *ACLU of N. Cal. v. DOJ, 70 F. Supp. 3d 1018, 2014 U.S. Dist. LEXIS 139273 (N.D. Cal., Sept. 30, 2014)*

Counsel: [*1] For American Civil Liberties Union of Northern California, Plaintiff: Linda Lye, Michael Temple Risher, LEAD ATTORNEYS, ACLU Foundation of Northern California, Inc., San Francisco, CA.

For Department of Justice, Defendant: Lynn Yuhee Lee, U.S. Dept. of Justice, Civil Division - Federal Programs Branch, Washington, DC.

Judges: MARIA-ELENA JAMES, United States Magistrate Judge.

Opinion by: MARIA-ELENA JAMES

Opinion

ORDER RE: CROSS-MOTIONS FOR SUMMARY JUDGMENT

Re: Dkt. Nos. 35, 36

INTRODUCTION

Plaintiff American Civil Liberties Union (the "ACLU") filed this lawsuit under the Freedom of Information Act ("FOIA"), *5 U.S.C. § 552*, seeking to compel the release of records concerning the federal Government's use of mobile tracking technology known as a cell site simulator[1] or "CSS." Compl. ¶ 1, Dkt. No. 1. Pending before the Court are the parties' cross-motions for summary judgment. Dkt. No. 35 ("Gov. Mot."); Dkt. No. 36 ("Pl. Mot."). Having considered the parties' positions, relevant legal authority, and the record in this case, the Court GRANTS IN PART and DENIES IN PART the Government's Motion and GRANTS IN PART and DENIES IN PART the ACLU's Motion for the reasons set forth below.

BACKGROUND

A. The FOIA Request and Stipulated Search Parameters

On April 11, 2013, the ACLU submitted a FOIA request to the United States Department of Justice's ("DOJ") Criminal Division and the Executive Office for United States Attorneys ("EOUSA") for records "pertaining to the federal government's use of mobile tracking technology commonly known as a StingRay but more generically known as an International Mobile Subscriber Identity or IMSI Catcher." Compl., Ex. 2; Sprung Decl., Ex. A, Dkt. No. 35-2. Specifically, the FOIA request sought the following:

> 1) Policies, procedures, practices, legal opinions, memoranda, briefs, correspondence (including e-mails) and training materials, template applications, template [*3] affidavits in support of applications, template proposed court orders or warrants, and any other document referencing or relating to IMSI catchers;
>
> 2) Policies, procedures, practices, legal opinions, memoranda, briefs, correspondence (including e-mails), training materials, and any other document referencing or relating to the Wireless Intercept and Tracking Team of the Federal Bureau of Investigation; and

[1] Cell site simulators, also known as "StingRays" (a brand name **[*2]** of one such device) or IMSI catchers (referring to the unique International Mobile Subscriber Identity number assigned to wireless devices), function by masquerading as the cellular phone towers used by wireless companies such as AT&T and T-Mobile. Lye Decl. ¶ 15, Dkt. No. 37, and Ex. 9, Dkt. No. 37-12. In doing so, they are used to identify each phone's unique numeric identifier and location, or capture the communications content of targets and bystanders alike. Lye Decl. ¶ 15.

> 3) All documents relating to the disclosure to the public and media coverage of [a] May 23, 2011 email attached to [plaintiff's request].

Id. The FOIA request also sought documents identified in response to an earlier FOIA request by Christopher Soghoian from August 1, 2011 (the "Soghoian Request"). *Id.* The ACLU asked for expedited processing of its request pursuant to 5 U.S.C. § 552(a)(6)(E) on the grounds that this matter is of "widespread and exceptional media interest" in which there exists "possible questions about the government's integrity which affect public confidence." *Id.*

On July 8, 2013, the ACLU filed the present suit, alleging that the Government had not yet provided a substantive response. Compl. ¶ 3. In a letter dated July 10, 2013, the DOJ granted the ACLU's request for expedited processing. [*4] Lye Decl. ¶ 2 & Ex. 18, Dkt. No. 37-15. The parties later enter into a stipulation regarding the scope and processing of the ACLU's request, with some documents to be processed by the EOUSA and others to be process by the Criminal Division. *See* Dkt. No. 14. Among other things, the stipulation did the following:

> • limited the search period to between January 1, 2008 and August 30, 2013;
>
> • limited the search for Parts 1-2 to "final policies, procedures and practices referencing or relating to either IMSI catchers or the Wireless Intercept and Tracking Team of the Federal Bureau of Investigation [FBI]" using agreed-upon search terms;
>
> • limited the search for Part 3 to "documents relating or referring to the disclosure to the public and media coverage pertaining to the May 23, 2011 email[;]"
>
> • provided that the Criminal Division would have its Computer Crime and Intellectual Property Section ("CCIPS") and Electronic Surveillance Unit ("ESU") search for responsive documents within its possession, custody, or control;
>
> • provided that EOUSA's FOIA unit would work with the Criminal Chiefs for the United States Attorney's Offices for ten specified federal districts, as well as the directors and [*5] deputy directors of certain other specified EOUSA component offices, to identify responsive documents within their possession, custody, or control; and
>
> • provided that the Government would process all documents identified in response to the Soghoian Request.

Id. at 2-4. Both the Criminal Division and EOUSA have confirmed that they searched for records in compliance with the stipulation, and the ACLU has not contended otherwise. *See* Sprung Decl. PP 11-20; Kornmeier Decl. ¶ 5.

B. The Government's Response

In December 2013, EOUSA disclosed one page and informed the ACLU that it was withholding 138 pages in full pursuant to *FOIA Exemptions 5*, *7(C)*, and *7(E)*. Kornmeier Decl.¶ 5 and Exs. A & B. The Criminal Division disclosed seven pages in part and informed the ACLU it was withholding 209 pages in full pursuant to *FOIA Exemptions 5*, *6*, *7(A)*, *7(C)*, *7(E)*, and *7(F)*. Sprung Decl. ¶ 24 and Ex. F.

In the course of briefing their motions for summary judgment, the parties exchanged additional information and some additional documents, narrowing the focus of their dispute as to the Criminal Division documents. *See generally* Suppl. Sprung Decl. & Suppl. Lye Decl. On February 3, 2015, the Court requested that the [*6] parties submit a joint statement clarifying the scope of the ACLU's remaining challenges. Dkt. No. 43. The Order also gave the Government an opportunity to submit additional declarations or evidence supporting asserted exemptions. *Id.* The ACLU was likewise given the opportunity to submit additional declarations as needed. *Id.*

The parties responded with a joint statement on March 3, 2015. Dkt. No. 46. The Government submitted an additional declaration in support of the Criminal Division documents, but stated that "with respect to the EOUSA templates, defendant rests on the *Vaughn* descriptions for these documents and the Declaration of John Kornmeier submitted with defendant's opening motion for summary judgment (ECF No. 35-1)." Jt. Stmnt. at 23.

As it stands, in the dispute with the EOUSA, the ACLU seeks two different set of legal templates described more fully below. *Id.* at 21-23. In the dispute with the Criminal Division, the issue is whether it should produce: (1) templates or "go-bys" relating to applications and proposed orders for authorization to use CSS and related technology; (2) legal guidance memoranda, including an email with an attached description of how CSS is utilized by law enforcement; (3) an excerpt [*7] from the USA Book, a DOJ agency manual; and (4) a sealed search warrant and supporting application and affidavit. *See id.* at 1-21.

C. Hearing and *In Camera* Review

On April 2, 2015, the Court held a hearing on this matter. Dkt. No. 50. Much of the parties' arguments involved comparing this case to a prior order in the related case, *Am. Civil Liberties Union of N. Cal. v. Dep't of Justice ("ACLU I"), F. Supp. 2d ,*

70 F. Supp. 3d 1018, 2014 U.S. Dist. LEXIS 139273, 2014 WL 4954277, at *9 (N.D. Cal. Sept. 30, 2014), which involved the same parties and a similar subject matter. The Government has appealed that Order. *See ACLU I*, No. 12-CV-04008-MEJ, 2014 U.S. Dist. LEXIS 139273, 2014 WL 4954277 (N.D. Cal.), Dkt. No. 66. At the hearing, the Court asked the parties whether they would consider staying this case pending the outcome of the related action. *See* Dkt. No. 50. The parties both agreed that they preferred a ruling on this case before the Court of Appeals decides *ACLU I. See id.*

The parties agreed, however, to allow the Government to submit the EOUSA documents as well as a sampling of the Criminal Division documents for the Court's *in camera* review. *Id.* Consequently, the Court ordered Documents 3 and 4 from the Kornmeier Declaration to be lodged with the Court, as well as the following documents from the Third Sprung Declaration: CRM-Lye-39451-39484 (only [*8] the portion containing the sealing order); CRM-Lye-2541 (USA Book); and internal memorandum at CRM-Lye-2948, CRM-Lye-3818-3825, CRM-Lye-9853-9897, CRM-Lye-15311-15316, CRM-Lye-28119-28126, CRM-Lye-34065-34066, and CRM-Lye-17543-17544. Dkt. No. 49. Additionally, the Court asked the Government to submit a list of documents that it proposed the Court should view as a representative sample of the Criminal Division templates. *Id.* The Court gave the ACLU the opportunity to respond if it believed that other or additional documents should be submitted. *Id.*

The Government submitted its proposed list on April 17, 2015. Dkt. No. 51. The ACLU did not file a response. Accordingly, the Court ordered that the Government lodge with the Court the documents it proposed on its list. Dkt. No. 52. This sample of documents includes the following: CRM-Lye-9002-9010; CRM-Lye-9011-9019; CRM-Lye-00015173-00015181; CRM-Lye-00015200-00015207; CRM-Lye-00031754-00031777; and CRM-Lye-00038268-00038270. *Id.* According to the Government, these documents are substantially similar to other withheld documents. *See* Dkt. No. 51 at 1-2 n.1-5. The Government has timely lodged all documents for the Court's *in camera* review. [*9] Now, having had the opportunity to conduct an *in camera* review of the above-referenced documents, the Court issues the following Order.

LEGAL STANDARD

A. The FOIA Statutory Scheme

FOIA's "core purpose" is to inform citizens about "what their government is up to." Yonemoto v. Dep't of Veterans Affairs, 686 F.3d 681, 687 (9th Cir. 2012) (quoting Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 773, 775, 109 S. Ct. 1468, 103 L. Ed. 2d 774 (1989)). This purpose is accomplished by "permit[ting] access to official information long shielded unnecessarily from public view and attempt[ing] to create a judicially enforceable public right to secure such information from possibly unwilling official hands." EPA v. Mink, 410 U.S. 73, 80, 93 S. Ct. 827, 35 L. Ed. 2d 119 (1973). Such access "ensure[s] an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." John Doe Agency v. John Doe Corp., 493 U.S. 146, 152, 110 S. Ct. 471, 107 L. Ed. 2d 462 (1989) (citation omitted). Congress enacted FOIA to "clos[e] the loopholes which allow agencies to deny legitimate information to the public." U.S. Dep't of Justice v. Tax Analysts, 492 U.S. 136, 150 (1989), 109 S. Ct. 2841, 106 L. Ed. 2d 112 (citations and internal marks omitted).

At the same time, FOIA contemplates that some information can legitimately be kept from the public through the invocation of nine "Exemptions" to disclosure. *See* 5 U.S.C. § 552(b)(1)-(9). "These limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act." Dep't of Interior v. Klamath Water Users Protective Ass'n, 532 U.S. 1, 7-8, 121 S. Ct. 1060, 149 L. Ed. 2d 87 (2001) (citation omitted). "Consistently with this purpose, as [*10] well as the plain language of the Act, the strong presumption in favor of disclosure places the burden on the agency to justify the withholding of any requested documents." United States Dep't of State v. Ray, 502 U.S. 164, 173, 112 S. Ct. 541, 116 L. Ed. 2d 526 (1991).

B. Summary Judgment Standard in FOIA Cases

"Summary judgment is the procedural vehicle by which nearly all FOIA cases are resolved." Nat'l Res. Def. Council v. U.S. Dep't of Def., 388 F. Supp. 2d 1086, 1094 (C.D. Cal. 2005) (quoting Mace v. EEOC, 37 F. Supp. 2d 1144, 1145 (E.D. Mo. 1999), *aff'd sub nom.* Mace v. EEOC, 197 F.3d 329 (8th Cir. 1999)). The underlying facts and possible inferences are construed in favor of the FOIA requester. *Id. at 1095* (citing Weisberg v. U.S. Dep't of Justice, 705 F.2d 1344, 1350, 227 U.S. App. D.C. 253 (D.C. Cir. 1983)). Because the facts are rarely in dispute in a FOIA case, the Court need not ask whether there is a genuine issue of material fact. Minier v. CIA, 88 F.3d 796, 800 (9th Cir. 1996).

The standard for summary judgment in a FOIA case generally requires a two-stage inquiry. *See* Animal Legal Def. Fund v. FDA, 2013 U.S. Dist. LEXIS 120417, 2013 WL 4511936, at *3 (N.D. Cal. Aug. 23, 2013). Under the first step of the inquiry, the Court must determine whether the agency has met its burden of

proving that it fully discharged its obligations under FOIA. *Zemansky v. EPA, 767 F.2d 569, 571 (9th Cir. 1985)* (citing *Weisberg, 705 F.2d at 1350-51*). In the second stage of the inquiry, the Court examines whether the agency has proven that the information that it withheld falls within one of the nine FOIA exemptions. *5 U.S.C. § 552(a)(4)(B)*; *Ray, 502 U.S. at 173* ("The burden remains with the agency when it seeks to justify the redaction of identifying information in a particular document as well as when it seeks to withhold an entire document."); [*11] *Dobronski v. FCC, 17 F.3d 275, 277 (9th Cir. 1994)*. When an agency chooses to invoke an exemption to shield information from disclosure, it bears the burden of proving the applicability of the exemption. *See Reporters Comm., 489 U.S. at 755*. An agency may withhold only that information to which the exemption applies, and must provide all "reasonably segregable" portions of that record to the requester. *5 U.S.C. § 552(b)(9)*; *see Mead Data Cent., Inc. v. Dep't of Air Force, 566 F.2d 242, 260, 184 U.S. App. D.C. 350 (D.C. Cir. 1977)*.

To carry their burden on summary judgment, "agencies are typically required to submit an index and 'detailed public affidavits' that, together, 'identify[ ] the documents withheld, the FOIA exemptions claimed, and a particularized explanation of why each document falls within the claimed exemption.'" *Yonemoto*, 686 F.3d at 688 (quoting *Lion Raisins v. Dep't of Agric., 354 F.3d 1072, 1082 (9th Cir. 2004)*) (modification in original). These submissions—commonly referred to as a *Vaughn* Index—must be from "affiants [who] are knowledgeable about the information sought" and "detailed enough to allow [a] court to make an independent assessment of the government's claim [of exemption]." *Id.* (citing *Lion Raisins, 354 F.3d at 1079*; *5 U.S.C. § 552(a)(4)(B)*). The government may also submit affidavits to satisfy its burden, but "the government 'may not rely upon conclusory and generalized allegations of exemptions.'" *Kamman v. IRS*, 56 F.3d 46, 48 (9th Cir. 1995) (quoting *Church of Scientology v. Dep't of the Army, 611 F.2d 738, 742 (9th Cir. 1980)*). The government's "affidavits must contain 'reasonably detailed descriptions of the documents [*12] and allege facts sufficient to establish an exemption.'" *Id.* (quoting *Lewis v. IRS, 823 F.2d 375, 378 (9th Cir. 1987)*). Courts "accord substantial weight to an agency's declarations regarding the application of a FOIA exemption." *Shannahan v. IRS, 672 F.3d 1142, 1148 (9th Cir. 2012)* (citing *Hunt v. CIA, 981 F.2d 1116, 1119-20 (9th Cir. 1992)*).

Finally, FOIA requires that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection." *5 U.S.C. § 552(b)*.

DISCUSSION

Because the parties have previously agreed upon the scope and methods of the DOJ's search for responsive documents, the only issue for the Court to decide on summary judgment is whether the Government properly withheld records under the FOIA exemptions. The Government contends that it is authorized to withhold documents under the following exemptions:

- *Exemption 5* (attorney work product privilege, attorney-client privilege, and deliberative process privilege)
- *Exemption 6* (private personnel and medical files)
- *Exemption 7* (law enforcement records or information)

In addition to these exemptions, the Government argues that (1) it may not disclose records courts have sealed in other cases, and (2) it has already produced all reasonably segregable portions of responsive records. The Court considers [*13] each of the documents at issue below.

A. Templates

Both the EOUSA and the Criminal Division withheld templates: the EOUSA withheld templates under *FOIA Exemption 5*, and the Criminal Division withheld templates pursuant to both *FOIA Exemptions 5* and *7(E)*.

1. EOUSA Templates

FOIA *Exemption 5* protects from disclosure "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." *5 U.S.C. § 552(b)(5)*. This provision essentially grants an agency the same power to withhold documents as it would have in the civil discovery context. *See NLRB v. Sears, Roebuck & Co., 421 U.S. 132, 149, 95 S. Ct. 1504, 44 L. Ed. 2d 29 (1975)*.

The EOUSA withheld the following documents on attorney work-product grounds: (1) a set of templates from the U.S. Attorney's Office ("USAO") for the Central District of California, consisting of (a) an Application for Use of an Electronic Serial Number Identifier, with a suggested memorandum of points and authorities and a proposed order, and (b) an Ex Parte Application for a Warrant Authorizing the Disclosure of GPS and Cell Site Information and Use of Mobile Electronic Device, with a request to seal the agent's declaration and the warrant (Kornmeier Decl., Ex. B at 2-3 ("Doc. #3")); and (2) [*14] a set of templates from the USAO for the Eastern District of Wisconsin consisting of an Application for a Warrant Authorizing the Disclosure of Data Relating to a Specified Cellular Telephone, with a warrant authorizing the disclosure

(*Id.* at 3-4 ("Doc. #4")).[2] The DOJ contends that these documents reflect the opinions and thought processes of attorneys "in the clear anticipation of serial litigation" and fall squarely within the definition of work product. Gov. Mot. at 8-9; Kornmeier Decl. PP 7-8; Ex. B at 2-4.

Attorney work-product protects "against disclosure of the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation" as well as "documents prepared in anticipation of litigation." *Fed. R. Civ. P. 26(b)(3)*. The purpose [*15] of this protection is to "protect[] the attorney's thought processes and legal recommendations from the prying eyes of his or her opponent." *In re EchoStar Commc'ns Corp., 448 F.3d 1294, 1301 (Fed. Cir. 2006)* (quotation and internal marks omitted), *cert. denied sub nom. TiVo, Inc. v. EchoStar Commc'ns Corp.*, 549 U.S. 1096, 127 S. Ct. 846, 166 L. Ed. 2d 665 (2006); *see also Hickman v. Taylor, 329 U.S. 495, 508, 67 S. Ct. 385, 91 L. Ed. 451 (1947)*. Importantly, "[i]f a document is fully protected as work product, then segregability is not required." *Judicial Watch, Inc. v. Dep't of Justice, 432 F.3d 366, 371, 369 U.S. App. D.C. 49 (D.C. Cir. 2005)* ("factual material is itself privileged when it appears within documents that are attorney work product"); *see also Tax Analysts v. IRS, 117 F.3d 607, 620, 326 U.S. App. D.C. 53 (D.C. Cir. 1997)* ("[a]ny part of [a document] prepared in anticipation of litigation, not just the portions concerning opinions, legal theories, and the like, is protected by the work product doctrine and falls under *exemption 5*."). "'In light of the strong policy of the FOIA that the public is entitled to know what its government is doing and why, *[E]xemption 5* is to be applied as narrowly as consistent with efficient Government operation.'" *Lahr v. Nat'l Transp. Safety Bd., 569 F.3d 964, 979 (9th Cir. 2009)* (quoting *Maricopa Audubon Soc'y v. U.S. Forest Serv., 108 F.3d 1089, 1093 (9th Cir. 1997)*), *cert. denied*, *561 U.S. 1007, 130 S. Ct. 3493, 177 L. Ed. 2d 1057 (2010)*.

The parties dispute whether EOUSA's withheld documents were "prepared in anticipation of litigation." The ACLU contends that the templates and proposed orders are not attorney work product because they do not pertain to any particular matter or specific case. Pl. Mot. at 12-13, 25. It argues that the Government offers no legal [*16] or factual basis to distinguish this case from *ACLU I*. In *ACLU I*, this Court considered whether template applications for court authorization to conduct electronic surveillance were protected as work product. 2014 U.S. Dist. LEXIS 139273, 2014 WL 4954277, at *7-10. The *ACLU I* templates were an "application and order for the use of a pen register and trap and trace device." 2014 U.S. Dist. LEXIS 139273, [WL] at *7. On review of the Government's supporting declarations and *Vaughn* Index, the Court concluded that the Government had not shown that these templates were protected as work product because there was no indication that they "provide legal theories or strategies for use in criminal litigation." 2014 U.S. Dist. LEXIS 139273, [WL] at *9. "Rather, they instruct government attorneys on how to apply for an order for location tracking information." *Id.; see also Judicial Watch, Inc. v. U.S. Dep't of Homeland Sec., 926 F. Supp. 2d 121, 143 (D.D.C. 2013)* ("While the memorandum may be, in a literal sense, 'in anticipation of litigation'—it simply does not anticipate litigation in the way the work-product doctrine demands, as there is no indication that the document includes the mental impressions, conclusions, opinions, or legal theories of . . . any [] agency attorney, relevant to any specific, ongoing or prospective case or cases.").

While the foregoing was the Court's primary basis for its opinion, [*17] it also found that the DOJ had "failed to establish that the template pertains to a specific claim or consists of more than general instructions to its attorneys with regard to applying for location tracking orders." *ACLU I*, 2014 U.S. Dist. LEXIS 139273, 2014 WL 4954277, at *10. Where government lawyers act "as legal advisors protecting their agency clients from the possibility of future litigation," the work product privilege may apply to documents advising the agency as to potential legal challenges. 2014 U.S. Dist. LEXIS 139273, [WL] at *9 (quoting *In re Sealed Case, 146 F.3d 881, 885, 330 U.S. App. D.C. 368 (D.C. Cir. 1998)*). But when government lawyers are acting as "prosecutors or investigators of suspected wrongdoers," the specific-claim test applies. *Id.* (citing *Coastal States Gas Corp. v. Dep't of Energy, 617 F.2d 854, 864-66, 199 U.S. App. D.C. 272 (D.C. Cir. 1980)* and *SafeCard Servs. Inc. v. SEC, 926 F.2d 1197, 1202-03, 288 U.S. App. D.C. 324 (D.C. Cir. 1991)*). As a result, the work product privilege only attaches to documents prepared "in the course of an active investigation focusing upon specific events and a specific possible violation by a specific party." 2014 U.S. Dist. LEXIS 139273, [WL] at *10 (quoting *Safecard, 926 F.2d at 1203* and citing *Judicial Watch, 926 F. Supp. 2d at 139-42*). The Court found that U.S. Attorneys act as prosecutors in utilizing these applications and orders, and not as attorneys advising an agency client on the agency's potential liability. *Id.* Consequently, the Court ultimately found that the documents the DOJ sought to withhold were not work product as they "set forth general legal standards, not an analysis

[2] The EOUSA also withheld a one-page email from an FBI Assistant General Counsel to an Assistant United States Attorney ("AUSA") in the District of Arizona regarding a criminal case, which discusses the best way to describe the use of a particular tracking technique in response to a question from the criminal defendant (Kornmeier Decl., Ex. B at 1-2 (Doc. #2)). The ACLU does not seek disclosure of this document. Pl. Mot. at 25.

[*18] of issues arising in 'identified litigation' or strategic decisions regarding any particular investigation." 2014 U.S. Dist. LEXIS 139273, [WL] at *10 n.5. The ACLU now urges the Court to adopt a similar holding here.

But the Court did not limit its holding to the degree the ACLU seeks. Specifically, the ACLU argues that the Court's earlier holding in *ACLU I* drew a distinction between "offensive and defensive postures" in determining whether the specific claim test applies. *See* Pl. Reply at 4, Dkt. No. 41. To the extent the ACLU reads the Court's holding this broadly, that was not the Court's intent. Importantly, in *ACLU I*, in addition to considering the "templates," the Court also considered whether certain internal memoranda were covered as attorney work product. The internal memoranda, like the templates here, were "prepared because of ongoing litigation and the prospect of future litigation" and were "intended to outline possible arguments and or litigation risks prosecutors could encounter" and to "assess the strengths and weaknesses of alternative litigating positions." 2014 U.S. Dist. LEXIS 139273, 2014 WL 4954277, at *11. Consequently, the Court found that the memoranda were protected as work product because they were "created to assist AUSAs with recurring litigation [*19] issues . . . that have arisen in current litigation." *Id.* The Court concluded that "[w]here, as here, the purpose of the documents is to convey litigation strategy, rather than convey routine agency policy, they are entitled to work product protection." *Id.* (citing *Am. Immigration Council v. U.S. Dep't of Homeland Sec., 905 F. Supp. 2d 206, 221 (D.D.C. 2012)*). As indicated, the primary concern in determining whether a document is protected as work product was and continues to be whether it was created in anticipation litigation in the way the work-product doctrine demands, i.e., by risking revealing mental impressions, conclusions, opinions, or legal theories of an agency attorney, relevant to any specific, ongoing, or prospective case or cases.

The Ninth Circuit has stated that "[t]o qualify for work-product protection, documents must: (1) be 'prepared in anticipation of litigation or for trial' and (2) be prepared 'by or for another party or by or for that other party's representative." *United States v. Richey, 632 F.3d 559, 567 (9th Cir. 2011)* (quoting *In re Grand Jury Subpoena, Mark Torf/Torf Envtl. Mgmt. ("Torf"), 357 F.3d 900, 907 (2004)*). *Torf* further elaborates that:

> [t]he "because of" standard does not consider whether litigation was a primary or secondary motive behind the creation of a document. Rather, it considers the totality of the circumstances and affords protection [*20] when it can fairly be said that the "document was created because of anticipated litigation, and *would not have been created in substantially similar form but for the prospect of that litigation* [.]"

Id. at 908 (quotation omitted; emphasis added). In concluding that the privilege applied on *Torf*'s facts, the Ninth Circuit stated that "[t]he documents are entitled to work product protection because, taking into account the facts surrounding their creation, their litigation purpose *so permeates any non-litigation purpose that the two purposes cannot be discretely separated* from the factual nexus as a whole." *Id.* at 910 (emphasis added); *see also City & Cnty. of Honolulu v. U.S. EPA, 2009 U.S. Dist. LEXIS 25621, 2009 WL 855896, at *9 (D. Haw. Mar. 27, 2009)* ("Under Ninth Circuit law, the test is whether the attorney would have generated the material 'but for' the prospect of litigation, though it is immaterial whether or when the litigation actually begins."); *Elkins v. D.C., 250 F.R.D. 20, 26 (D.D.C. 2008)* ("Plaintiffs argue that some documents were not prepared in anticipation of *this* litigation, *i.e.* they were prepared in anticipation of obtaining the search warrant and thus in anticipation of the administrative proceeding. But the doctrine protects documents prepared in anticipation of litigation; it does not have to be for this district court proceeding." [*21] (citations omitted; emphasis in original)).

This case presents a novel question in the work product realm as the Government's applications and proposed orders seek authorization to obtain and collect information that will be used in investigations of suspected criminals and that may ultimately lead to the prosecution of those individuals. According to the Government's supporting declaration, these templates were prepared in anticipation of "serial litigation." Kornmeier Decl., Ex. B at 2-4. They contain "specific research" by Government attorneys and those attorneys' "opinions and thought processes." *Id.* Specifically, the EOUSA's *Vaughn* Index entries for the withheld documents state in relevant part:

> Government attorneys, based on their research and analysis, have prepared this document as legal advice, in the clear anticipation of serial litigation. They contain specific research that the attorneys for the USAO think are pertinent to criminal litigation involving tracking devices. [They contain instructions for alternative situations.][3] These are the opinions and thought processes of attorneys in anticipation of litigation[.]

[3] This sentence was only included for Doc. #3, not Doc. #4.

Kornmeier Decl., Ex. B at 2-4.[4] The Government explains that [*22] "the templates were intended to assist prosecutors in anticipating and addressing potential legal risks and pitfalls in applying for the CSS." Gov. Reply at 6, Dkt. No. 40.

The actual purpose of the documents is to obtain the sought-after information, but the ultimate goal of that information is to use it towards the prosecution of alleged criminals. In that prosecution, a criminal defendant may challenge the Government's evidence through a motion to suppress, which in turn may implicate a number of the same factual and legal issues addressed in these [*23] withheld documents. In this sense, the Court cannot divorce the non-litigation purpose—i.e., simply procuring court authorization to obtain the suspected evidence—from the litigation purpose—i.e., forming the support for the criminal case and developing arguments to protect against attempts to prevent the acquired evidence's use. *See* Gen. Elec. Co. v. Johnson, 2006 U.S. Dist. LEXIS 64907, 2006 WL 2616187, at *11 (D.D.C. Sep. 12, 2006) ("a work-product assertion must be supported by some articulable, specific fact or circumstance that illustrates the reasonableness of a belief that litigation was foreseeable."). Put another way, there are two stages at which the Government must support that the evidence acquired can be used in criminal litigation: first, in applying for the authorization to obtain the evidence, and second, in defending a potential motion to suppress. In reviewing the *in camera* documents, the Government's legal analysis is geared toward the first stage but that same analysis could readily be applied later in the criminal litigation including on a motion to suppress. The litigation purpose and concerns in the later adversarial setting permeate the document's non-litigation purpose. Accordingly, the Court finds these documents protected as work product. *See also* Elkins, 250 F.R.D. at 26 (finding [*24] documents prepared in anticipation of obtaining a search warrant protected as work product).

Additionally, if a document is covered by the attorney work-product privilege, the Government need not segregate and disclose its factual contents. *See* 5 U.S.C. § 552(b); Maricopa Audubon Soc'y, 108 F.3d at 1092; Pac. Fisheries, Inc. v. United States, 539 F.3d 1143, 1148 (9th Cir. 2008). Having reviewed the *in camera* documents, and finding the legal analysis within closely tied to the facts of how this technology is used, the Court finds that the documents were created in whole in anticipation of litigation.

2. Criminal Division Templates

The Criminal Division also withheld templates under *Exemption 5* as protected by the attorney work product privilege,[5] as well as *Exemption 7(E)*. These templates include applications, agent affidavits, memorandums of law, and proposed orders for the use of a CSS and other investigative techniques. Second Sprung Decl. ¶ 27; Third Sprung Decl. ¶ 8.

The Government maintains that the templates withheld by the Criminal Division were prepared "in anticipation of specific [*25] litigation—to wit, a criminal prosecution in which evidence derived from a CSS was to be instrumental." Gov. Mot. at 18-19. It argues that the withheld materials are "litigation strategy documents that were provided by DOJ attorneys—frequently Criminal Division subject matter experts, addressing questions from prosecutors arising from specific cases—to advise prosecutors on the types of legal risks and challenges confronting them in applying for permission to use CSS." Gov. Reply at 8. "These documents anticipate a foreseeable prosecution of the individuals implicated in the investigation of the criminal activity in which the template will be used and are disseminated for the purpose of assisting prosecutors to defend subsequent motions to suppress filed by criminal defendants." Third Sprung Decl. ¶ 8; Sec. Sprung Decl. ¶ 27; *see also* First Sprung Decl. ¶ 42(h). "They are drafted or collected by Criminal Division legal advisors who are subject matter experts for the use of federal prosecutors who are working on active investigations." *Id.* (all). "The templates do not instruct government attorneys on how they must apply for location tracking information, although they do contain Criminal [*26] Division attorneys' interpretation of recent case law and reflect the strategies that prosecutors may use to obtain court authorization." *Id.* (all).

---

[4] *Compare ACLU I*, 2014 U.S. Dist. LEXIS 139273, 2014 WL 4954277, at *7, where *Vaughn* Index stated:

> These 16 pages were created by the U.S. Attorney's Office for the Northern District of California. The 16 pages are templates for an application and order for the use of a pen register and trap and trace device. The templates incorporate the interpretation of the law by the U.S. Attorney's Office and give advice on what information to include in particular situations. These templates represent the opinions of attorneys for the U.S. Attorney's Office on the applicable law and are prepared to provide legal advice and in anticipation of litigation[.]

[5] The Government previously asserted that these templates were protected by the deliberative process privilege, but the Government has withdrawn its claim to this privilege as to these documents. *See* Third Sprung Decl. at 4 n.1; *see also* Jt. Stmnt. at 1-14.

These descriptions parallel the Court's analysis above. Specifically, the Government uses these template applications, affidavits, memorandums of law, and proposed orders to secure court permission to utilize CSS and related technology, which results in the foreseeable prosecution of the individuals implicated in the investigation of the criminal activity. The templates also provide advice on the types of "legal risks" and challenges in applying for permission to use CSS and may later help prosecutors in defending subsequent motions to suppress. *See* Schiller v. NLRB, 964 F.2d 1205, 1208, 296 U.S. App. D.C. 84 (D.C. Cir. 1992)) (protecting an internal NLRB memorandum that "contain[ed] advice on how to build an [Equal Access to Justice Act] defense and how to litigate EAJA cases," as well as other documents that outlined instructions for preparing and filing pleadings, contained legal arguments, and identified supporting authorities), *abrogated on other ground by* Milner v. Dep't of the Navy, 562 U.S. 562, 131 S. Ct. 1259, 179 L. Ed. 2d 268 (2011). As with *ACLU I*'s legal memoranda, these documents reflect strategies, opinions, and advice that arise from "specific cases" and are used by attorneys working on "active [*27] investigations" and "foreseeable prosecution[s]." Third Sprung Decl. ¶ 8. In accordance with the Court's analysis above, and having reviewed these documents *in camera*, the Court finds the Criminal Division templates protected as work product under *Exemption 5*.

B. Memorandums

The Government also withheld a variety of legal memoranda and an email under various Exemptions described in turn below. *See* Third Sprung Decl. ¶¶ 9-15; Suppl. Lye Decl. ¶¶ 12-13.

1. Documents Withheld Under Exemptions 5 and 7(E)

First, several of the documents described as internal memorandum are substantially similar to the so-called "template" or "go-by" documents the Court found protected as attorney work product. According to that same analysis, and having conducted an *in camera* review of the following documents, the Court finds them protected as work product:

- **CRM-Lye-2948**, which contains "model language for federal prosecutors to include in a proposed order authorizing the use of a CSS by DEA and other law enforcement personnel under the PR/TT statute." Third Sprung Decl. ¶ 9.
- **CRM-Lye-9853-9897**, which contains "advice of CCIPS legal advisors for prosecutors to follow when seeking court-authorization to use Title III and [*28] PR/TT orders authorizing the use of location tracking information in various scenarios arising in criminal investigations." *Id.* ¶ 11. "The document describes how the Government may obtain location tracking information, what types of information is available from wireless providers, when emergency authorization is available, what kind of legal process is required under various circumstances, notification requirements, and extraterritorial jurisdiction issues." *Id.* The document also includes with it "template applications and proposed orders for using each of the various technologies, and contains links for consent forms, model pleadings and briefs, selected court opinions, and training materials." *Id.* "Access to these materials is restricted to prosecutors and Criminal Division attorneys via the CCIPS intranet site." *Id.*
- **CRM-Lye-34065-34066** "contains advice of legal advisors in the Criminal Division for prosecutors to follow when handling kidnapping cases, including how to seek emergency authorization to engage in electronic surveillance and to use location tracking technologies when time is of the essence." *Id.* ¶ 14.
- **CRM-Lye-15311-15316 and CRM-Lye-19179-19184** are "copies of template [*29] applications and proposed orders for federal prosecutors to use when seeking court-authorization to use a CSS under the PR-TT statute. They also include cover memorandum from the Associate Director of the Criminal Division's Office of Enforcement Operations that describes the technology and provides legal guidance concerning what kinds of information may lawfully be obtained." *Id.* ¶ 12. The Government withheld these documents under *Exemption 5* as attorney work product. *Id.*[6]

A review of these documents reveals that they were prepared in contemplation of issues arising in future litigation, and as such, the Court finds that a litigation purpose permeates these documents. Accordingly, *Exemption 5* applies and these documents are properly withheld.

However, second, the Government has not demonstrated that the following documents are protected as attorney work product:

- **CRM-Lye-3818-3825, CRM-Lye-23249-23256, CRM-Lye-33358-33365** are "copies of a document containing advice of legal advisors [*30] in the Criminal Division for AUSAs to follow when seeking court-authorization to utilize different location tracking

[6] Additionally, the Government withheld the documents under ***Exemptions 6*** and *7(C)* for "reveal[ing] the name and other personal information of the Associate Director for the Criminal Division's OEO." Third Sprung Decl. ¶ 12.

technologies for wireless devices in various scenarios in particular criminal investigations." *Id.* ¶ 10. The document "discusses legal requirements, procedures to be followed, when an individual's consent may be used in lieu of a court order, and a description of the underlying technologies." *Id.*

• **CRM-Lye-28119-28126** is "a collection and analysis of technical terminology, legal authorities, and internal DOJ procedures prepared for the purpose of assisting federal prosecutors and law enforcement agents concerning various types of electronic surveillance used in criminal investigations, including location tracking technologies for wireless devices." *Id.* ¶ 13.

According to the Government, all the documents described above "were prepared because the Department of Justice was conducting a criminal prosecution or anticipating doing so" and were created "to assist the Department in prosecutions and investigations." *Id.* ¶ 16.

But the Government has not shown how these documents were prepared in anticipation of litigation in the way the work product doctrine contemplates. Rather [*31] the documents provide instructions to government attorneys about how they might seek to use the technology in various circumstances. In other words, they instruct government attorneys on how they must apply for location tracking information. *Compare ACLU I*, 2014 U.S. Dist. LEXIS 139273, 2014 WL 4954277, at *9 (finding no attorney work product where the Government's *Vaughn* Index and related affidavits established only that the documents "instruct[ed] government attorneys on how to apply for an order for location tracking information."). Nothing about these documents or their supporting declarations demonstrates that a litigation purpose permeates these documents. Rather, the first set of documents provides instructions about how to obtain authorization for use of the technology, functioning more like an agency manual rather than revealing mental impressions. And the second set of documents contains a list of terms, regurgitating statutory definitions and, in some cases, dictionary definitions, with no indication that the disclosure of such a document would reveal mental impressions that would be detrimental or prejudicial in the adversarial process. Accordingly, the Court cannot find these documents protected as work product.

The question then is whether [*32] they are protected by *Exemption 7(E)*. FOIA *Exemption 7* permits the government to withhold "records or information compiled for law enforcement purposes" under certain enumerated conditions. *5 U.S.C. § 552(b)(7)*. Particularly, *Exemption 7(E)* provides that "records or information compiled for law enforcement purposes" may be withheld if they "would disclose techniques and procedures for law enforcement investigations or prosecutions." *Id.* However, "*Exemption 7(E)* only exempts investigative techniques not generally known to the public." *Rosenfeld v. Dep't of Justice, 57 F.3d 803, 815 (9th Cir. 1995)*. The Government may also withhold detailed information regarding a publicly known technique where the public disclosure did not provide "a technical analysis of the techniques and procedures used to conduct law enforcement investigations." *See Bowen v. U.S. Food & Drug Admin., 925 F.2d 1225, 1228-29 (9th Cir 1991)*; *see also Elec. Frontier Found. v. Dep't of Defense, 2012 U.S. Dist. LEXIS 137010, 2012 WL 4364532, at *4 (N.D. Cal., Sep. 24, 2012)*. "[T]he government must show, by evidence admissible on summary judgment, that release of the withheld information 'would reasonably be expected to risk circumvention of the law.'" *2012 U.S. Dist. LEXIS 137010, [WL] at *3* (quoting *5 U.S.C. § 552(b)(7)(E)*).

The threshold test under *Exemption 7* is whether the documents have a law enforcement purpose, which requires an examination of whether the agency serves a "law enforcement function." *Church of Scientology Int'l v. IRS, 995 F.2d 916, 919 (9th Cir. 1993)* (internal citation and quotation marks omitted). [*33] In order to satisfy *Exemption 7*'s threshold requirement, a government agency with a clear law enforcement mandate "'need only establish a rational nexus between enforcement of a federal law and the document for which [a law enforcement] exemption is claimed.'" *Rosenfeld, 57 F.3d at 808* (internal citation omitted). There is no dispute here that the DOJ has a clear law enforcement mandate and the two documents as to which the Criminal Division asserts law enforcement exemptions bear a rational nexus to enforcement of federal law.

The Government, however, provides little explanation as to how the disclosure of any of the documents above "could reasonably be expected to risk circumvention of the law." *5 U.S.C. § 552(b)(7)(E)*. The Government presents two primary arguments as to why *Exemption 7(E)* applies to the materials it has withheld. First, it argues in a footnote that *Exemption 7(E)* is best interpreted as providing categorical protection to materials describing "techniques and procedures" while its inquiry into whether "disclosure could reasonably be expected to risk circumvention" applies only to "guidelines." Gov. Reply at 7 n.4; *see also 5 U.S.C. § 552(b)(7)(E)*. As the withheld materials relate to techniques and procedures, presumably—by the Government's [*34] logic—these materials would be categorically protected and properly withheld. In support, the DOJ cites *Asian Law Caucus v. U.S. Dep't of Homeland Sec., 2008 U.S. Dist. LEXIS 98344, 2008 WL 5047839, at *3 (N.D. Cal. Nov. 24, 2008)*, which found that the Ninth Circuit had yet to "squarely address" the distinction between guidelines and techniques and procedures, but ultimately did not rule on whether categorical protection existed as to techniques and

procedures. With respect to that court's finding, the Court agrees with the ACLU that the Ninth Circuit's holding in *Rosenfeld* "adopted [] as the law of this Circuit," that "*Exemption 7(E)* only exempts investigative techniques not generally known to the public." *Rosenfeld, 57 F.3d at 815*. This holding establishes that techniques and procedures are not categorically withheld under *Exemption 7(E)*. *See id.* & n.9. The Court sees no cause to distinguish the Ninth Circuit's holding here.

Second, the Government argues that the information it seeks to protect "goes beyond" the known fact that the government can and does track individuals using CSS and instead provides "particularized detail on what tactics and factors DOJ attorneys take into account in deciding whether, how, and when to use CSS—information that could assist unlawful actors in evading detection." Gov. Reply at 7. However, several [*35] courts, including this one, have found inadequate an agency's conclusory assertions that *Exemption 7(E)* protects specifics about how and when the technique at issue is used if the technique itself is otherwise generally known to the public. *See Rosenfeld, 57 F.3d at 815* (holding that the government "simply by saying that the 'investigative technique' at issue is not the practice but the application of the practice to the particular facts underlying that FOIA request" cannot be adequate under *Exemption 7(E)* because otherwise it would prove too much); *Am. Civil Liberties Union v. FBI, 2013 U.S. Dist. LEXIS 93079, 2013 WL 3346845, at *9 (N.D. Cal. July 1, 2013)* ("The FBI's conclusory assertion that, even though the technique is generally known, the specifics on how and when the technique is used is not generally known, is not adequate."); *Feshbach v. SEC, 5 F. Supp. 2d 774, 787 (N.D. Cal. 1997)* (rejecting *Exemption 7(E)* withholding where government failed to "provide non-conclusory reasons why disclosure of each category of withheld documents would risk circumvention of the law."); *ACLU I*, 2014 U.S. Dist. LEXIS 139273, 2014 WL 4954277, at *15 (*Exemption 7(E)* unavailable where declarations "set forth only conclusory statements that the public is not aware of the specifics of how or when the techniques are used, but do not state that the techniques are not generally known to the public."). This is not to suggest a categorical exception [*36] to *Exemption 7(E)*; in other words, the fact that the technique is generally known will not make specific applications of that technique or procedure always subject to disclosure. But the Government cannot rely on conclusory assertions to show that release of the withheld information risks circumventing of the law. "*Exemption 7(E)* requires that the agency demonstrate logically how the release of the requested information might create a risk of circumvention of the law." *Am. Civil Liberties Union v. FBI, 2014 U.S. Dist. LEXIS 130501, 2014 WL 4629110, at *11 (N.D. Cal. Sept. 16, 2014)* (citing *Mayer Brown LLP v. IRS, 562 F.3d 1190, 1194, 385 U.S. App. D.C. 250 (D.C. Cir. 2009)*).

The ACLU has put forward substantial evidence—including evidence the DOJ itself had made public—that the techniques and procedures relating to the use of cell site simulators is generally known to the public. *See* Lye Decl., Ex. 1 (Electronic Surveillance Issues) at 151, 153; Ex. 2 (Electronic Surveillance Manual) at 40[7], 48; Ex. 4 (Electronic Surveillance Manual Chapter XIV, dated August 21, 3013, entitled "Cell Site Simulators/Digital Analyzers/Triggerfish"). CSS and its use by the federal government has also been the subject of extensive news coverage. Lye Decl. ¶¶ 12, 13, & Exs. 6-7 (dozens of news articles about the government's use of CSS). The public domain evidently contains enough information about the technology behind CSS that members of the public have actually created their [*37] own CSS devices. Lye Decl. ¶ 16, Ex. 10. This evidence demonstrates that the public in general knows that the government possesses and utilizes such cell phone technology in its investigations to locate and obtain information about the cell-phone holder. The Government has not distinguished this case from *ACLU I*, for instance by addressing "the fact that the public is already aware that minimizing vehicular or cell phone usage will allow them to evade detection." *ACLU I*, 2014 U.S. Dist. LEXIS 139273, 2014 WL 4954277, at *14. Thus, as in *ACLU I*, "[t]o the extent that potential law violators can evade detection by the government's location tracking technologies, that risk already exists." *Id.* And for that matter, the ACLU has presented evidence that the public already has tools that can detect CSS. Lye Decl. ¶ 17, Ex. 11.

Of course, that is not to say that the mere existence of an already present risk or threat to effectiveness of the Government's investigative techniques is enough, alone, to make *Exemption 7(E)* inapplicable. However, where, as here, the Government provides only conclusory statements showing no distinct risk associated with the disclosure of documents it seeks to withhold, [*38] application of *Exemption 7(E)* is improper. *Rosenfeld, 57 F.3d at 815* ("It would not serve the purposes of FOIA to allow the government to withhold information to keep secret an investigative technique that is routine and generally known."); *compare Bowen, 925 F.2d at 1228-29* (government may withhold detailed information regarding a publicly known technique where the public disclosure provides "a technical analysis of the techniques and procedures used to conduct law enforcement investigations."); *Asian Law Caucus, 2008 U.S. Dist. LEXIS 98344, 2008 WL 5047839, at *4* (while use of watchlists to screen travelers was a matter of common knowledge, government could withhold information about the operation of those lists, which was not generally known or understood by the

[7] *See* Dkt. No. 48 for page 40 of the Electronic Surveillance Manual.

public). Unlike *Bowen* and *Asian Law Causus*, the Government has not provided any indication, other than conclusory statements, that the withheld documents contain information that "goes beyond" what is already generally available to the public. The Government bears the burden of demonstrating that the material is exempt from disclosure, but its current evidence—including the supplemental declaration ordered by the Court and the *in camera* documents—fails to provide the necessary support to meet its burden. *See Maricopa Audubon Soc'y, 108 F.3d at 1092* ("To meet its burden, the agency [*39] must offer oral testimony or affidavits that are 'detailed enough for the district court to make a de novo assessment of the government's claim of exemption.'" (citation omitted)). Even reviewing these documents *in camera*, the Court cannot say that they reveal more than what is generally available to the public or that they risk circumvention of the law such that the application of *Exemption 7(E)* is required.

2. Email Withheld Under Exemptions 5, 6, and 7.

The Government also argues that it properly withheld the following document:

> • **CRM-Lye-17543-17544**, "an email message dated August 22, 2012 from an ESU attorney to another Criminal Division attorney containing the Criminal Division's legal advice on how law enforcement may use its own equipment to obtain location information for a particular wireless device." Third Sprung Decl. ¶ 15. "The email describes the technology, what type of legal process is necessary, and what type of information the device can gather." *Id.* The government withheld the email under the attorney work product, the deliberative process, and the attorney-client privileges of *Exemption 5*, as well as *Exemptions 6* and *7(C)*. *Id.*

The *Vaughn* Index describes this document [*40] as "**EMAIL. *Subject***: N/A ***Re***: Attached description and guidance on how cell site simulators and related technologies are utilized and implemented by law enforcement." *Vaughn* Index at 134, Dkt. No. 35-7; Jt. Stmnt. at 21. While the Government contests release of this document under several exemptions, it also acknowledges that the document "excerpts test of a document in the public domain, which has been released to Plaintiff." Third Sprung Decl. ¶ 15.

Theoretically what remains for this Court's review is the non-public portion, but it is not evident which portion of the document the Government has continued to withhold. For clarity, the Government shall file a declaration following this Order indicating which portion of the document is non-public and presently withheld. The Court will issue an order regarding this email following its review of that declaration.

C. USA Book

The Government describes withheld document CRM-Lye-2541 as a page from USA Book on cell site simulators, Triggerfish, and cell phones, which "describes the underlying technology, discusses the legal basis for its use, identifies certain of the unique capacities of a CSS that present significant litigation risk, names the ESU attorney who is a legal expert [*41] on the subject, and references other relevant DOJ legal resources." Suppl. Sprung Decl. ¶ 26; Third Sprung Decl. ¶ 7. The Index describes it as "USA Book, Electronic Surveillance, Cell Site Simulators, Triggerfish, Cell Phones Re: Description of the technology." Jt. Stmnt. at 1. The Government asserts that it properly withheld this document under the attorney work product of *Exemption 5*. Third Sprung Decl. ¶ 7; Jt. Stmnt. at 1.

The Government provides no grounds for why CRM-Lye-2541 is protectable as such. First, its supporting declarations provide no indication that the material was prepared in anticipation of litigation. While the Third Sprung Declaration indicates that this document contains the "legal basis" for the CSS's use, names an expert attorney on the subject, and refers to legal resources, there is no indication that any part of this document was created in anticipation of litigation, either current or prospective. The *Vaughn* Index itself provides little explanation other than that the document contains a "description of the technology." *See* Jt. Stmnt. at 1. This does not show anything connecting the document to attorney work product. Nothing in the government's evidence shows that disclosure of this page from the [*42] USA Book threatens the attorney work product protection's aim of "protect[ing] the attorney's thought processes and legal recommendations from the prying eyes of his or her opponent." *In re EchoStar, 448 F.3d at 1301*; *see also Hickman, 329 U.S. at 508*.

Second, having reviewed this document *in camera*, the Court finds nothing that would be protected as work product. There is no indication that this page of the USA Book was prepared in anticipation of litigation or that its "litigation purpose so permeates any non-litigation purpose that the two purposes cannot be discretely separated from the factual nexus as a whole." *Torf*, 357 F.3d at 910. The document informs government officials about the technology, its legal basis, and which resources are available in the event the technology is needed, but there is nothing that demonstrates this document was created in anticipation of litigation in the way the work product doctrine contemplates.

As the Government only sought protection of this document under *Exemption 5*, the Court cannot find that this document is entitled to exemption.

D. Sealed Documents

The parties' final dispute concerns CRM-Lye-39451-39484, which contains a search warrant issued by the U.S. District Court for the Central District of California, a supporting *ex parte* [*43] application and agent affidavit, and a sealing order authorizing the use of CSS in a particular investigation. Third Sprung Decl. ¶ 6. Previously, the ACLU asserted that the "DOJ should be ordered to produce the search warrant and supporting application and affidavit unless it submits a declaration averring that the investigation at issue remains active." Pl. Reply at 14. The Government's latest declaration states that "the underlying investigation has concluded and that none of the subjects of the investigation were charged." Third Sprung Decl. ¶ 6. Nevertheless, the matter "remains under seal." *Id.* According to the Government, "[t]he documents were properly withheld because the language of the sealing order indicates that it was intended to preclude disclosure while the seal remains in effect and therefore the DOJ has no discretion to release the documents in this matter." *Id.*[8]

"[T]he mere existence of a court seal is, without more, insufficient to justify nondisclosure under the FOIA. Instead, only those sealing orders intended to operate as the functional equivalent [*44] of an injunction prohibiting disclosure can justify an agency's decision to withhold records that do not fall within one of the specific FOIA exemptions." *Concepcion v. FBI, 699 F. Supp. 2d 106, 111 (D.D.C. 2010)* (quoting *Morgan v. United States, 923 F.2d 195, 199, 287 U.S. App. D.C. 372 (D.C. Cir. 1991)*; *cf. GTE Sylvania, Inc. v. Consumers Union of the U.S., Inc., 445 U.S. 375, 387, 100 S. Ct. 1194, 63 L. Ed. 2d 467 (1980)*. The agency bears "the burden of demonstrating that the court issued the seal with the intent to prohibit the [agency] from disclosing the [document] as long as the seal remains in effect." *Id.* (quoting *Morgan, 923 F.2d at 198* (alterations in original)). The Government can demonstrate intent through "(1) the sealing order itself; (2) extrinsic evidence, such as transcripts and papers filed with the sealing court, casting light on the factors that motivated the court to impose the seal; (3) sealing orders of the same court in similar cases that explain the purpose for the imposition of the seals; or (4) the court's general rules or procedures governing the imposition of seals." *Morgan, 923 F.2d at 198* (footnote omitted).

Having reviewed the sealing order itself,[9] the Court finds that there is no evidence that it was intended to operate as the functional equivalent of an injunction. The sealing order was originally a proposed order submitted by the Government and adopted and signed by the court. It provides that the document is kept under seal until the Government [*45] notifies the court that it is appropriate to unseal the documents. Accordingly, the Government's assertion that the court intended the documents to remain sealed is inconsistent with the Order that for all intents and purposes allows the Government to decide when to unseal those documents.

Additionally, as the Government admits that the investigation related to these materials has concluded, the common law right of access applies. *See United States v. Bus. of Custer Battlefield Museum & Store Located at Interstate 90, Exit 514, S. of Billings, Mont., 658 F.3d 1188, 1194 (9th Cir. 2011)* (holding that "the public has a qualified common law right of access to warrant materials after an investigation has been terminated."). "When the common law right of access applies to the type of document at issue in a particular case, a 'strong presumption in favor of access' is the starting point" and the party seeking to restrict access to the document "bears the burden of overcoming this strong presumption by . . . 'articulat[ing] compelling reasons' . . . that outweigh the general history of access and the public policies favoring disclosure." *Id. at 1194-95* (citations and internal marks omitted). The [*46] Government has not argued that any such compelling reasons exist as to why maintaining the secrecy of these documents outweighs the public policy favoring disclosure.

However, the Government has raised concerns that these documents "contain the names and other personal information about the subjects, as well as personal information about the prosecutor and agent and a third party/witness victim." Third Sprung Decl. ¶ 6. As such, the DOJ asserts that the documents are properly withheld under *Exemption 6* and *Exemption 7(C)*. *Id.*

Exemption 7(C) permits withholding of "records or information compiled for law enforcement purposes" to the extent that their production "could reasonably be expected to constitute an unwarranted invasion of personal privacy." *5 U.S.C. § 552(b)(7)(C)*. Such information is protected from disclosure unless "the public interests in disclosing the *particular* information requested outweigh those privacy interests." *Yonemoto*, 686 F.3d at 694 (emphasis in original). *Exemption 6* is similar but distinct from *Exemption 7(C)*; specifically, *Exemption 6* provides that an agency may withhold "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." [*47] *5 U.S.C. § 552(b)(6)*; *see Yonemoto*, 686 F.3d at 693 n.7. The Court is thus required "to protect, in the proper degree, the personal privacy of citizens against the uncontrolled release of

[8] The Government does not assert that these documents contain materials covered under the Pen Register Statute (18 U.S.C. § 3123(d)) or Title III (18 U.S.C. § 2518(8)(b)).

[9] The Court reviewed only the sealing order, not any of the related documents.

information." *Lane v. Dep't of the Interior, 523 F.3d 1128, 1137 (9th Cir. 2008)*. The Court must "balance the public interest in disclosure against the [privacy] interest Congress intended the Exemption to protect." *Reporters Comm., 489 U.S. at 776*; *Forest Serv. Emps. for Envtl. Ethics v. U.S. Forest Serv., 524 F.3d 1021, 1025 n.2 (9th Cir. 2008)*.

The Government's arguments do not support that *Exemption 6* or *7(C)* should be used to withhold these documents in their entirety. Rather, the more appropriate solution under these Exemptions is to disclose the documents and redact the personal information of the persons described in those documents. Accordingly, the Government will produce the documents at CRM-Lye-39451-39484, redacted in accordance with this Order.

CONCLUSION

Based on the analysis above, the DOJ's Motion for Summary Judgment is **GRANTED IN PART** and **DENIED IN PART** and the ACLU's Motion for Summary Judgment is **GRANTED IN PART** and **DENIED IN PART**. The Government properly withheld under *Exemption 5* the following documents: (1) EOUSA Docs. #3 and #4; (2) Criminal Division internal memoranda, CRM-Lye-2948; CRM-Lye-9853-9897; CRM-Lye-34065-34066; CRM-Lye-15311-15316; CRM-Lye-19179-19184; and (3) Criminal Division templates, CRM-Lye-9002-9010; [*48] CRM-Lye-9011-9019; CRM-Lye-00015173-00015181; CRM-Lye-00015200-00015207; CRM-Lye-00031754-00031777; CRM-Lye-00038268-00038270. However, the Government must produce CRM-Lye-39451-39484 (sealing order, warrant, and application); CRM-Lye-2541 (USA Book); CRM-Lye-3818-3825, CRM-Lye-23249-23256, CRM-Lye-33358-33365, and CRM-Lye-28119-28126 (internal memoranda). The Government must also file a declaration by June 24, 2015, indicating which portion of CRM-Lye-17543-17544 (email) is non-public and presently withheld.

IT IS SO ORDERED.

Dated: June 17, 2015

/s/ Maria-Elena James

MARIA-ELENA JAMES

United States Magistrate Judge

B

Korn v. Wagner

Court of Chancery of Delaware

September 1, 2011, Submitted; September 7, 2011, Decided

C.A. No. 6149-VCN

Reporter
2011 Del. Ch. LEXIS 130; 2011 WL 4357244

RICHARD KORN, Plaintiff, v. STATE OF DELAWARE AUDITOR OF ACCOUNTS R. THOMAS WAGNER, JR. IN HIS OFFICIAL CAPACITY AS STATE AUDITOR, Defendant.

Notice: THIS OPINION HAS NOT BEEN RELEASED FOR PUBLICATION. UNTIL RELEASED, IT IS SUBJECT TO REVISION OR WITHDRAWAL.

Subsequent History: Related proceeding at *Korn v. State, 2012 Del. Super. LEXIS 471 (Del. Super. Ct., Sept. 28, 2012)*

Counsel: [*1] Ronald G. Poliquin, Esquire, The Law Firm of Ronald G. Poliquin, P.A., Dover, Delaware, Attorney for Plaintiff.

Frank N. Broujos, Esquire and Judy Oken Hodas, Esquire, Department of Justice, Wilmington, Delaware, Attorneys for Defendant.

Judges: NOBLE, Vice Chancellor.

Opinion by: NOBLE

Opinion

MEMORANDUM OPINION

NOBLE, Vice Chancellor

I. BACKGROUND[1]

Plaintiff Richard Korn is a Delaware taxpayer residing in Wilmington, Delaware. Defendant R. Thomas Wagner, Jr., is the State of Delaware Auditor of Accounts. The Plaintiff asserts claims against the Defendant based upon two distinct sets of factual circumstances. The first group of claims relates to the Defendant's alleged noncompliance with *29 Del. C. § 2906(f)*, which states, in part, that the "Auditor of Accounts shall conduct postaudits of local school district tax funds budget and expenditures annually." The Defendant conducted these audits annually from the time of his appointment in 1989 through 2002. The Defendant stopped conducting these audits annually in 2003, and, again according to the Plaintiff, as a result, theft and fraud of approximately $49,000,000 [*2] at several school districts went undetected. Second, the Plaintiff alleges that the Defendant violated Delaware's Freedom of Information Act [2] ("FOIA") by failing to provide the Plaintiff with copies of Office of the Auditor employee time sheets which he duly requested.

II. CONTENTIONS

The Plaintiff seeks, first, a declaratory judgment that Defendant's failure to perform annual local school district compliance audits is a violation of *29 Del. C. § 2906(f)*, and, second, preliminary and permanent injunctions directing the Defendant to perform these audits annually (the "Audit Claims"). Additionally, the Plaintiff requests a declaratory judgment that the Defendant's failure to furnish the requested timesheets is a violation of FOIA, together with an injunction and a writ of mandamus directing the Defendant to disclose the timesheets (the "FOIA Claims"). The Defendant contends that dismissal of the Complaint is appropriate under Court of Chancery Rules 12(b)(1) and 12(b)(6) for lack of subject matter jurisdiction and for failure to state a claim upon which relief may be granted. [3]

III. ANALYSIS

A. *Audit Claims*

The Defendant argues that the Audit Claims must be dismissed because this Court lacks the subject matter jurisdiction necessary

---

[1] The factual background is based on allegations in the first amended verified complaint (the "Complaint").

[2] *29 Del. C.* ch. 100.

[3] Before oral argument, the Defendant agreed to waive the previously raised defense that the **[*3]** Plaintiff's claim should be dismissed under Court of Chancery Rule 12(b)(5) for insufficient service of process.

to adjudicate them. The Court of Chancery is a court of limited jurisdiction and lacks subject matter jurisdiction where there is an adequate remedy at law. [4] The primary issue at the core of the Audit Claims is one solely of statutory interpretation, simple as this interpretation may be. Such issues "are, beyond question, legal issues capable of resolution by the Superior Court, and declaratory relief is available to the same extent as it is [in the Court of Chancery]." [5]

Since declaratory relief of the type sought here could be obtained, if at all, [6] in the Superior Court, there is an adequate remedy at law for both the Plaintiff's declaratory judgment claim and injunction claims. Clearly the availability of a declaratory judgment [*4] from the Superior Court suffices as an adequate legal remedy for the Plaintiff's declaratory relief claim. Furthermore, despite the Plaintiff's protestations to the contrary, [7] a declaratory judgment is an adequate legal remedy for the Plaintiff's injunction claims. [8] Declaratory judgments "are self executing and 'have the force and effect of a final judgment or decree.'" [9] Additionally, aside from a conclusory allegation, [10] nothing in the Complaint alleges or suggests the Defendant, an elected State official, would act in defiance of a Superior Court order.

Since an adequate legal remedy is available for all of the Plaintiff's Audit Claims, this Court lacks subject matter jurisdiction over them. Accordingly, the Audit Claims will be dismissed but may be transferred to the [*7] Superior Court in accordance with *10 Del. C. § 1902*.

B. *FOIA Claims*

The Plaintiff alleges that the Defendant violated *29 Del. C. § 10003* by refusing to provide the Plaintiff with the requested time sheets. The Defendant argues that the Plaintiff has failed to exhaust available administrative remedies, and the Plaintiff acknowledges that dismissal on this ground is appropriate.

Under *29 Del. C. § 10005*, a citizen alleging a FOIA violation must seek an administrative review before filing suit in court when the Attorney General is obligated to represent the public body with the sought-after public records pursuant to *29 Del.*

---

[4] 10 *Del. C.* § 342.

[5] *Reeder v. Wagner*, 2007 Del. Ch. LEXIS 149, 2007 WL 3301026, at *1 (Del. Ch. Nov. 1, 2007); *Reed v. Brady*, 2002 Del. Ch. LEXIS 83, 2002 WL 1402238, at *3 n. 7 (Del. Ch. June 21, 2002), *aff'd*, ***818 A.2d 150 (Del. 2003)*** (TABLE).

[6] Beyond the issue of this Court's jurisdiction is the question of whether the Plaintiff has standing to bring these claims. The Plaintiff asserts both individual and taxpayer standing in the Complaint. A plaintiff suing as a citizen must show that he or she "suffered an injury in fact — an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) there must be a causal connection between the injury and the conduct complained of — the injury has to be fairly traceable to the challenged action of the defendant and not the result of the independent **[*5]** action of some third party not before the court; and (3) it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Dover Historical Soc. v. Dover Planning Comm'n*, 838 A.2d 1103, 1110 (Del. 2003) (quoting *Society Hill Towers Owners' Ass'n v. Rendell*, 210 F.3d 168, 175-76 (3d Cir. 2000)). Generally, a plaintiff must prove that his or her interest in the controversy is different from the interest of the public at large. *See Stuart Kingston, Inc. v. Robinson*, 596 A.2d 1378, 1382 (Del. 1991).

The Plaintiff's allegations appear to fall short of this standard. For instance, the Plaintiff has not alleged he has suffered any unique harm as result of the alleged misconduct that is distinguishable from the harm suffered by the general public. Furthermore, the alleged harm, theft of school district funds, is remote from the alleged misconduct. There are no allegations that the Defendant participated in any fraud or theft. At best, an audit performed after money has been spent *may* detect or deter theft, or *may* lead to a recovery of misappropriated funds, though the extent to which it will succeed in any of these aims is unknowable. For this **[*6]** same reason, it appears speculative that the alleged injury would be redressed by a decision in the Plaintiff's favor.

In Delaware, taxpayer standing is "reserved for a narrow set of claims involving challenges either to expenditures of public funds or use of public lands." *Reeder v. Wagner*, 974 A.2d 858, 2009 WL 1525945, at *2 (Del. 2009) (TABLE) (quoting *O'Neil v. Town of Middletown*, 2006 Del. Ch. LEXIS 10, 2006 WL 205071 (Del. Ch. Jan. 18, 2006)). As in *Reeder*, the Plaintiff here seeks not to enjoin the misuse of public funds or land, but to obtain an advisory opinion adopting his interpretation of the law. *See id.* As such, it is unlikely that taxpayer standing is available.

While the Court notes the foregoing, it withholds judgment on the question of standing, as these claims are disposed of on other grounds.

[7] Pl.'s Answering Br. at 9-11.

[8] *See Reed,* 2002 Del. Ch. LEXIS 83, 2002 WL 1402238 at *3.

[9] *Id.* (quoting 10 *Del. C.* § 6501).

[10] *See* Pl.'s Answering Br. at 9 ("Auditor Wagner has no intention of changing his conduct").

C. § 2504. [11] In such a case, the person denied access to public records must present a petition and all supporting documentation to the Chief Deputy Attorney General, who must then render a written determination declaring whether a violation has occurred. Only after Chief Deputy's determination is made, may the petitioner or public body appeal the matter to the Superior Court. [12]

By *29 Del. C. § 2504*, the Attorney General is obligated to represent the Auditor of Accounts in suits brought against him in his official capacity. The Complaint [*8] fails to allege that the Plaintiff first petitioned the Attorney General and received an unfavorable administrative determination. The Plaintiff acknowledges his failure to exhaust administrative remedies requires dismissal.

IV. CONCLUSION

As set forth above, this Court lacks subject matter jurisdiction over the Audit Claims, and the FOIA Claims must be dismissed because of Plaintiff's failure to exhaust administrative remedies. An implementing order will be entered.

---

[11] 29 *Del. C.* §§ 10005(b) & (e).

[12] *Id.*

C

State v. Andrews

Court of Special Appeals of Maryland

March 30, 2016, Filed

No. 1496, September Term, 2015

Reporter
2016 Md. App. LEXIS 33

STATE OF MARYLAND v. KERRON ANDREWS

Disposition: JUDGMENTS OF THE CIRCUIT COURT FOR BALTIMORE CITY AFFIRMED. COSTS TO BE PAID BY MAYOR AND CITY COUNCIL OF BALTIMORE.

Judges: [*1] Leahy, Friedman, Thieme, Raymond G., Jr. (Retired, Specially Assigned), JJ. Opinion by Leahy, J.

Opinion by: Leahy

Opinion

Opinion by Leahy, J.

> "[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."

Riley v. California, 134 S. Ct. 2473, 2484, 189 L. Ed. 2d 430 (2014).

This case presents a *Fourth Amendment* issue of first impression in this State: whether a cell phone—a piece of technology so ubiquitous as to be on the person of practically every citizen—may be transformed into a real-time tracking device by the government without a warrant.

On the evening of May 5, 2014, the Baltimore City Police Department (BPD) used an active cell site simulator, without a warrant, to locate Appellee Kerron Andrews who was wanted on charges of attempted murder. The cell site simulator, known under the brand name "Hailstorm," forced Andrews's cell phone into transmitting signals that allowed the police to track it to a precise location inside a residence located at 5032 Clifton Avenue in Baltimore City. The officers found Andrews sitting on the couch in the living room and arrested him pursuant to a valid arrest warrant. The cell phone was in his pants pocket. After obtaining a warrant [*2] to search the residence, the police found a gun in the cushions of the couch.

In the Circuit Court for Baltimore City, Andrews successfully argued that the warrantless use of the Hailstorm device was an unreasonable search under the *Fourth Amendment of the United States Constitution*. The court suppressed all evidence obtained by the police from the residence as fruit of the poisonous tree. The State, pursuant to Maryland Code (1973, 2013 Repl. Vol., 2015 Supp.), *Courts and Judicial Proceedings Article ("CJP"), § 12-302(c)(4)*, now appeals the court's decision to suppress that evidence.

The specific questions before us, as framed by the State, are:

> 1) Did the motions court err in finding that the use of a cellular tracking device to locate Andrews's phone violated the *Fourth Amendment*?
>
> 2) Did the motions court err in finding that Andrews did not have to show standing before challenging the search of the home where he was arrested?
>
> 3) Did the motions court err in finding that the search warrant for the home where Andrews was located was invalid?
>
> 4) Did the motions court err in excluding the items recovered in this case?

We conclude that people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement, and—recognizing that the *Fourth Amendment* protects people and not simply [*3] areas—that people have an objectively reasonable expectation of privacy in real-time cell phone location information. Thus, we hold that the use of a cell site simulator requires a valid search warrant, or an order satisfying the constitutional requisites of a warrant, unless an established exception to the warrant requirement applies.

We hold that BPD's use of Hailstorm was not supported by a warrant or an order requiring a showing of probable cause and reasonable limitations on the scope and manner of the search. Once the constitutionally tainted information, obtained through the use of Hailstorm, was excised from the subsequently issued search warrant for 5032 Clifton Avenue, what remained was insufficient to establish probable cause for a search of that residence. Because the antecedent *Fourth Amendment* violation by police provided the only information relied upon to establish probable cause in their warrant application, those same officers

cannot find shelter in the good faith exception, and the evidence seized in that search withers as fruit of the poisoned tree. We affirm.

BACKGROUND

Andrews was positively identified via photographic array as the person who shot three people on April 27, 2014, [*4] as they were attempting to purchase drugs on the 4900 block of Stafford Street in Baltimore City.[1] He was charged with attempted first-degree murder and attendant offenses in connection with the shooting, and a warrant for his arrest was issued on May 2, 2014.

Pen Register and Trap & Trace Order

Unable to locate Andrews, Detective Michael Spinnato of the BPD confirmed Andrews's cell phone number through a confidential informant, and then submitted an application in the Circuit Court for Baltimore City for a pen register/trap & trace order for Andrews's cell phone.[2] Specifically, Det. Spinnato requested authorization for the "installation and use of device known as a "Pen Register\Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits, which registers telephone numbers dialed or pulsed from or to the telephone(s) having the number(s) . . . ." The application stated that Andrews was aware of the arrest warrant, and that to hide from police

> suspects will contact family, girlfriends, and other acquaintances to assist in their day to day covert affairs. Detective [*5] Spinnato would like to track/monitor Mr. Andrews'[s] cell phone activity to further the investigation an [sic] assist in Mr. Andrews'[s] apprehension.
>
> * * *
>
> Your Applicant hereby certifies that the information likely to be obtained concerning the aforesaid individual'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 being conducted by the Agency.

On May 5, 2014, Det. Spinnato's application was approved in a signed order stating, in part:

> **[T]he Court finds that probable cause exists and that the applicant has certified that the information likely to be obtained by the use of the above listed device(s) is relevant to an ongoing criminal investigation**, To wit: Attempted Murder.
>
> * * *

(Emphasis in original). And, as requested in the application, the court,

> **ORDERED**, pursuant to *Section 10-4B-04 of the Courts and Judicial Proceedings Article* . . . [Applicants] are authorized to use for a period of sixty (60) days from the date of installation, a Pen Register \ Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits . . .
>
> * * *
>
> **ORDERED**, . . . [t]he Agencies are *authorized 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*, unobtrusively [*7] and with a minimum of interference to the service of subscriber(s) of the aforesaid telephone, and

---

[1] The State later admitted that there were also two negative photo arrays.

[2] As discussed further *infra*, pursuant to the Maryland Pen Register, Trap and Trace Statute, found at CJP § 10-4B-01 *et seq.* ("Maryland pen register statute"), a court having jurisdiction over the crime being investigated may authorize the use of a "pen register" and/or a "trap and trace device," defined as:

> '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.

CJP § 10-4B-01(c)(1). The statute continues, stating:

> 'Trap and trace device' means a device or process that captures the incoming electronic or other impulses that identify the **[*6]** 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). Under Maryland law, an order for a pen register/trap & trace is issued without a warrant and on something less than probable cause.

shall initiate a signal to determine the location of the subject's mobile device . . . .

(Emphasis added).

Cell Phone in a Hailstorm

As soon as Det. Spinnato obtained the pen register\trap & trace order on May 5, he sent a copy to the BPD's Advanced Technical Team (the "ATT"). The ATT then issued a form request to the service provider (Sprint) for the following: subscriber information; historical cell site location information ("CSLI") for the period from April 5 to May 5, 2014; pen register data for 60 days; and precision GPS data from Andrews's phone.[3] An additional request followed for "GPS Precise Locations and email."

Later on the same day—May 5—Det. Spinnato began receiving emails from ATT with GPS coordinates for Andrews's cell phone (within a range of a 200 to 1600 meter radius). Det. Spinnato and officers from the Warrant Apprehension Task Force [*9] ("WATF") proceeded to the general area and waited until they received information from ATT that the cell phone was in the area of 5000 Clifton Avenue, Baltimore City. They proceeded to an area where there were approximately 30 to 35 apartments around a U-shaped sidewalk. Detective John Haley from ATT arrived and, using a cell site simulator known by the brand name "Hailstorm," was able to pinpoint the location of the cell phone as being inside the residence at 5032 Clifton Avenue.[4]

Det. Spinnato knocked on the door and, [*10] after obtaining the consent of the woman who answered, entered the residence along with several other officers. They found Andrews seated on the couch in the living room with the cell phone in his pants pocket. Det. Spinnato arrested Andrews and secured the location until a search warrant could be obtained. Once they had the warrant, the BPD searched the home and found a gun in the couch cushions.

Initial Hearings

Andrews was indicted by a grand jury on May 29, 2014, on numerous charges related to the April 27, 2014 shooting. On July 1, 2014, the Assistant Public Defender representing Andrews filed an "omnibus" motion including requests for discovery and the production of documents. The State responded with an initial disclosure and supplemental disclosure on July 9 and 11, respectively. Those disclosures, however, failed to reveal the method used to locate Andrews on the date of his arrest.

On November 3, 2014, defense counsel filed a supplemental discovery request seeking, *inter alia*, "[a]ll evidence indicating how Andrews was located at 5032 Clifton Avenue." The State's response to that request, dated January 8, 2015, stated, "[a]t this time the State does not possess information related to [*11] the method used to locate [Andrews] at 5032 Clifton Avenue." However, five months later defense counsel received an email from the Assistant State's Attorney ("ASA") assigned to the case indicating that it was her understanding that "the ATT used a stingray to locate[] your client via his cell phone," but she was waiting for "the paperwork." The next day, May 7, the ASA also notified defense counsel of exculpatory evidence in the form of a negative photo array that was conducted the previous January.

On May 12, 2015, defense counsel requested that the court dismiss the case based on discovery violations and moved for suppression of evidence, including the gun, phone records, and

[3] Two broad categories of CSLI may be sought from the service provider. The first is historical CSLI, which is used to look back through service provider records to determine a suspect's location at a given point in the past. *See, e.g., United States v. Graham*, 796 F.3d 332, 343 (4th Cir. 2015) ("Historical CSLI identifies cell sites, or 'base stations,' to and from which a cell phone has sent or received radio signals, and the particular points in time at which these transmissions occurred, over a given timeframe. . . . The cell **[*8]** sites listed can be used to interpolate the path the cell phone, and the person carrying the phone, travelled during a given time period."), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015). Law enforcement frequently uses historical CSLI to prove that a defendant was in the area where a crime of which he is accused occurred. The second category of CSLI is real-time data, used to track the whereabouts and movements of a suspect by using the cell phone as a tracking device. *See, e.g., Tracey v. State*, 152 So. 3d 504, 507 (Fla. 2014), *reh'g denied* (Dec. 8, 2014). Here, the BPD obtained real-time location information from the service provider when it received the GPS coordinates associated with the cell phone from Sprint. Andrews's motion to suppress, however, was focused primarily on the BPD's ensuing use of a cell site simulator to directly obtain pin-point location data. Therefore, on appeal we do not address whether the real-time location information from Sprint should have been obtained under a warrant or special order.

[4] True to its brand name, the Hailstorm device generates an electronic barrage that impacts all the mobile devices within its range. As noted in the *amicus* brief filed by the American Civil Liberties Union ("ACLU") and Electronic Frontier Foundation ("EFF") at page 3, the fact that cell site simulators actively locate phones by forcing them to repeatedly transmit their unique identifying electronic serial numbers, and then calculating the signal strength until the target phone is pinpointed, is found in several recent federal publications and cases, including a Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology 2 (Sept. 3, 2015), *available at* https://www.justice.gov/opa/file/767321/download [https://perma.cc/K99L-H643].

identification testimony. A few days later, on May 15, the State filed a supplemental disclosure, which provided:

> WATF did not have the Clifton Ave address as a possible location until ATT provided that information. Det. Spinnato recalls that he was in touch with Det. Haley from ATT. ATT was provided that information from Sprint in the form of GPS coordinates, Det. Spinnato received the same information either from Sprint directly, or forwarded from ATT. Det. Spinnato provided ATT with the phone number associated [*12] to Defendant from the shooting investigation and, [redacted in original]-Det. Spinnato recalls that ATT gave Det. Spinnato the Clifton Ave address in the afternoon/early evening on May 5, 2014. . . .

The State's supplemental disclosure also identified a second negative photo array conducted on May 4, 2014.

Andrews's initial motions were heard in the circuit court on May 12, 21, and June 4, 2015. At the conclusion of the hearing on June 4, the circuit court found that one of the lead investigators intentionally withheld exculpatory evidence—including both negative photo arrays. As a result, the circuit court partially granted the pending defense motion for sanctions and excluded that detective's testimony from trial. The court declined to dismiss the case and denied the motion to exclude the gun and cell phone on the basis of the State's withholding of discoverable materials. However, as a consequence of the State's failure to timely disclose information concerning Hailstorm surveillance technology that was used by the BPD, the Court granted the defense additional time to file a motion to suppress.

Motion to Suppress

Andrews filed a Motion to Suppress—over 50 pages including exhibits—on [*13] June 30, 2015, in which he challenged the BPD's surreptitious use of the Hailstorm cell site simulator to search Andrews's phone, without a warrant, under the *Fourth Amendment to the United States Constitution*. Andrews moved to suppress all evidence obtained from 5032 Clifton Avenue.

During the ensuing hearing on the motion to suppress, held August 20, 2015, the State suggested, and the defense agreed, that the circuit court rely on the transcripts and exhibits from the earlier motions hearings for an understanding of the function of the Hailstorm device and its use by the BPD:

> [STATE'S ATTORNEY]: . . . The exact testimony that we're going to hear about with regard to the *Fourth Amendment* issue Counsel heard as it related to the discovery issue because the discovery issue bled into the *Fourth Amendment* issue. So there is nothing new. There is nothing -- Counsel's aware that the equipment is called Hailstorm not Stingray because of the testimony that Counsel heard and extracted from the detective as it relates to this very case. So there simply is, there is nothing new. We're at the exact same issue that we were two months ago.
>
> THE COURT: So do we even need, do you need to call the witness or can I just rely on the transcript?
>
> [STATE'S ATTORNEY]: It would seem to me [*14] to rely on the transcript.
>
> * * *
>
> THE COURT: . . . So the State is indicating that the testimony that the State would present today is the same testimony that was presented --
>
> [DEFENSE COUNSEL]: Right.
>
> THE COURT: -- there.
>
> [DEFENSE COUNSEL]: Right.
>
> THE COURT: And that's in the transcript, and the Court can just rely on the transcript to rule on your motion.
>
> [DEFENSE COUNSEL]: Right.
>
> THE COURT: You're fine with that?
>
> [DEFENSE COUNSEL]: Yep.

The court took a recess for several hours to review the motions and transcripts. The following excerpts from the June 4th hearing, entered as Defendant's Exhibit 1C, pertain to the function of the cell site simulator:

> [DETECTIVE HALEY]: What happened in this case was, Detective Sp[innato] from our WATF, which is the Warrant Apprehension Unit, apparently interviewed somebody -- got a phone number. He then responds down here to the Circuit Court . . . and gets a Court Order signed.
>
> He then sends the Court order down to our office, depending on what the carrier is, Verizon, Sprint, T-Mobile, AT&T. We then send it to them. I ask for subscriber information, call-detail records.
>
> They provide us with GPS locations, in this case. And once we get all the information, then we have [*15] equipment that we can go out and locate cell phones.
>
> [DEFENSE COUNSEL]: Okay. When you say, we have equipment that we can locate cell phones, you're talking about the Stingray equipment, is that what was used in this case?

[DETECTIVE HALEY]: Yeah, it's called the Hailstorm. It used to be -- Stingray is kind of first generation.

* * *

[DEFENSE COUNSEL]: Tell me what the Hailstorm does.

[DETECTIVE HALEY]: What we get from the phone company is the subscriber information. So, when we get the subscriber information, it has a [sic] identifier on there, if you will, a serial number. We put that into the Hailstorm equipment. And the Hailstorm equipment acts like a cell tower. So, we go into a certain area, and basically, the equipment is looking for that particular identifier, that serial number.

[DEFENSE COUNSEL]: Okay. And so, if a person is inside of a home, that equipment peers over the wall of the home, to see if that cell phone is behind the wall of that house, right?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: And it sends an electronic transmission through the wall of that house, correct?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: Did you get a separate search warrant for that search into the [*16] home?

[DETECTIVE HALEY]: You'd have to talk to Detective Spinnato about that. Because he's the one that got the Court Order signed.

[DEFENSE COUNSEL]: Did you do the search? You conducted the equipment in this -- you operated —

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: -- the equipment?

[DETECTIVE HALEY]: Yes.

* * *

[DEFENSE COUNSEL]: Tell me all of the information the Hailstorm can retrieve from a phone.

[DETECTIVE HALEY]: It's going to retrieve, like I said before, the serial number of the phone, depending on what kind of phone it is. It's going to -- there's [sic] different identifiers. Like for Sprint, in this case, it's called the MSID. And that's like a ten-digit -- like a ten-digit number. So, it's retrieving that. And there's also the electronic serial number. It's retrieving that. And that's really it.

[DEFENSE COUNSEL]: Can you capture the telephone calls as they're being made?

[DETECTIVE HALEY]: No.

[DEFENSE COUNSEL]: And how do you know where the phone -- and it doesn't capture any data on the phone?

[DETECTIVE HALEY]: No.

[DEFENSE COUNSEL]: Are you sure?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: So, how do you get information about where the phone is on the machine?

[DETECTIVE HALEY]: [*17] Because when it captures that identifier that you put into the machine or the equipment, it then tells you -- it looks like a clock on the equipment. And it tells you where the signal's coming from, like 12, 1, 2, 3 o'clock (indicating). And it will give you like a reading. Like if it says 1:00 at like an 80, well, then you know that you're kind of close to it. But if it says 1:00 at like a 40, then you know that you're probably within, I don't know, probably, you know, 20 yards of it.

[DEFENSE COUNSEL]: The person doesn't have to be using their phone for you to get that information, do they?

[DETECTIVE HALEY]: Actually, if they're on their phone, then they're already connected to -- in this case, the Sprint network. And we're not going to be able to pull them off of that until they're -- until they hang -- until they hang the call up.

[DEFENSE COUNSEL]: So, they hang the call up. And the phone can be in their pocket, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: And then you're reaching in to grab an electronic signal about where that phone is? It's not pinging, in other words, right?

* * *

MR. HALEY: Like I said, our equipment acts like a cell tower. So, it draws the phone to our [*18] equipment.

[DEFENSE COUNSEL]: But you just said, if the person's on the phone, your equipment won't work, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: So, it doesn't act like a cell tower, because you can find the phone only when they are not on the phone, correct?

[DETECTIVE HALEY]: Well, I would say it does act like a cell tower, because the only time that you're going to connect -- the only time that you're going to connect to the network, or to a tower is when you go to try to use it.

[DEFENSE COUNSEL]: But you're connecting to where the phone is, when they're not on the phone, didn't you just say that

[DETECTIVE HALEY]: Maybe I'm getting confused, or I'm not understanding what you're asking me.

[DEFENSE COUNSEL]: My question to you was, for example, I have my phone in my pocket. And I'm sitting in my house, right?

[DETECTIVE HALEY]: Okay.

[DEFENSE COUNSEL]: And you want to know where I am, correct?

[DETECTIVE HALEY]: Okay.

* * *

[DEFENSE COUNSEL]: When I am not on my phone, you will drive by my house, and you will get a signal from my phone indicating where I am, right?

[DETECTIVE HALEY]: Correct.

[DEFENSE COUNSEL]: If I am using the phone, you won't get that signal, right?

[DETECTIVE [*19] HALEY]: Correct.

[DEFENSE COUNSEL]: So, the phone cannot be in use. You are searching for my phone as you're driving through my neighborhood, right?

[DETECTIVE HALEY]: Yes.

[DEFENSE COUNSEL]: And in order to get to my phone, you are sending an electronic signal into my house, right?

[DETECTIVE HALEY]: Yes.

When the hearing resumed, the court made several preliminary findings, and invited counsel to respond. In regard to the pen register/trap & trace order, the court observed:

> I don't find that Judge Williams' order is invalid as a pen register or trap and trace, but I do find that the order does not authorize the use of Hailstorm and I . . . invite the State to tell me otherwise.
>
> * * *
>
> So this is very different from an order authorizing, for example, GPS or cell site information, because that is information that's generated by the phone. And my understanding of this equipment is essentially that it's forcing the phone to emit information, or its taking information from the phone that the phone is not sort of on its own generating at the time which is very different.

On the issue of whether Andrews's arrest was lawful, the parties acknowledged that a valid warrant was outstanding for his arrest. [*20] However, the court questioned whether, as argued by defense counsel, Andrews's presence at 5032 Clifton Avenue "or the warrant they got as a result of him being there is fruit of the poisonous tree because there was a violation of his *Fourth Amendment* rights by [Det. Haley] using the Hailstorm on this phone to locate him at that residence in the first place." Looking then to the application for the warrant to search 5032 Clifton Avenue, the court noted that there was no independent corroboration for the warrant because, "all it says he was located at this address and so we want to search this address. I mean that's really all it says."

After hearing argument, the circuit court found that "the use of the Hailstorm violates the Defendant's *Fourth Amendment* rights," and "any information generated from the use of the Hailstorm [must] be suppressed." The court continued on the record:

> And so just so that I'm clear, it means that the jury cannot hear any testimony or evidence about information obtained from the Hailstorm, obtained through the Hailstorm device. And just so that I'm clear, it's my understanding that the Hailstorm device is what told the police that the Defendant was at that location.
>
> And so that includes any [*21] testimony or evidence then that the Defendant was at that location, if that's what -- because that's what the Hailstorm told the police. And so the jury would be prohibited from hearing evidence or testimony of that. It does not invalidate the arrest or the search [incident to] the arrest with the phone that's in his pocket.[5]
>
> Now anything that came off the phone, again if it came through the Hailstorm device it is suppressed. There can be no evidence or testimony about it. And then again, any police knowledge that the Defendant was at that location again also suppressed, so the jury would not be able to hear any evidence or testimony of that.
>
> So then that leaves us with the fruit of the poisonous tree argument for the search and seizure warrant. I reviewed the warrant and it literally says the Defendant was in there so

[5] Mr. Andrews did not challenge the legality of his arrest or search incident to arrest, either in the circuit court or before this Court. He did, however, seek to suppress the cell phone, but that motion was denied and Mr. Andrews did not file a cross-appeal to contest that ruling.

> now we need a warrant. And information generated from the use of the Hailstorm be suppressed, that's all that it is. And so I analyze this different, a little bit different from a normal sort of motion to suppress a search and seizure warrant or even *Franks* in terms of standing.
>
> I don't -- I understand the State's argument in terms of standing and this not being his residence, [*22] and the Defense's argument that he was at a minimum an overnight guest and has some reasonable expectation of privacy. I don't think I need to reach those issues because the warrant is really just fruit of the poisonous tree of the illegally obtained information about the Defendant's location. That's what it is.
>
> And so I am granting the suppression of that for that very reason. And so that the record is clear — and I know that the State is asking to take an appeal, the record is clear. The ruling of the Court is that the government violated the Defendant's *Fourth Amendment* rights by essentially using the Hailstorm to locate him at that residence.

The State noticed its appeal on September 3, 2015.

DISCUSSION

Motion to Dismiss

Before turning to the merits, we must address Andrews's motion to dismiss this appeal on the ground that the notice of appeal was defective, and therefore, not filed within the time prescribed by Rule 8-202.

The State [*23] filed its notice of appeal on September 3, 2015; however, the signed certificate of service—indicating that a copy of the notice was "mailed first-class, postage prepaid" on that same day—failed to list the party that was served. Andrews acknowledges that a copy of the notice was delivered to the Office of the Public Defender on September 4, 2015. Nevertheless, Andrews argues that the State's notice did not comply with the certificate of service requirements of *Maryland Rule 1-323*, and that the clerk should not have accepted the filing. Consequently, according to Andrews, no valid notice of appeal was filed in this case. The State concedes that the failure to name the party to be served was a defect in the certificate of service, but maintains the clerk was required to accept the filing because the certificate complied with the literal requirements of *Rule 1-323*. The State urges that it would be improper to dismiss the appeal because there is no dispute that the opposing party was served in a timely fashion.

Maryland Rule 1-323 directs that the court clerk may not accept for filing a pleading or other paper requiring service, unless it is accompanied by "an admission or waiver of service or a signed certificate showing the date and [*24] manner of making service." In *Director of Finance of Baltimore City v. Harris*, this Court addressed whether a certificate of service that failed to identify all the persons upon whom service was required should have been rejected for filing by the court clerk. *90 Md. App. 506, 513-14, 602 A.2d 191 (1992)*. Looking to the 1984 revision of the Maryland Rules that produced the current *Rule 1-323*, this Court observed:

> Under the old Rule, the clerk may have had some obligation to determine whether the certificate actually showed service on the "opposite party." But, as noted, that obligation, if it ever did exist, has been eliminated. . . . The obligation of the clerk under the current Rule is simply to assure that there is, in fact, an admission, a waiver, or a certificate showing the date and manner of service. If such a certificate is attached to the paper, the clerk must file the paper, leaving it then to the parties or the court to deal with any deficiency.[6]

More recently, in *Lovero v. Da Silva*, this Court clarified that, by mandating that proof of service (or a waiver of service) appear on each pleading or paper, "*Rule 1-323* assures the court . . . that each party has been duly notified before action is taken by the court in response to or as a result of the subject pleading or paper." *200 Md. App. 433, 446, 28 A.3d 43 (2011)*. We determined that Lovero's notice of appeal should have been rejected by the clerk, explaining that

---

[6] This Court further illuminated the evolution of Rule 1-323 stating:

> Rule 1-323 is derived ultimately from Rule 1(a)(2), Part Two, V, of the General Rules of Practice and Procedure, adopted by the Court of Appeals and approved by the General Assembly pursuant to 1939 Md. Laws, ch. 719, § 35A. Rule 1(a)(2) provided, in relevant part, that **[*25]** a paper "shall not be received and filed by the clerk of the court unless accompanied by an admission or proof of service of a copy thereof *upon the opposite party or his attorney of record* in accordance with this rule." (Emphasis added.) Other parts of the Rule prescribed how service was to be made. That Rule was carried over into the Maryland Rules of Procedure as Rule 306 a.2., which stated that "[t]he clerk shall not accept or file any paper requiring service other than an original pleading unless it is accompanied by an admission or proof of service of a copy thereof *upon the opposite party, or his attorney of record*." (Emphasis added.)
>
> Until the 1984 revision of the Maryland Rules, the Rule remained in that form.

Harris, 90 Md. App. at 511-12.

> [w]here, as in the instant case, the notice of appeal contains no [*26] proof of service whatsoever, we have no basis upon which to conclude that the notice of appeal was served on the opposing party or parties. Indeed, it is undisputed here that the Notice of Appeal was never served on Da Silva.

Id. at 449.

In the present case, there is no dispute that the notice was served on defense counsel. Indeed, the State made it clear at the August 20 hearing that it would be filing an appeal as reflected in the court's ruling; "and so that the record is clear — and I know that the State is asking to take an appeal, the record is clear." It is also clear now that, although the omission in the certificate of service is a defect, the certificate met the literal requirements of *Rule 1-323*—it provided the date and manner of service. Where there is no evidence that Andrews was prejudiced or that the course of the appeal was delayed by a defect, "it is the practice of this Court to decide appeals on the merits rather than on technicalities." *Bond v. Slavin, 157 Md. App. 340, 352-53, 851 A.2d 598 (2004)*. *Cf. Williams v. Hofmann Balancing Techniques, Ltd., 139 Md. App. 339, 356-57, 776 A.2d 4 (2001)* (holding that the appellant's failure to identify one of the appellees on his notice of appeal did not deprive this Court of jurisdiction). To be sure, the Court of Appeals has observed that "[o]ur cases, and those of the Court of Special Appeals, have [*27] generally been quite liberal in construing timely orders for appeal." *Newman v. Reilly, 314 Md. 364, 386, 550 A.2d 959 (1988)*; *see also Lovero, 200 Md. App. at 450-51 n.8* (and the cases cited therein) (recognizing that where a challenged notice of appeal was timely filed the courts of Maryland construe the notice in favor of deciding the appeal on the merits). We deny Andrews's motion to dismiss the appeal.

Standard of Review

We review the grant of a motion to suppress based on the record of the suppression hearing, and we view the facts in the light most favorable to the prevailing party. *State v. Donaldson, 221 Md. App. 134, 138, 108 A.3d 500* (citing *Holt v. State, 435 Md. 443, 457, 78 A.3d 415 (2013)*, *cert. denied*, *442 Md. 745, 114 A.3d 711 (2015)*. Further, "we extend 'great deference' to the factual findings and credibility determinations of the circuit court, and review those findings only for clear error." *Id.* (citing *Brown v. State, 397 Md. 89, 98, 916 A.2d 245 (2007)*). But we make an independent, *de novo*, appraisal of whether a constitutional right has been violated by applying the law to facts presented in a particular case. *Williams v. State, 372 Md. 386, 401, 813 A.2d 231 (2002)* (citations omitted); *see also Brown, 397 Md. at 98* ("[W]e review the court's legal conclusions *de novo* and exercise our independent judgment as to whether an officer's encounter with a criminal defendant was lawful." (Citation omitted)).

I.

Fourth Amendment Search

In 1966, in the wake of prominent Congressional hearings on government invasions of privacy, Justice Douglas, [*28] dissenting in *Osborn v. United States* and *Lewis v. United States*, and concurring in *Hoffa v. United States*, observed:

> We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. The aggressive breaches of privacy by the Government increase by geometric proportions. Wiretapping and 'bugging' run rampant, without effective judicial or legislative control.
>
> * * *
>
> Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of man's life at will.

Osborn v. United States, 385 U.S. 323, 340-43, 87 S. Ct. 429, 17 L. Ed. 2d 394 (1966) (Douglas, J., dissenting).[7] Fifty years later we face the same concern—to what extent have advances in technology created an "age of no privacy."[8]

The *Fourth Amendment to the United States Constitution*, made applicable to the States by the *Fourteenth Amendment*, *Mapp v. Ohio, 367 U.S. 643, 655, 81 S. Ct. 1684, 6 L. Ed. 2d 1081, 86 Ohio Law Abs. 513 (1961)*, provides:

> 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

[7] The question presented in *Osborn*, as cast by Justice Douglas, was "whether the Government may compound the invasion of privacy by using hidden recording devices to record incriminating statements made by the unwary suspect to a secret federal agent." *Osborn*, 385 U.S. at 340.

[8] *See also City of Ontario, Cal. v. Quon, 560 U.S. 746, 760, 130 S. Ct. 2619, 177 L. Ed. 2d 216 (2010)* ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential **[*29]** means or necessary instruments for self-expression, even self-identification.").

> affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The first clause protects individuals against unreasonable searches and seizures,[9] *see* *Katz v. United States, 389 U.S. 347, 359, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967)* ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures[]"), and the second clause requires that warrants must be particular and supported by probable cause, *see* *Payton v. New York, 445 U.S. 573, 584, 100 S. Ct. 1371, 63 L. Ed. 2d 639 (1980)*.

A "search" within the meaning of the *Fourth Amendment* occurs where the government invades a matter in which a person has an expectation of privacy that society is willing to recognize as reasonable. *Kyllo v. United States, 533 U.S. 27, 33, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001)* (citing *Katz, 389 U.S. at 361* (Harlan, J., concurring)). As we made clear in *Raynor v. State*, "[t]he burden of demonstrating a 'legitimate' or 'reasonable' expectation of privacy includes both a subjective and an objective component." *201 Md. App. 209, 218, 29 A.3d 617 (2011)*, *aff'd*, *440 Md. 71, 99 A.3d 753 (2014)* (citation and footnote omitted). "[I]n order to claim the protection of the *Fourth Amendment*, a defendant must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable; *i.e.*, one that has 'a source outside of the *Fourth Amendment*, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.'" *Minnesota v. Carter, 525 U.S. 83, 88, 119 S. Ct. 469, 142 L. Ed. 2d 373 (1998)* (quoting *Rakas v. Illinois, 439 U.S. 128, 143-44 n.12, 99 S. Ct. 421, 58 L. Ed. 2d 387 (1978)*).

The *Fourth Amendment* protects not against all intrusions as such, "but **against intrusions which are not justified in the circumstances, or which are made in an improper manner**." *Maryland v. King, 133 S. Ct. 1958, 1969, 186 L. Ed. 2d 1 (2013)* (emphasis added) (quoting *Schmerber v. California, 384 U.S. 757, 768, 86 S. Ct. 1826, 16 L. Ed. 2d 908 (1966)*). "Although the underlying command of the *Fourth Amendment* is always [*31] that searches and seizures be reasonable, *what is reasonable depends on the context within which a search takes place*." *State v. Alexander, 124 Md. App. 258, 265, 721 A.2d 275 (1998)* (emphasis added in *Alexander*) (quoting *New Jersey v. T.L.O., 469 U.S. 325, 337, 105 S. Ct. 733, 83 L. Ed. 2d 720 (1985)*). Subject to a few well-delineated exceptions, "warrantless searches 'are *per se* unreasonable under the *Fourth Amendment*.'" *Quon, 560 U.S. at 760 (2010)* (quoting *Katz, 389 U.S. at 357*); *see also* *United States v. Karo, 468 U.S. 705, 717, 104 S. Ct. 3296, 82 L. Ed. 2d 530 (1984)* (citations omitted).

a. Effects of the Nondisclosure Agreement

Before we examine the reasonableness of the State's intrusion *in context*, we address the nondisclosure agreement entered into between the State's Attorney for Baltimore City and the Federal Bureau of Investigation in early August 2011 as a condition of BPD's purchase of certain "wireless collection equipment/technology manufactured by Harris [Corporation]." The nondisclosure agreement provided, in part:

> [T]o ensure that [] wireless collection equipment/technology continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and **use shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including b[ut] not limited to: in press release, in court documents, during judicial hearings**, or during other public [*32] forums or proceedings. Accordingly, the Baltimore City Police Department agrees to the following conditions in connection with its purchase and use of the Harris Corporation equipment/technology:
>
> * * *
>
> 5. The Baltimore City Police Department and Office of the State's Attorney for Baltimore City **shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation**

[9] Although the parties do not present their arguments under the Maryland Constitution, Declaration of Rights, we note that Article 26—governing warrants for search and seizure—is generally construed to be co-extensive with the ***Fourth Amendment***. *See* *Upshur v. State*, 208 Md. App. 383, 397, 56 A.3d 620 (2012) (citing *Hamel v. State*, 179 Md. App. 1, 18, 943 A.2d 686 (2008)). Article 26 of the Maryland Declaration of Rights provides:

> That all warrants, without oath or affirmation, to search suspected places, or to seize any person or property, are grievous and oppressive; and all general warrants to search suspected **[*30]** places, or to apprehend suspected persons, without naming or describing the place, or the person in special, are illegal, and ought not to be granted.

(including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use the equipment/technology including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State's case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI.

. . .

(Emphasis added). The agreement directs that in the event of a Freedom of Information Act request, or a court order directing disclosure of information regarding Harris [*33] Corporation equipment or technology, the FBI must be notified immediately to allow them time to intervene "and potential[ly] compromise." If necessary "the Office of the State's Attorney for Baltimore will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to provide, any information concerning the Harris Corporation wireless collection equipment/technology[.]"

We observe that such an extensive prohibition on disclosure of information to the court—from special order and/or warrant application through appellate review—prevents the court from exercising its fundamental duties under the Constitution. To undertake the *Fourth Amendment* analysis and ascertain "the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security," *Terry v. Ohio, 392 U.S. 1, 19, 88 S. Ct. 1868, 20 L. Ed. 2d 889 (1968)*, it is self-evident that the court must understand why and *how* the search is to be conducted. The reasonableness of a search or seizure depends "'on a **balance** between the public interest and the individual's right to personal security free from arbitrary interference by law officers.'" *Pennsylvania v. Mimms, 434 U.S. 106, 109, 98 S. Ct. 330, 54 L. Ed. 2d 331 (1977)* (emphasis added) (quoting *United States v. Brignoni-Ponce, 422 U.S. 873, 878, 95 S. Ct. 2574, 45 L. Ed. 2d 607 (1975)*). The analytical framework requires analysis of the functionality of the surveillance [*34] device and the range of information potentially revealed by its use. A nondisclosure agreement that prevents law enforcement from providing details sufficient to assure the court that a novel method of conducting a search is a reasonable intrusion made in a proper manner and "justified by the circumstances," obstructs the court's ability to make the necessary constitutional appraisal. *Cf. King, 133 S. Ct. at 1970* ("Even if a warrant is not required, a search is not beyond *Fourth Amendment* scrutiny; for it must be reasonable in its scope and manner of execution. Urgent government interests are not a license for indiscriminate police behavior."). In *West v. State*, this Court stated that "to assure that the purpose of the *Fourth Amendment* is upheld, police officers must provide details within affidavits when attempting to acquire search warrants, even if such information would seem to the police officer of trivial consequence at the time." *137 Md. App. 314, 331, 768 A.2d 150 (2001)*.

As discussed further in Section III *infra*, it appears that as a consequence of the nondisclosure agreement, rather than apply for a warrant, prosecutors and police obtained an order under the Maryland pen register statute that failed to provide the necessary information upon which the court could make the [*35] constitutional assessments mandated in this case. The BPD certified to the court that pursuant to the order "the information likely to be obtained concerning the aforesaid individual'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** . . . ." However, the suppression court, having the benefit of Det. Haley's testimony (reproduced above), learned that the BPD actually employed the Hailstorm device, which is capable of obtaining active real-time location information—far different from a pen register (a device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument) or track and trace device (a device or process that captures the incoming electronic or other impulses that identify the originating number). *See* fn.2 *supra*.[10]

We perceive the State's actions in this case to protect the Hailstorm technology, driven by a nondisclosure agreement to which [*36] it bound itself, as detrimental to its position and inimical to the constitutional principles we revere.

b. What Constitutes a "Search"—Level of Intrusion and Expectation of Privacy

The State argues that the use of a cell site simulator does not constitute a "search" under the *Fourth Amendment*. The State maintains that the circuit court's decision "was based upon both factually unreasonable conclusions about how the cell site simulator worked in this case, and legally incorrect determinations about what constitutes a 'search.'" The State acknowledges that the factual bases for the circuit court's rulings are found in the June 4, 2015 testimony of Det. Haley. However, the State argues that Det. Haley's testimony "was necessarily rather summary," and does not support the factual conclusions of the circuit court.

[10] It is not clear from the record whether Det. Haley's testimony was authorized through written approval from the FBI as required in paragraph 5 of the nondisclosure agreement.

According to the State, the cell site simulator "acts like a cell tower, and waits to receive a signal bearing the target IMSI" [International Mobil Subscriber Identity]. The State maintains that, properly construed, Det. Haley's testimony reveals that "the process of a cell phone sending its identifying information to a cell tower was indistinguishable from the process of a cell phone sending [*37] its identifying information to a cell site simulator." The State asserts that the Hailstorm device "merely reads the ID number regularly transmitted by activated cell phones as part of their ordinary use" and "[w]hen the device detects a signal from the target phone, it notifies the operator the direction of the signal and the relative strength, allowing the operator to estimate the probable location of the phone." Therefore, the State argues that no reasonable expectation of privacy existed in the information obtained by the Hailstorm device and no intrusion or "search" occurred.

Andrews countercharges that there was ample, explicit support in the record for the circuit court's finding that the Hailstorm device operated by emitting a signal "through the wall of a house" and "into the phone" triggering the phone to respond to the device. Andrews argues that, through the use of an "active cellular surveillance device," the State violated his reasonable expectation of privacy in the personal information contained and generated by his cell phone, without which the government would not have been able to discover his location inside the home.

Presumably because of the nondisclosure agreement discussed [*38] above, the State provided limited information regarding the function and use of the Hailstorm device. And presumably, the State would have limited itself in this manner regardless of whether it relied on testimony from the prior hearing or produced live testimony before the suppression court.[11] Notwithstanding this, it is clear from Det. Haley's testimony that "the Hailstorm equipment acts like a cell tower," but, unlike a cell tower awaiting incoming signals, the Hailstorm is an active device that can send an electronic signal through the wall of a house and "draw[] the phone to [the] equipment." Based on the direction and strength of the signal the Hailstorm receives from a cell phone in response, law enforcement can pinpoint the real-time location of a cell phone (and likely the person to whom it belongs) within less than 20 yards.

These points from Det. Haley's testimony regarding the function of the Hailstorm device are consistent with what other courts and legal scholars have been able to discern about the device. Hailstorm, along with the earlier-model cell site simulator known as "StingRay," to which Det. Haley referred, are far from discrete, limited surveillance tools. Rather, as described in a recent article in the Harvard Journal of Law and Technology cited by Appellee and the *amici*:[12]

> This technology, commonly called the StingRay, the most well-known brand name of a family of surveillance devices known more generically as "IMSI catchers," is used by law enforcement agencies to obtain, directly and in real time, unique device identifiers and detailed location information of cellular phones—data that it would otherwise be unable to obtain without the assistance of a wireless carrier.
>
> * * *
>
> By impersonating a cellular network base station, a StingRay—a surveillance device that can be carried by hand, installed in a vehicle, or even mounted on a drone—**tricks all nearby phones and other mobile devices into identifying themselves (by revealing their** [*40] **unique serial numbers)** just as they would register with genuine base stations in the immediate vicinity. As each phone in the area identifies itself, the StingRay can determine the location from which the signal came.

Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J. L. & Tech. 134, 142, 145-46 (2014) (emphasis added; footnotes omitted).

The Supreme Court of Wisconsin examined whether law enforcement could obtain location data through cell site information or a StingRay pursuant to a warrant and, before holding that the warrant was sufficiently particularized, based on probable cause, and passed constitutional muster, observed:

> A stingray is an electronic device that mimics the signal from a cellphone tower, which causes the cell phone to send a responding signal. If the stingray is within the cell phone's signal range, the stingray measures signals from the phone, and based on the [*41] cell phone's signal strength, the stingray can provide an initial general location of the

[11] In a suppression hearing, "[w]here . . . the defendant establishes initially that the police proceeded warrantlessly, the burden shifts to the State to establish that strong justification existed for proceeding under one of the 'jealously and carefully drawn' exceptions to the warrant requirement." *Jones v. State*, 139 Md. App. 212, 226, 775 A.2d 421 (2001) (citation omitted). Where the evidence presented is inconclusive, **[*39]** the consequence for the State is that the defendant wins. *Id.*

[12] In addition to the ACLU and EFF, Professor David Gray of the University of Maryland Francis King Carey School of Law filed a detailed and informative amicus brief in this case.

> phone. By collecting the cell phone's signals from several locations, the stingray can develop the location of the phone quite precisely.

State v. Tate, 2014 WI 89, 357 Wis. 2d 172, 849 N.W.2d 798, 826 n.8 (Wisc. 2014) (citation omitted), *cert. denied*, *135 S. Ct. 1166, 190 L. Ed. 2d 921 (2015)*; *see also, e.g., 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 an earlier-model device, the "Triggerfish," as equipment that "enables law enforcement to gather cell site location information directly, without the assistance of the service provider"). We cannot say that the factual findings of the circuit court, in this case, were erroneous; they are firmly grounded in the testimony before that court, and the State has provided no evidence to the contrary.

In determining then whether a *Fourth Amendment* "search" occurred, we apply the court's factual findings to the test pronounced in *Katz, supra.* Rather than limit the constitutional appraisal to a trespass analysis,[13] the *Katz* test requires a two-fold showing: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *389 U.S. at 361* (Harlan, J., concurring).[14] Even under the more [*42] flexible *Katz* test, however, rapid advancements in technology make ascertaining what constitutes a search under the *Fourth Amendment* ever more challenging.[15]

Charles Katz was charged with transmitting wagering information by telephone in violation of federal law. *Katz, 389 U.S. at 348*. He objected during his trial to the government's introduction of evidence collected by FBI agents who overheard and recorded his end of telephone conversations from inside a public telephone booth. *Id.* The agents had placed a recording device on the outside of the phone booth from which Katz placed his calls. *Id.* The government [*45] contended on appeal that their surveillance did not constitute a search prohibited by

---

[13] In *Olmstead v. United States*, the Supreme Court held that the government's use of a wire-tapping device over an extended period of time did not constitute a violation of the ***Fourth Amendment*** because the wires were installed in a manner that did not constitute a trespass upon the property of the petitioners. 277 U.S. 438, 464, 48 S. Ct. 564, 72 L. Ed. 944 (1928). Thus, the Court stated that a ***Fourth Amendment*** violation would occur where there was a tangible, physical intrusion by the government. *Cf. id.* at 466. *Olmstead* was overruled in part by the Court in *Katz*. 389 U.S. at 353.

[14] Maryland appellate courts have, so far, only addressed the admissibility of historical CSLI obtained from a service provider. *See State v. Payne*, 440 Md. 680, 690-91, 104 A.3d 142 (2014) (stating that whether a detective "should have been qualified as an expert before being allowed to engage in the process of identifying the geographic location of the cell towers and the locations themselves depends on understanding just what are cell phone records and what their contents reveal."); *Hall v. State*, 225 Md. App. 72, 91, 123 A.3d 577 (2015) (concluding that the State's witness was properly qualified as an expert to testify regarding the mapping of appellant's cell phone data); *Stevenson v. State*, 222 Md. App. 118, 129-30, 112 A.3d 959 (determining that a **[*43]** *Frye-Reed* hearing on admissibility of novel scientific evidence and expert scientific testimony was not required for admission of cellular tower "ping" evidence), *cert. denied*, ***443 Md. 737, 118 A.3d 863 (2015)***; *Wilder v. State*, 191 Md. App. 319, 364, 991 A.2d 172 (2010) (holding that the admission of CSLI required the qualification of the sponsoring witness as an expert); *Coleman-Fuller v. State*, 192 Md. App. 577, 619, 995 A.2d 985 (2010) (same). Maryland courts have not previously addressed CSLI in the context of a ***Fourth Amendment*** challenge and have never addressed police use of cell site simulators or obtaining real-time CSLI. Because key factual distinctions in this case involve the function of Hailstorm and the ability of law enforcement to track a cell phone directly and in real time, our own cases provide limited guidance.

[15] *See generally* Renée McDonald Hutchins, *Tied Up In Knotts? GPS Technology and The Fourth Amendment*, 55 UCLA L. Rev. 409 (2007). Professor Hutchins notes that the Supreme Court has developed a differential treatment in its intrusiveness analysis under the ***Fourth Amendment*** based on the type of information revealed, explaining:

> When gauging the objective reasonableness of various privacy expectations, the Court has leaned heavily on its assessment of the type of information revealed to segregate challenged surveillance technologies into two rough groups: sense-augmenting surveillance and extrasensory **[*44]** surveillance. Sense augmenting surveillance refers to surveillance that reveals information that could theoretically be attained through one of the five human senses. With regard to this type of surveillance, the Court has tended to find that simple mechanical substitutes for or enhancements of human perception typically trigger no ***Fourth Amendment*** concerns in cases in which human perception alone would not have required a warrant.
>
> Extrasensory surveillance, conversely, is that which reveals information otherwise indiscernible to the unaided human senses. The Court has adopted a more privacy-protective view of this form of technologically enhanced police conduct. In fact, the case law suggests that surveillance of this type is largely prohibited in the absence of a warrant.

Id. at 432-33.

the *Fourth Amendment* because Katz was in a public location that was not constitutionally protected and because the technique they employed involved no physical penetration of the telephone booth. *Id. at 352*. Writing for the majority, Justice Stewart rejected the formulation of the issues by the parties, premised on whether the telephone booth was a "constitutionally protected area," and instructed that "[t]he *Fourth Amendment* protects people, not places . . . what [Katz] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id. at 361* (citations omitted). The Court continued, stating that "once it is recognized that the *Fourth Amendment* protects people—and not simply 'areas'—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." *Id. at 350, 353*.

Almost 20 years after establishing in *Katz* that an examination of intrusiveness under the *Fourth Amendment* is not simply measured by physical invasion, the Supreme Court addressed the constitutionality of the government's surreptitious use of a radio transmitter to track the movements [*46] of a container to and inside a private residence. *United States v. Karo, supra, 468 U.S. at 709-10*. The physical installation of the transmitter was not at issue; rather, the question before the Court was "whether the monitoring of a beeper in a private residence, not open to visual surveillance, violates the *Fourth Amendment* rights of those who have a justifiable interest in the privacy of the residence." *Id. at 714*. Although the Court noted that the monitoring of an electronic device is "less intrusive than a full-scale search," it, nevertheless, reveals information about the interior of the residence that the government "could not have otherwise obtained without a warrant." *Id. at 715*. The Supreme Court stated:

> We cannot accept the Government's contention that it should be completely free from the constraints of the *Fourth Amendment* to determine by means of an electronic device, without warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of *Fourth Amendment* oversight.

Id. at 716 (footnote omitted). Notably, the Court [*47] also soundly rejected the government's contention that it should be able to engage in warrantless monitoring of an electronic device inside a private residence "if there is the requisite justification in the facts for believing that a crime is being or will be committed and that monitoring the beeper **wherever it goes** is likely to produce evidence of criminal activity." *Id. at 717* (emphasis added). The Court recognized limited exceptions to the general rule, such as in the case of exigency, but explained why in its view the government exaggerated the difficulties associated with obtaining a warrant:

> The Government argues that the traditional justifications for the warrant requirement are inapplicable in beeper cases, but to a large extent that argument is based upon the contention, rejected above, that the beeper constitutes only a minuscule intrusion on protected privacy interests. The primary reason for the warrant requirement is to interpose a 'neutral and detached magistrate' between the citizen and 'officer engaged in the often competitive enterprise of ferreting out crime.'
>
> * * *
>
> The Government contends that it would be impossible to describe the 'place' to be searched, because the location [*48] of the place is precisely what is sought to be discovered through the search. [ ] However true that may be, it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested.

Id. at 717-18 (citing *Johnson v. United States, 333 U.S. 10, 14, 68 S. Ct. 367, 92 L. Ed. 436 (1948)*).

In *Kyllo, supra*, the Supreme Court considered whether a *Fourth Amendment* search had occurred when the government used a thermal imaging device to detect infrared radiation inside a home. *533 U.S. at 29-30*. Federal agents, suspecting that Danny Kyllo was growing marijuana inside his home, were able to confirm areas of heat coming from high intensity lamps used to grow marijuana plants indoors. *Id.* At the threshold of his analysis, Justice Scalia, writing for the majority, observed:

> It would be foolish to contend that the degree of privacy secured to citizens by the *Fourth Amendment* has been entirely unaffected by the advance of technology. . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

Id. at 33-34. The Court then noted that, although the *Katz* test—"whether the individual has an expectation of privacy that society is prepared to recognize [*49] as reasonable"—may be difficult to apply to some locations, such as telephone booths and automobiles—the expectation of privacy in the home had "roots deep in the common law." *Id. at 34*.

In support of the use of its thermal imaging technology, the government in *Kyllo* argued that there was no "search" because

the device detected "'only heat radiating from the external surface of the house[.]'" *Id. at 35*. The Supreme Court, however, cast aside this contention as the kind of mechanical interpretation rejected in *Katz* and stated, "so also a powerful directional microphone picks up only sound emanating from a house—and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house." *Id.* Rather than abandon *Katz* and take such a mechanical approach, the Court sought to adopt a rule "tak[ing] account of more sophisticated [surveillance] systems that are already in use or in development." *Id. at 35-36* (footnote omitted). Accordingly, the Court held that "[w]here . . . the Government uses a device that is not in general public use, to explore the details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable [*50] without a warrant." *Id. at 40*. Furthermore, the Court repeated the caveat of *Silverman v. United States*, that the "protection of the home has never been tied to the measurement of the quality or quantity of information obtained" for any invasion of the home, "'by even a fraction of an inch' [is] too much." *Id. at 37* (quoting *Silverman, 365 U.S. 505, 512, 81 S. Ct. 679, 5 L. Ed. 2d 734 (1961)*).

From *Katz* to *Kyllo*, the Supreme Court has firmly held that use of surveillance technology not in general public use to obtain information about the interior of a home, not otherwise available without trespass, is a "search" under the *Fourth Amendment*. These decisions resolved to protect an "expectation of privacy that society is prepared to recognize as reasonable." After *Kyllo*, however, the question remained whether electronic tracking or surveillance outside the home could constitute a search under the *Fourth Amendment*.

In *United States v. Jones*, the Supreme Court reviewed the use of a GPS tracking device affixed to the undercarriage of a vehicle to track the movements of the defendant over a period of 28 days. *132 S. Ct. 945, 948, 181 L. Ed. 2d 911 (2012)*. The Court unanimously affirmed the United States Court of Appeals for the District of Columbia Circuit's holding that the electronic location surveillance over a period of 28 days was a search and that [*51] admission of evidence obtained by the warrantless use of the GPS device violated the *Fourth Amendment*. The Court was unable, however, to reach full agreement as to the basis for its decision. *See id. at 953* (majority opinion); *954* (Sotomayor, J., concurring); *957* (Alito, J., concurring in the judgment). Justice Scalia's majority opinion found that a search occurred under the traditional, pre-*Katz* "trespass" rationale, but acknowledged that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id. at 953* (emphasis in original).

Agreeing with Justice Brennan's concurrence in *Knotts v. United States*, Justice Scalia expounded that "'when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the *Fourth Amendment*.'" *Id. at 951* (quoting *Knotts, 460 U.S. 276, 286, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983)*). When law enforcement placed the GPS tracking system on Jones's vehicle, without a warrant, the government physically invaded a constitutionally protected area, *id. at 949, 952*, and factors beyond trespass need not be considered to find there was a *Fourth Amendment* violation. *Id. at 953-54*. Justice Scalia explained that the common-law trespass test was essentially a minimum test and that the [*52] *Katz* test was "*added to*, not *substituted for*, the common-law trespassory test." *Id. at 952*.

Justice Sotomayor revisited the *Katz* analysis in her concurring opinion, stating that, "even in the absence of a trespass, 'a *Fourth Amendment* search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'" *Id. at 954-55* (Sotomayor, J., concurring) (citations omitted). Recognizing that "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance[,]" Justice Sotomayor opined that the unique attributes of GPS location surveillance will require careful application of the *Katz* analysis. *Id.* She urged the Court to update its understanding of peoples' expectations of privacy in the information age:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. *See, e.g., People v. Weaver, 12 N.Y.3d 433, 441-442, 882 N.Y.S.2d 357, 909 N.E.2d 1195, 1199 (2009)* ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic [*53] surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. [*United States v.*] *Pineda*—Moreno, 617 F.3d[1120,] 1124 [(9th Cir. 2010)] (opinion of Kozinski, C.J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." *Illinois v. Lidster, 540 U.S. 419, 426, 124 S.Ct. 885, 157 L.Ed.2d 843 (2004)*.

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." *United States v. Cuevas—Perez, 640 F.3d 272, 285 (C.A.7 2011)* (Flaum, [*54] J., concurring).
>
> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques. See *Kyllo, 533 U.S., at 35, n.2, 121 S.Ct. 2038*; *ante, at 954* (leaving open the possibility that duplicating traditional surveillance "through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy"). I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the *Fourth Amendment*'s goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance," *United States v. Di Re, 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948)*.

Jones, 132 S. Ct. at 955-56 (Sotomayor, J., concurring) (footnote omitted).

Justice Alito, concurring only in the judgment, disagreed with the majority's [*55] reliance on a trespassory theory. *Jones, 132 S. Ct. at 958*. Instead, Justice Alito found the appropriate inquiry to be "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." *Id.* Justice Alito stated that the majority's reasoning "disregard[ed] what is really important (the *use* of a GPS for the purpose of long-term tracking)" and "will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked." *Id. at 962* (emphasis in original).

From the above precedent, we glean two broad principles regarding the *Fourth Amendment* analysis of surveillance technology. First, where surveillance technology is used without a warrant to obtain information about the contents of a home, not otherwise discernable without physical intrusion, there has been an unlawful search. *See Kyllo, 533 U.S. at 34-35*. Second, where the government has engaged in surveillance using "electronic signals without trespass[,]" the intrusion will "*remain* subject to *Katz* analysis." *Jones, 132 S. Ct. at 953* (emphasis in original). The Supreme Court has recognized, however, that cell phones present novel privacy concerns.

In *Riley, supra*, the Supreme Court made [*56] clear that a search of the information contained in a cell phone is subject to the warrant requirement regardless of its location. *134 S. Ct. at 2489-91*. The Court held that even during a search incident to arrest, the government must first obtain a warrant before searching the digital contents of a cell phone found on the person being arrested. *Id. at 2485-86*.

Chief Justice Roberts described the modern cell phone as much more than a phone:

> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.
>
> One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. Most people cannot lug around every piece of mail they have received for the [*57] past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in *Chadwick, supra*, rather than a container the size of the cigarette package in *Robinson*.

Id. at 2489.

The State argues that its use of the Hailstorm here should be analogized to *Knotts, 460 U.S. 276, 103 S. Ct. 1081, 75 L. Ed. 2d 55*, wherein the Supreme Court upheld law enforcement officers' use of a radio transmitter to track the movements of a container, by automobile, to a defendant's home. In *Knotts*, the Court noted that "[t]he governmental surveillance conducted by means of the beeper in this case amounted principally to the

following of an automobile on public streets and highways." *Id. at 281*. The Court concluded that:

> A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when [*58] he exited from public roads onto private property.

Id. at 281-82. Here, the State argues that because Andrews's cell phone was "constantly emitting 'pings' giving its location to the nearest cell tower, . . . there can be no reasonable expectation of privacy in [that] information" under *Knotts*.

The State's reliance on *Knotts*, however, is misplaced. In *Karo*, the Supreme Court clarified that in *Knotts* the electronic device "told the authorities nothing about the interior of Knotts' cabin." *468 U.S. at 715*. Rather, the information obtained in *Knotts* was "voluntarily conveyed to anyone who wanted to look[,]" *id.* (quoting *Knotts, 460 U.S. at 281*), and the subsequent search warrant was also supported by "intermittent visual surveillance" of the cabin, *Knotts, 460 U.S. at 279*. As noted in *Kyllo*, the Supreme Court has long recognized that "[v]isual surveillance [i]s unquestionably lawful because 'the eye cannot by the laws of England be guilty of a trespass.'" *533 U.S. at 31-32* (quoting *Boyd v. United States, 116 U.S. 616, 628, 6 S. Ct. 524, 29 L. Ed. 746 (1886)*).

Here, there was no visual surveillance. The mere fact that police *could* have located Andrews within the residence by following him as he travelled over public thoroughfares does not change the fact that the police did not know where he was, so they could not follow him. Unlike *Knotts*, the information o btained [*59] in this case did reveal at least one critical detail about the residence; i.e., that its contents included Andrews's cell phone, and therefore, most likely Andrews himself. Further, "pings" from Andrews's cell phone to the nearest tower were not available "to anyone who wanted to look." We find the surreptitious conversion of a cell phone into a tracking device and the electronic interception of location data from that cell phone markedly distinct from the combined use of visual surveillance and a "beeper to signal the presence of [the defendant's] automobile to the police receiver" to track a vehicle over public roads. *See Knotts, 460 U.S. at 282*. Put simply, the information obtained by police in this case was not readily available and in the public view as it was in *Knotts*.

Cell site simulators, such as Hailstorm, can locate and track the movements of a cell phone and its user across both public and private spaces. Unchecked, the use of this technology would allow the government to discover the private and personal habits of any user. As Justice Sotomayor predicted in her concurring opinion in *Jones, supra*, we are compelled to ask "whether people reasonably expect that their movements will be recorded and aggregated [*60] in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *132 S. Ct. at 956* (Sotomayor, J., concurring). We conclude that they do not.

We agree with the United States Court of Appeals for the Fourth Circuit in *United States v. Graham*, in declaring, "[w]e cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person." *796 F.3d 332, 355 (4th Cir.)*, *reh'g en banc granted*, *624 F. App'x 75 (4th Cir. 2015)*.[16] Federal courts reviewing pen register\trap & trace applications have similarly recognized a reasonable expectation of privacy in cell site location information. *See, e.g., In re the Application of the United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006)* ("[D]etailed location information, such as triangulation and GPS data, ... unquestionably implicate *Fourth Amendment* privacy rights."); *In re Application of the United States for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed), 402 F. Supp. 2d 597, 604-05 (D. Md. 2005)* (recognizing that monitoring of cell phone location information is likely to violate a reasonable expectation of privacy)). We also

[16] The recent cell phone encryption battle between Apple and the United States Government illustrates how fervently people care about protecting their personal location information. In 2011, consumers learned that their iPhones stored months of data regarding Wi-Fi hotspots and cell towers around their location in a format that was not encrypted. The ensuing barrage of complaints caused Apple to revise its operating system to protect consumers' location information. Apple, Inc. Press Release, Apple Q&A on Location Data (April 27, 2011) (available at https://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html) [https://perma.cc/PJ5V-KHGE]. Apple refused to comply with a court order to create software to disable certain security protections of an iPhone. *See* Testimony of Bruce Sewell, *Encryption Tightrope: Balancing American's Security and Privacy*, Hearing before the House Comm. on the Judiciary, 114th Cong. (March 1, 2016); Timothy B. Lee,

[*62] *Apple's Battle with the FBI over iPhone Security, Explained*, Vox (Feb. 17, 2016), http://www.vox.com/2016/2/17/11037748/fbi-apple-san-bernardino [http://perma.cc/4MFA-JZ4D].

accept [*61] the circuit court's finding in this case that "no one expects that their phone information is being sent directly to the police department on their apparatus."[17] Recognizing that the *Fourth Amendment* protects people and not simply areas, *Katz, 389 U.S. at 353*, we conclude that people have a reasonable expectation of privacy in real-time cell phone location information.

Moreover, because the use of the cell site simulator in this case revealed the location of the phone and Andrews inside a residence, we are presented with the additional concern that an electronic device not in general public use has been used to obtain information about the contents of a home, not otherwise discernable without physical intrusion. *See Kyllo, 533 U.S. at 34-35*. Under the applicable precedent, this is undoubtedly an intrusion that rises to the level of a *Fourth Amendment* "search." *See id.* Indeed, "the *Fourth Amendment* draws a firm line at the entrance to the house[.]" *Id. at 40* (citation and internal quotation marks omitted). Although we recognize that the use of a cell site simulator to track a phone will not always result in locating the phone within a residence, we agree with the Fourth Circuit's observation that "the government cannot know in advance of obtaining this information how revealing it will be or whether it will detail the cell phone user's movements in private spaces." [*63] *Graham, 796 F.3d at 350* (citation omitted). The United States District Court for the District of Maryland articulated the same concern when addressing the government's use of a particular cell phone as a tracking device to aid in execution of an arrest warrant. The district court stated:

> Location data from a cell phone is distinguishable from traditional physical surveillance because it enables law enforcement to locate a person entirely divorced from all visual observation. Indeed, this is ostensibly the very characteristic that makes obtaining location data a desirable method of locating the subject of an arrest warrant. This also means, however, that **there is no way to know before receipt of location data whether the phone is physically located in a constitutionally-protected place. In other words, it is impossible for law enforcement agents to determine prior to obtaining real-time location data whether doing so infringes upon the subject's reasonable expectation of privacy and therefore constitutes a Fourth Amendment search**.

In re Application of United States for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 540 (D. Md. 2011) (emphasis added).

It would be impractical to fashion a rule prohibiting a warrantless search only retrospectively based on the fact that the search resulted [*64] in locating the cell phone inside a home or some other constitutionally protected area. *See, e.g., Kyllo, 533 U.S. at 38-39* (declining to adopt a Fourth Amendment standard that would only bar the use of thermal imaging to discern "intimate details" in the home because "no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." (emphasis in original)); *cf. Karo, 468 U.S. at 718* ("We are also unpersuaded by the argument that a warrant should not be required because of the difficulty in satisfying the particularity requirement of the *Fourth Amendment*."). Such a rule would provide neither guidance nor deterrence, and would do nothing to thwart unconstitutional intrusions. *Cf. In re the Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device, 396 F. Supp. 2d 294, 323 (E.D.N.Y.2005)* ("Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking . . . which routinely require probable cause." (Internal quotations and citations omitted)).

We determine that cell phone users have an objectively reasonable expectation that their [*65] cell phones will not be used as real-time tracking devices through the direct and active interference of law enforcement. We hold, therefore, that the use of a cell site simulator, such as Hailstorm, by the government, requires a search warrant based on probable cause and describing with particularity the object and manner of the search, unless an established exception to the warrant requirement applies.

We turn to consider whether such an exception applies in this case.

c. The Third Party Doctrine

The State maintains that the "Third Party Doctrine" exception to the warrant requirement applied to the BPD's use of Hailstorm to track down Andrews's cell phone. The doctrine—providing that an individual forfeits his or her expectation of privacy in information that is turned over to a third party—finds its strongest expression in *United States v. Miller, 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976)* and *Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979)*.

In *Smith v. Maryland*, the Supreme Court was presented with the issues of whether the warrantless installation and use of a

[17] As the Supreme Court stated in *Katz*, "[t]o read the Constitution more narrowly is to ignore the vital role that the ... telephone has come to play in private communication." 389 U.S. at 352.

pen register to collect the telephone numbers dialed from a telephone at the petitioner's home constituted a "search" within the meaning of the *Fourth Amendment*. *442 U.S. at 736-37*. The Court described the function of pen registers, stating that they "disclose only the [*66] telephone numbers that have been dialed—a means of establishing communication. Neither the purpose of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.'" *Id. at 741* (quoting *United States v. New York Tel. Co., 434 U.S. 159, 167, 98 S. Ct. 364, 54 L. Ed. 2d 376 (1977)*). Accordingly, the Court narrowed the issue before it, stating:

> Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.

Id. at 742. In *United States v. Miller*, the Supreme Court held that no reasonable expectation of privacy existed once the owner of financial checks turned financial instruments over to a bank and "exposed [them] to [bank] employees in the ordinary course of business." *425 U.S. at 442*.

The State argues that the cell site simulator used in this case merely "detects the signal emitted by the cell phone, just as a regular cell tower would[,]" and, therefore, "the police used data that Andrews voluntarily shared with third parties—specifically his cell phone provider—to locate his phone." The State maintains that, under *Smith* no *Fourth Amendment* "search" [*67] occurred because Andrews had no reasonable expectation of privacy in information he voluntarily transmitted to a third party. The State contends that, by 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 [*68] 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 [*69] 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 [*70] 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 [*71] 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 [*72] 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, 906 A.2d 1054 (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, 99 S. Ct. 421, 58 L. Ed. 2d 387 (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, [*73] 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

[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 **[*74]** he was an overnight guest—Andrews's proffer under the circumstances may have been sufficient to counter the State's standing argument.

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 "[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 [*75] 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, 83 S. Ct. 407, 9 L. Ed. 2d 441 (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 [*76] 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-01:

> **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 [*77] 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 [*78] 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, 552 A.2d 1351 (1989) (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 [*79] 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 *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 [*81] 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, [*82] 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.

---

[19] In the federal district court in *United States v. Wilford*, a defendant more recently argued that cell phone pinging was not authorized by Maryland's pen register statute. ***961 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 **[*80]** guidance as to the scope of the Maryland statute with respect to pinging." *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.

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 Sates. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012)*. [*83]

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 [*84] 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, 2015. Maryland Code (2001, 2008 Repl. Vol., 2015 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
>
> 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. [*85] 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 [*86] 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,

---

[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).

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 [*87] 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 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 [*88] 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 [*89] 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 [*90] 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

---

[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.

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 [*91] 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, 103 S. Ct. 2317, 76 L. Ed. 2d 527 (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, 798 A.2d 5 (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, 96 S. Ct. 2737, 49 L. Ed. 2d 627 (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 over-reaching order into a warrant. The "probable cause" articulated in the resulting order is merely that "**information likely to be obtained . .** [*92] **. 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 [*93] 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 [*94] 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

[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 **[*95]** under the ***Fourth Amendment***.'" *Kentucky v. King*, 563 U.S. 452, 460, 131 S. Ct. 1849, 179 L. Ed. 2d 865 (2011) (some internal quotation marks omitted) (quoting *Mincey v. Arizona*, 437 U.S. 385, 394, 98 S. Ct. 2408, 57 L. Ed. 2d 290 (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, 813 A.2d 231 (2002) (citations omitted). It remains the State's burden to establish exigent circumstances

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 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 [*96] 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, 41 S. Ct. 266, 65 L. Ed. 654 (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 [*97] 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, 73 A.3d 385 (2013)* (quoting *Williams v. State, 372 Md. 386, 419, 813 A.2d 231 (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 [*98] 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

sufficient to justify a warrantless search. *Wengert v. State*, 364 Md. 76, 85, 771 A.2d 389 (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.

[*99] should be suppressed.[23] *Id.* And, we soundly rejected the argument that evidence in a warrant 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, 45 A.3d 948 (2012)*. *See also Murray v. United States, 487 U.S. 533, 534, 108 S. Ct. 2529, 101 L. Ed. 2d 472 (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 fo rms 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 [*101] no independent lawful source to establish a nexus between Andrews and the residence. *Cf. Agurs v. State, 415 Md. 62, 84, 998 A.2d 868 (2010)* (stating that "police should have been aware that there must be a 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, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (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 [*102] 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, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (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 [*103] to enforce the requirements of the *Fourth*

[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 **[*100]** 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 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*.

> *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, 86 Ohio Law Abs. 513 (1961)*, is to deter unreasonable police behavior, *Leon* and [*Massachusetts v. Sheppard, 468 U.S. 981, 104 S. Ct. 3424, 82 L. Ed. 2d 737 (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, 837 A.2d 989 (2003) aff'd, *384 Md. 484, 864 A.2d 1006 (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 [*104] *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. [*105] *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, 118 A.3d 864 (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 [*106] 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, 422 U.S. 531, 539, 95 S. Ct. 2313, 45 L. Ed. 2d 374 (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.

D

State ex rel. Biden v. Camden-Wyoming Sewer & Water Auth.

Superior Court of Delaware, Kent

October 1, 2012, Submitted; November 7, 2012, Decided

C.A. No: 11C-08-004 (RBY)

Reporter
2012 Del. Super. LEXIS 479; 2012 WL 5431035

STATE OF DELAWARE, ex rel. Joseph R. Biden, III, Attorney General of the State of Delaware, Plaintiff, v. THE CAMDEN-WYOMING SEWER AND WATER AUTHORITY, Defendant.

Notice: THIS OPINION HAS NOT BEEN RELEASED FOR PUBLICATION. UNTIL RELEASED, IT IS SUBJECT TO REVISION OR WITHDRAWAL.

Prior History: [*1] Upon Consideration of Plaintiff's Motion for Judgment on the Pleadings.

Disposition: GRANTED IN PART, DENIED IN PART.

Counsel: Ralph K. Durstein, III, Esq., Deputy Attorney General, Frank N. Broujos, Esq., Deputy Attorney General, and Peter O. Jaminson, Esq., Deputy Attorney General, Department of Justice, Wilmington, Delaware for Plaintiff.

Mary E. Sherlock, Esq., Weber, Gallagher, Simpson, Stapleton & Fires, Dover, Delaware for Defendant.

Judges: Robert B. Young, J.

Opinion by: Robert B. Young

Opinion

OPINION AND ORDER

Young, J.

SUMMARY

Coming to this Court is Plaintiff's Motion for Judgment on the Pleadings in this case seeking information, particularly employee salary information, under Delaware Freedom of Information Act. Since the Plaintiff has appropriately commenced this action on behalf of the individual who was denied that information by the Camden-Wyoming Sewer and Water Authority; and since that Authority is a public entity as properly designated by the Delaware Legislature; that Authority is obligated to disclose the requested information. Accordingly, Plaintiff's Motion for Judgment on the Pleadings and costs, as a matter of law, is well-taken, and is **GRANTED.** Plaintiff's accompanying motion for attorneys' fees is **DENIED** inasmuch [*2] as this is a question of first impression, and legitimately contested.

FACTS

Established by formal resolutions of the Towns of Camden and Wyoming in 1962, the Camden-Wyoming Sewer and Water Authority ("CWSWA") provides water treatment and services to those towns, located in Kent County, Delaware. CWSWA was formed pursuant to the provisions of 16 *Del. C.* Chapter 14. According to the briefs, it is the only sewer and water authority in the state.

CWSWA's Board is comprised of six (6) members, three (3) appointed by the Town of Camden and three (3) appointed by the Town of Wyoming. Board members' salaries are not paid directly out of the treasuries of the Towns. Aside from the appointment of members, the Towns appear to have no input or control over the day-to-day operations or administration. The Board holds monthly meetings, all of which are open to the public, a process which has been in effect since its inception.

In addition to the Board, CWSWA has a superintendent and a staff of ten (10) current employees. The enabling statute provides the CWSWA with the authority necessary to conduct almost all aspects of its business, granting it the power to contract; to purchase or lease property; [*3] to borrow money; to adopt bylaws necessary to regulate its affairs and conduct its business; to fix and collect the rates and fees; and to appoint officers, agents, employees and servants, prescribing their duties and compensation.

CWSWA does not receive public funds from the entities of the State or the Towns of Camden and Wyoming. All of its operational revenue is generated through user fees, paid by its customers for the use of sewer and water services. The ten (10) employees mentioned above are not considered State of Delaware employees for any purpose, nor are they employees of either of the Towns. They are not eligible for state pensions or benefits.

Chapter 100 of Title 29 (*29 Del. C. §10001-10006*) contains the sections collectively known as the Freedom of Information Act ("FOIA"). [1] Due to events outside the pleadings of this case, the Attorney General had at a prior time issued an opinion stating that, under FOIA as it existed at that time, CWSWA did not fall within the definition of "public body." [2] In response, the General Assembly promptly amended *§10002*, specifically including authorities created under Chapter 14 of Title 16 within FOIA's definition of a "public body." On [*4] May 9, 2011 after the passage of that Amendment to S.B. 36, one Georgette Williams submitted a request, under FOIA to CWSWA, for information regarding the compensation paid by CWSWA to its employees and contractors during the 2010 calendar year. CWSWA denied the request on the ground that it was not a "public body" subject to the disclosure requirements imposed by FOIA. Ms. Williams subsequently filed a complaint with the State Attorney General's Office requesting a determination of whether CWSWA's denial violated FOIA.

The State Department of Justice responded by letter dated July 1, 2011, advising [*5] Ms. Williams that CWSWA was a "public body" subject to the disclosure requirements, and was in violation of FOIA by denying her request for records. Ms. Williams requested that the Attorney General's Office file suit on her behalf. That was done on August 3, 2011.

STANDARD OF REVIEW

According to Superior Court Civil Rule 12(c), "[a]fter the pleadings are closed but within such time as not to delay the trial, any party may move for judgment on the pleadings." [3] A motion for judgment on the pleadings will be granted when there are no material issues of fact remaining, and the moving party is entitled to judgment as a matter of law. [4] The non-moving party will be entitled to the benefit of any inferences that may be drawn from the pleadings. [5] If there exists even one single set of conceivable circumstances under which the non-moving party could succeed, based on the evidence presented to this point, then the motion must be denied. [6] The standard for granting a motion for judgment on the pleadings is a stringent one, and will be denied unless it is clear that the moving party is entitled to a judgment as a matter of law. [7] All parties agree that no issue of material fact exists herein.

DISCUSSION

The pleadings have raised several significant legal issues, which will be considered separately:

1. Does the Superior Court have jurisdiction to decide this matter?

2. Is The Camden-Wyoming Sewer and Water Authority a "public body" ?

3. Is The Camden-Wyoming Sewer and Water Authority, as a "public body," obliged to disclose its employees' salaries?

4. Does FOIA, as amended, apply to documents created/in existence before the amendment made The Camden-Wyoming Sewer and Water Authority a "public body"?

5. Does the Attorney General have the authority to pursue this matter on behalf of Georgette Williams-which is really to ask: is the entity for whom or for which this action is undertaken a "citizen" ?

1. Does the Superior Court have jurisdiction to decide this matter?

The Defendant initially questioned this Court's subject matter jurisdiction over the claims presented in its Answering Brief. However, no explanation was provided to explain the basis for such [*7] an objection to jurisdiction by this Court. The hearing revealed that there was no longer disagreement between the parties on this issue. For the sake of completeness, the basis of jurisdiction will be discussed.

---

[1] The General Assembly adopted amendments to some portions of Chapter 100 of Title 29 in August, 2012. Though the changes were relatively minor in terms of substance, they did impact the lettering of some sub-parts. The citations used in this opinion reflect the statute in its most recently updated form. For that reason, the citations used in this opinion differ slightly from the citations appearing in the parties's briefs, presented to the Court before the amendments were reflected in most electronic versions of the Delaware Code.

[2] Del. Op. Att'y Gen. 11-IIB03, 2011 Del. AG LEXIS 3, 2011 WL 1428938 (March 16, 2011).

[3] Del. Super. Ct. R. 12(c).

[4] *O'Leary v. Telecom Resources, LLC*, 2011 Del. Super. LEXIS 36, 2011 WL 379300, at *3 (Del. Super. Jan. 14, 2011) **[*6]** (internal citations omitted).

[5] *Id.*

[6] *Hennegan v. Cardiology Consultants, P.A.*, 2007 Del. Super. LEXIS 534, 2007 WL 4200811, at *2 (Del. Super. Sept. 6, 2007).

[7] *Textron, Inc. v. Acument Global Technologies, Inc.*, 2011 Del. Super. LEXIS 157, 2011 WL 1326842 at *5 (Del. Super. April 6, 2011).

The applicable statute does not specifically set out jurisdiction for the scenario at issue. Despite that, the statute does provide some general language to help the Court reach a decision. §10005 describes enforcement procedures. It is there that several other jurisdictional grants are found. According to §10005(b), in cases where a "citizen" has been denied access to "public records," "venue shall be placed in a court of competent jurisdiction for the county or city in which the public body ordinarily meets or in which the plaintiff resides." This particular passage also contains language specifically giving jurisdiction to the Superior Court for any appeals from a determination by the Chief Deputy Attorney General made pursuant to the procedures set forth in §10005(e). As jurisdiction is placed in this Court for decisions involving a public body represented by the Attorney General, it would certainly be logical and appropriate to find that actions by the Attorney General [*8] against a public body would also fall under this Court's jurisdiction. Furthermore, there is nothing about the requested remedies that would cause this action to fall outside of this Court's jurisdiction. Declaratory judgment actions are within the jurisdiction of the Superior Court, unless there is a special basis for equitable jurisdiction.

2. Is The Camden-Wyoming Sewer and Water Authority a "public body"?

The applicable portion of the definition of a "public body" as set forth in 29 Del. C. §10002(g) includes any body empowered by the state that: "(1) Is supported in whole or in part by any public funds; or (2) Expends or disburses any public funds, including grants, gifts or other similar disbursals and distributions; or (3) Is impliedly or specifically charged by any other public official, body, or agency to advise or make reports, investigations or recommendations." Before the amendment clarifying the intent of the statute, CWSWA was not considered to be a "public body", according to an Attorney General Opinion issued March 16, 2011. [8]

CWSWA contends that the language inserted by the Amendment fails to fit within [*9] the intent of the statute, because it does not describe a body that comports with the rest of the definition for "public body." More specifically, CWSWA argues that it not supported by, and does not expend or disburse, public funds of any kind. It is also not impliedly or specifically charged to investigate, or make reports or recommendations. Consequently, CWSWA believes that it should not be considered a "public body."

The General Assembly's authority to make law is derived from the State Constitution. The Delaware Constitution states that "[t]he legislative power of this state shall be vested in a General Assembly . . . ." [9] In fact, Delaware's courts have consistently described the General Assembly's power to make law as "unlimited." [10] Plaintiff argues, and this Court agrees, that regardless of any motive or wisdom which a party asserts might be behind the amendment, the judicial branch is "bound by a most solemn sense of responsibility to sustain the legislative will in the appropriate field of its exercise . . . ." [11]

Acts [*10] of the General Assembly necessarily enjoy a presumption of constitutionality. [12] The imposition of this presumption places the burden on the party attacking the constitutionality of an act to demonstrate why it is invalid. [13] It also implies that the Court must give deference to the decisions of the legislature. [14] Under Delaware's constitutional scheme, the General Assembly's unlimited power to legislate will be restrained only by limitations imposed in either the state or national constitution. [15]

The enabling statute explicitly declares that authorities created under the act are "public bodies." [16] The Amendment in question was directed to ensuring that such water and sewer authorities would not be able to rely on what some purported to be a "loophole" to justify a refusal to comply with a FOIA request. Curative legislation of this kind does not violate the separation of powers. It is well within the General Assembly's

---

[8] Del. Op. Att'y Gen. 11-IIB03, 2011 Del. AG LEXIS 3, 2011 WL 1428938 (March 16, 2011).

[9] Del. Const. Article II, Section 1.

[10] *E.g.*, *State ex rel. James v. Schorr*, 45 Del. 18, 65 A.2d 810, 812 (Del. 1948).

[11] *Collison v. State ex rel. Green*, 2 A.2d 97, 108, 39 Del. 460, 9 W.W. Harr. 460, (Del. 1938).

[12] *New Castle County Council v. State*, 688 A.2d 888, 891 (Del. Nov. 8, 1996).

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] 16 *Del. C.* §1402(a)(1).

Authority. [17] Such legislation serves the dual purpose of clarifying public policy and the intent of the law. [18]

Defendant next argues that the present situation invokes usage of the fundamental rules of statutory construction. A court engages in statutory construction and interpretation only when the statutory language in question is ambiguous. In some cases, a court may engage in this exercise when "giving a literal interpretation to words of the statute would lead to such unreasonable absurd consequences as to compel a conviction that. . . could not have been intended by the Legislature." [19] Neither of these scenarios is presented by the case at hand. The General Assembly could not have been more clear in amending the statute. The results are exactly what were expected and intended. Thus, the rules and cases cited by Defendant are inapposite to the present case.

Defendant's final argument associated with this question is that allowing CWSWA to be designated a "public body" under FOIA creates a slippery slope. Some private corporations are engaged in exactly the same business, funded by the same revenue source as CWSWA. Such a scenario, would allegedly empower [*12] the General Assembly to extend the requirements of FOIA to private corporations. While this "slippery slope" argument does give the Court some pause, Plaintiff's position on this issue is much stronger. As noted, the General Assembly has practically "unlimited" power to legislate. The language of the statute is clear and unambiguous. There is no question that the General Assembly intended to bring CWSWA within the definition of a "public body." If the Defendant cannot demonstrate that the amendment violates the constitutional limits on the General Assembly's power to legislate, the Court will sustain the judgment of the legislature. [20] Therefore, the Court finds that The Camden-Wyoming Sewer and Water Authority is a "public body" subject to the requirements of the FOIA.

3. Is The Camden-Wyoming Sewer and Water Authority, as a "public body", obliged to disclose its employees' salaries?

Whether information is subject to disclosure under FOIA depends upon whether that information is a "public record." According to *29 Del. C. §10002(k)*, information constitutes a "public record" [*13] when it meets the following three-step test:

(1) The information is "owned, made, used, retained, received, produced, composed, drafted or otherwise complied or collected by any public body," and

(2) The information relates "in any way to public business," and

(3) Does not fall within an exception. [21]

The information Ms. Williams requested meets all three prongs of the test. Salary information would be completely within the creation and control of CWSWA such that the first prong is met. Given the CWSWA's position as a public body, one cannot dispute that salary information relates in some way to public business, satisfying the second prong. Finally, such information would not fall within any of the exceptions.

Delaware case law solidly supports the Plaintiff's position on this issue. The Court in *Gannett Co., Inc. v. Christian* held that salary information must be disclosed under FOIA, because there was no right to privacy in salary information. [22] Previous legal analysis by the Attorney General's Office also found that salaries paid by public taxpayer funds must be disclosed. [23]

The Defendant aims to distinguish this case from *Gannett* based on the specific language used by the Court in that case in its decision: "it is generally recognized that the public has a legitimate interest in knowing the salaries of persons who are paid with public funds and public employees have no right of privacy over this information." [24] CWSWA argues that this language implies that disclosure is required only of the salaries of persons paid with traditionally defined public funds, or who are public employees. CWSWA's employees are not public employees, nor are they paid with traditionally defined public

---

[17] *Sierra Club v. DNREC*, 919 A.2d 547 (Del. Ch. 2007), **[*11]** *aff'd* ***919 A.2d 547 (Del. 2007)***.

[18] *Id.*

[19] *Coastal Barge Corp. v. Coastal Zone Industrial Control Board*, 492 A.2d 1242, 1246 (Del. Super. 1985).

[20] *New Castle County Council v. State*, 688 A.2d 888, 891 (Del. 1996).

[21] *29 Del. C.* §10002(k)(1)-(19).

[22] *Gannett Co., v. Christian*, 1983 Del. Super. LEXIS 791, 1983 WL 473048 (Del. Super. Aug. 19, 1983).

[23] Del. Op. Att'y Gen. 3W-077 (Aug. 4, 1977) **[*14]** ; Del. Op. Att'y Gen. 3W-023(March 10, 1978); Del. Op. Att'y Gen. 02-IB24 (Oct. 1, 2002); Del. Op. Att'y Gen. 06-IB11, 2006 Del. AG LEXIS 9 (May 31, 2006).

[24] *Gannett*, 1983 Del. Super. LEXIS 791, 1983 WL 473048, at *1.

funds. That is not dispositive of the issue. A statement by the Court requiring disclosure of the salaries of public employees or those paid with public funds, does not necessarily preclude disclosure of the salaries of non-public employees or those not paid with public funds.

Despite CWSWA's contention that case law actually makes the answer to the question less clear, the Court [*15] needs only to look to the governing statues to arrive at a conclusion. The enabling legislation sets forth a mandate of disclosure and access to financial records. [25] According to the statute, there are many records, including salary information, that CWSWA will have to maintain and make available to the public. [26] Furthermore, the Towns of Camden and Wyoming, as the founding municipalities, must be afforded full access to all of Defendant's books and records. [27] The General Assembly was very clear about its intention. Chapter 14 defines both the sources of funding and still mandates that financial information must be fully disclosed, consistent with the duty a public body would have under FOIA. [28] The Court finds that the Defendant must disclose the requested information as it is within FOIA's definition of "public records."

4. Does FOIA, as amended, apply to documents created/in existence before the amendment made The Camden-Wyoming Sewer and Water Authority a "public body"?

CWSWA argues that it should not be ordered to produce documents in response to the FOIA request filed by Ms. Williams, because she requested [*16] only "salary information," not documents. This is no more than a quibble over semantics, which is ineffective. Still, the Defendant contends that any documents created before April 19, 2011, or that pertain to events occurring prior to that date, are not subject to FOIA's disclosure requirement. This argument is based on the fact that prior to the Amendment in question, the CWSWA was not considered within FOIA's definition of a "public body." [29]

There is no support for such a refusal to disclose found in either Chapter 14 or Chapter 100. In fact, the language found in the statutes completely refutes the Defendant's position. CWSWA already had an ongoing duty to maintain certain records, including salaries, for public inspection. [30] The duty was not affected by the FOIA amendment, because it merely established that CWSWA was a "public body."

The applicable statute makes clear that the intention is to cover "all public records." [31] In fact, FOIA includes specific language demonstrating that it does not matter whether the record is in active use or storage. [32] Furthermore, there is no time frame or time [*17] period limitation present in FOIA. Defendant attempts to argue that forcing this disclosure is a retroactive application of FOIA. That is not correct. The FOIA language states the intention of the General Assembly to include past and current documents. Thus, the duty to produce records under FOIA applies to any and all applicable records existing on the date the request was made. The time or date when those records were created is irrelevant.

5. Does the Attorney General have the authority to pursue this matter on behalf of Georgette Williams-which is really to ask: is the entity for whom or for which this action is undertaken a "citizen"?

29 Del. C. §10005(e) explicitly authorizes the Attorney General of Delaware to bring suit on behalf of a "citizen," to compel compliance with FOIA. The Defendant alleges Ms. Williams was acting in her official capacity as town councilperson and treasurer, and therefore does not fall within the definition of citizen. CWSWA does not dispute that Georgette Williams is a "citizen." Instead, Defendant argues that Ms. Williams made the request in her official capacity. Thus, she was allegedly acting on behalf of the [*18] Town of Wyoming. Defendant's position is that the Town, as a non-citizen, should be represented by its own solicitor, and not the Attorney General's Office. For these reasons, the Defendant believes that the Attorney General should have declined to pursue this matter, because he has no standing to bring the case.

In support of this argument, the Defendant cites to *Koyste v. Delaware State Police* and *Office of Public Defenders v. Delaware*

---

[25] 16 *Del C.* §1405(e).

[26] *Id.*

[27] 16 *Del. C.* §1405(e).

[28] 16 *Del C.* §1401-1421.

[29] Del. Op. Att'y Gen. 11-IIB03, 2011 Del. AG LEXIS 3, 2011 WL 1428938 (March 16, 2011).

[30] 16 *Del. C.* §1405(e).

[31] 29 *Del. C.* §10003(a).

[32] *Id.* §10003(a).

State Police in an attempt to draw a comparison to the present case. [33] In *Koyste*, the Plaintiff was an employee and representative of the Federal Public Defenders Office. [34] His request was a circuitous attempt to gain access to state police files and records, in order to prepare a defense for a client who had already been denied access to the same materials on three separate occasions. [35] The reason for the denial was that the documents fell under the pending litigation exemption. [36] Attempting to act as a "citizen" to obtain these documents for defense purposes is not what FOIA was intended to allow, the Court held. [37]

In [*19] *Office of Public Defenders*, one of the Assistant Public Defenders asked for documents from the state police, in both her official and individual capacities. [38] The documents in question (training manuals and standard operating procedures) were desired in relation to pending litigation. [39] The Court made clear that the documents would not be disclosed to the Public Defender, though they could potentially be disclosed to a "citizen." [40] The facts in that case did not support the claim by the Assistant to standing as an individual citizen. [41] The Assistant was clearly "asserting citizenship only to avoid the bar on her employer imposed by the Act's standing requirement." [42] A contention evidenced by the fact that the Assistant stated in the Complaint that she was "acting on behalf of the Public Defender." [43]

The present case is easily distinguished from the aforementioned examples. Most importantly, Ms. Williams did not request information protected from required disclosure by any exemption. Furthermore, [*20] she was acting in her individual capacity, not on behalf or at the behest of, an entity. Finally, as far as the pleadings show, Ms. Williams was not trying to circumvent prior court rulings, or to act inappropriately, in making her request.

Defendant's next argument alleges that the original request, made by Georgette Williams, was made in her official capacity. That request is not an aspect of this case. There is but one request at issue here: the request made on May 9, 2011. Documents related to other matters and related allegations are outside of these pleadings. Facts and arguments outside the pleadings cannot be considered in a motion for judgment on the pleadings. [44] The additional documents submitted by the Defendant in support of this contention will not be considered by this Court in deciding Plaintiff's Motion.

The Defendant also attempts to speculate as to Ms. Williams' motives, based on her affiliation with the town council. Ms. Williams does not lose her rights as a citizen by virtue of holding a public office, a point made exceptionally clear by the United States Supreme Court in a discussion [*21] of the federal FOIA. [45] In that case, the Court said that the decision to allow access to records "cannot turn on the purposes for which the [FOIA] request is made." The Court goes on to say that "the identity of the requesting party has no bearing on the merits of his/her FOIA request." [46] This position is cited by the Attorney General's Office in a 2006 opinion. [47] "Under FOIA, a record

---

[33] *Koyste v. Delaware State Police*, 2001 Del. Super. LEXIS 352, 2001 WL 1198950 (Del. Super. Sept. 18, 2001); *Office of Public Defenders v. Delaware State Police*, 2003 Del. Super. LEXIS 111, 2003 WL 1769758 (Del. Super. March 31, 2003).

[34] Koyste, 2001 Del. Super. LEXIS 352, 2001 WL 1198950, at *2.

[35] 2001 Del. Super. LEXIS 352, [WL] at *3.

[36] *Id.*

[37] 29 *Del. C.* §10001.

[38] *Office of Public Defenders v. Delaware State Police*, 2003 Del. Super. LEXIS 111, 2003 WL 1769758, at *1 (Del. Super. March 31, 2003).

[39] 2003 Del. Super. LEXIS 111, [WL] at *1.

[40] *Id.*

[41] 2003 Del. Super. LEXIS 111, [WL] at *4.

[42] *Id.*

[43] *Office of Public Defenders*, 2003 Del. Super. LEXIS 111, 2003 WL 1769758, at *4.

[44] *Mergenthaler v. Asbestos Corp. of America*, 500 A.2d 1357, 1361 (Del. Super. 1985).

[45] *United States Dep't. of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 771, 109 S. Ct. 1468, 103 L. Ed. 2d 774 (1988).

[46] *Id.*

[47] Del. Op. Att'y Gen. 06-IB09, 2006 Del. AG LEXIS 7, 2006 WL 1779490, at *5 (April 25, 2006).

is public, or it is not." [48] Public bodies are provided no discretion to require a person to state the purpose for a request. Such a requirement could have a potentially chilling effect on the exercise of rights, by citizens, under FOIA. [49]

CONCLUSION

For the forgoing reasons, Plaintiff's Motion for Judgment on the Pleadings is **GRANTED** as to the requests for a declaratory judgment and writ of mandamus, but **DENIED** as to Plaintiff's request for the award of attorneys' fees. Costs are awarded to Plaintiff.

SO ORDERED this 7th day of November, 2012.

/s/ Robert B. Young

J.

[48] *Id.*

[49] *Id.*