UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AMERICAN CIVIL LIBERTIES UNION, *et al.* Plaintiffs, v. UNITED STATES DEPARTMENT OF JUSTICE Defendant.	No. 08-cv-1157 (JR)

PLAINTIFFS' MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT, AND IN SUPPORT OF PLAINTIFFS' CROSS-MOTION FOR SUMMARY JUDGMENT

In this action under the Freedom of Information Act, plaintiffs seek the disclosure of records regarding the government's tracking of the location of individuals' cellular telephones without a judicial determination of probable cause. Hundreds of millions of Americans now carry cell phones. Such surveillance has been the subject of widespread media attention. The ACLU agrees with the magistrate bench of this Court that federal statutory law does not authorize the government to track cell phones without a showing of probable cause. The ACLU filed its FOIA request to shed light on this controversial and legally dubious surveillance practice.

Specifically at issue in this proceeding are two categories of information: (1) the case names and docket numbers (including court) of criminal prosecutions brought against individuals whom the government had tracked without a prior judicial determination of probable cause, and (2) certain records concerning the government's policies, procedures and practices for cell phone tracking. Defendant has failed adequately to search for responsive material and has failed to

carry its burden of justifying its assertions of exemption regarding certain other records. This Court should order defendant to conduct an adequate search and to release certain documents.

FACTUAL BACKGROUND

Over the past decade, cell phones have gone from being a luxury good to an essential communications device. As of December 2008, 270 million people—87 % of the United States population—carried a wireless electronic communication device. CTIA, *CTIA's Semi-Annual Wireless Industry Survey, available at* http://files.ctia.org/pdf/CTIA_Survey_Year-End_2008_Graphics.pdf (last viewed July 9, 2009). While cell phones are best known as devices used to make voice calls and send text messages, they are also capable of being used as tracking devices. This capability is of obvious interest to law enforcement agents. It raises equally obvious concerns about privacy, for people carry their phones in their pockets and purses as they traverse public and private spaces.

Cell phone carriers (i.e. Verizon, T-Mobile, etc.) are technically capable of tracking cell phones. According to defendant's *Electronic Surveillance Manual*, "[i]n order to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular phone, the portion of the tower facing the phone, and often the signal strength of the phone." DOJ, *Electronic Surveillance Manual* (2005) at 41, *available at* http://www.usdoj.gov/criminal/foia/docs/elec-sur-manual.pdf (last viewed July 13, 2009). If a cell phone has GPS ("Global Positioning System") capability—GPS is a device which communicates with a network of satellites, generating information about the location of the phone—the carrier may also be able to collect more precise information about the phone's location. *See* Sahl Declaration, dated July 24, 2009, Exhibit 1 (exhibits to the Sahl Decl. are

hereinafter cited as "Exh.") (Mark Eckenweiler, *Current Legal Issues in Wireless Phone Location*) at p. 4.

The government distinguishes between two types of tracking data it can obtain through carriers. The government generally refers to the first type as Cell Site data.[1] It appears that when the government seeks Cell Site data, it asks the carrier to tell it which cell phone tower the target phone is nearest, as well as which portion of the tower the phone is facing.[2] Because the physical location of the towers is known, knowing what tower a phone is nearest gives the phone's approximate location. While sometimes the government requests only the phone's location at the beginning and end of phone calls,[3] at other times the government requests the phone's location during the course of phone calls,[4] and in still other cases, the government requests the phone's location whenever it is turned on.[5] According to defendant, the precision of Cell Site data depends on how closely grouped the towers are in a given area.[6] Defendant can obtain both historical and real-time Cell Site data. Exh. 1 at p. 4.

---

[1] S*ee, e.g., In Re Application Of The United States Of America For An Order For Disclosure Of Telecommunications Records And Authorizing The Use Of A Pen Register And Trap And Trace*, 405 F.Supp.2d 435 (S.D.N.Y. 2005).

[2] *See, e.g., In the Matter of the Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 412 F. Supp.2d 947 (E.D. Wis. 2006).

[3] S*ee, e.g., In Re Application Of The United States Of America For An Order For Disclosure Of Telecommunications Records And Authorizing The Use Of A Pen Register And Trap And Trace*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005),

[4] S*ee, e.g., In The Matter Of An Application Of The United States For An Order (1) Authorizing The Use Of A Pen Register And A Trap And Trace Device And (2) Authorizing Release Of Subscriber Information And/Or Cell Site Information*, 396 F.Supp.2d 294, 295 (E.D.N.Y. 2005).

[5] *See, e.g., In The Matter Of The Application Of The United States Of America For An Order Authorizing The Installation And Use Of A Pen Register And A Caller Identification System On Telephone Numbers [Sealed] And [Sealed] And The Production Of Real Time Cell Site Information*, 402 F. Supp.2d 597 (D. Md. 2005).

[6] Defendant asserts that cell tower service radius ranges from 200 meters to 30 km. Exh. 1 at p.4.

The second type of cell phone tracking information defendant can obtain is Latitude/Longitude or "Lat/Long" data. Exh. 1 at 12. According to defendant, there are two distinct forms of Lat/Long data. *Id.* The first is GPS. FCC rules require GPS to be accurate within 50 meters for 67% of calls and to 150 meters for 95% of calls. *Id.* The second form of Lat/Long Data is "network solution" data, derived by the service provider by triangulating the signal characteristics of the phone relative to one or more towers. *Id.* at 6. FCC rules require accuracy to 100 m for 67% of calls and to 300 m for 95% of calls. *Id.* According to DOJ, Lat/Long Data is generally only available in real time. *Id.* at 10.

Defendant has taken the view that the evidentiary standard it must meet to obtain court orders to track cell phones depends on whether it seeks Cell Site or Lat/Long data. Defendant's Office of Enforcement Operations "recommends invoking Rule 41 [probable cause] to obtain lat-long data" because "[a]nything less presents significant risks of suppression." *Id.* at 15. Defendant argues that it may constitutionally obtain Cell Site data so long as it provides "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation."[7]

Plaintiffs believe that the Fourth Amendment compels the government to obtain a warrant for all cell phone tracking. Law enforcement tracking of individuals "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance." *United States v. Karo*, 468 U.S. 705, 707 (1984). Because cell phone users

[7] Brief for the United States at 10, Dkt. No. 00316415313, *In The Matter Of The Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government*, No. 08-4227 (3d Cir. pending) (historical Cell Site data); *In re Application Of The United States Of America For An Order For Disclosure Of Telecommunications Records And Authorizing The Use Of A Pen Register And Trap And Trace*, 405 F. Supp. 2d 435, 444 (S.D.N.Y. 2005) (prospective Cell Site data).

typically carry their phones wherever they go, and traverse both public and private spaces as they travel, *Karo* is implicated and the government must obtain a warrant.

The extent to which United States Attorney's Offices (USAOs) around the country heed DOJ's advice regarding the applicable legal standard is unclear, and it is largely unknown whether courts are accepting or rejecting defendant's position that probable cause is unnecessary. Applications for cell phone tracking are generally filed under seal and, unless a magistrate judge goes out of his or her way to publish an opinion, the court's response to the application is also secret. The net result is that the body of law governing when the government may secretly track an individual's cell phones is itself largely secret. It is a secret law of secret surveillance.

With regard to Lat/Long tracking, there are no publicly available opinions specifically addressing whether this form of cell phone tracking can take place in the absence of a warrant. This FOIA uncovered the fact that the USAOs for the District of New Jersey and Southern District of Florida are obtaining court permission to engage in GPS or similarly precise cell phone tracking without a warrant. Exh. 2 (Letter from W.G. Stewart, II to C. Crump re: the Southern District of Florida (December 31, 2008)) at p.1 and Exh. 3 (Letter from W.G. Stewart, II to C. Crump re: the District of New Jersey (December 31, 2008)) at p.1. Thus, not all USAOs heed defendant's apparently discretionary recommendation to obtain a warrant when seeking Lat/Long data.

With regard to Cell Site data, plaintiffs have been able to identify opinions on the issue in some districts in 12 states, Washington D.C. and Puerto Rico.[8] For the vast majority of the

[8] *See, e.g., In The Matter Of The Application Of The United States Of America For An Order Authorizing The Release Of Prospective Cell Site Information*, 407 F.Supp.2d 134 (D. D.C. 2006); *In re U.S. For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government*, 534 F.Supp.2d 585 (W.D.Pa. 2008), a*ff'd*, 2008 Wl 4191511 (W.D.Pa. 2008), *Appeal Docketed*, No. 08-4227 (3rd Cir. Oct. 22, 2008); *In re*

country, the legal standard to which the government is held when it seeks to track people through their cell phones is unknown.

According to defendant, magistrate judges in at least twelve districts have rejected the government's position and held that the government needs to show probable cause to engage in Cell Site tracking. Exh. 1 at 9. In 2005, for example, all of the magistrates of this Court signed a joint order stating that they would no longer grant cell phone tracking applications based on less

---

Application Of U.S. For An Order Authorizing Use Of A Pen Register With Caller Identification Device Cell Site Location Authority On A Cellular Telephone, 2009 Wl 159187 (S.D.N.Y. 2009); *In re U.S. For An Order*, 433 F.Supp.2d 804 (S.D. Tex. 2006); *In re Application Of United States*, 497 F. Supp. 2d 301; (D.P.R. 2007); *In re Applications Of U.S. For An Order Authorizing Continued Use Of A Pen Register And Trap And Trace With Caller I.D.*, 530 F. Supp. 2d 367 (D. Mass 2007); *In re Application For An Order Authorizing The Installation And Use Of A Pen Register And Directing The Disclosure Of Telecomms. Records For Cellular Phone Assigned The No. [Sealed]*, 439 F. Supp. 2d 456, 457 (D. Md. 2006); *In re Application For An Order Authorizing The Extension And Use Of A Pen Register Device Etc*, 2007 U.S. Dist. Lexis 11682, 2007 Wl 397129 (E.D. Ca. Feb. 1, 2007); *In re Application Of U.S. For Order Re-Authorizing Use Of A Pen Register And Trap And Trace Device With Prospective Cell-Site Information Slip Copy*, 2009 Wl 1594003 (E.D.N.Y. 2009); *In re The Application Of The U.S. For An Order Authorizing The Installation And Use Of A Pen Register With Caller Identification Device And Cell Site Location Authority On A Certain Cellular Telephone*, 415 F. Supp. 2d 663 (S.D.W. Va. 2006); *In re Application Of The U.S. For An Order: (1) Authorizing The Installation And Use Of A Pen Register And Trap And Trace Device; And (2) Authorizing Release Of Subscriber Information And/Or Cell Site Information*, 411 F. Supp. 2d 678 (W.D. La. Jan. 26, 2006); *In re The Application Of The U.S. For An Order Authorizing The Installation And Use Of A Pen Register And/Or Trap And Trace For Mobile Identification Number (585) 111-1111 And The Disclosure Of Subscriber And Activity Information Under 18 U.S.C. 2703*, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); *In The Matter Of The Application Of The United States Of America For An Order: (1) Authorizing The Installation And Use Of A Pen Register And Trap And Trace Device; (2) Authorizing The Release Of Subscriber And Other Information; And (3) Authorizing The Disclosure Of Location-Based Services* and *In The Matter Of The Application Of The United States Of America For An Order: (1) Authorizing The Installation And Use Of A Pen Register And Trap And Trace Device; (2) Authorizing The Release Of Subscriber And Other Information; And (3) Location Of Cell Site Origination And/Or Termination*, Case Nos. 1:06-Mc-6, 1:06-Mc-7, 2006 WL 1876847 (N.D. Ind. July 5, 2006) (Unreported); *In The Matter Of The Application Of The United States Of America For An Order Authorizing The Disclosure Of Prospective Cell Site Information*, 412 F. Supp.2d 947 (E.D.Wis. 2006), *aff'd*, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (unpublished); *United States v. Bermudez*, 2006 WL 3197181 (S.D. Ind. June 30, 2006); *U.S. v. Suarez-Blanca*, 2008 WL 4200156 (N.D.Ga. 2008).

than probable cause, at least not unless the government came up with a new legal theory. *In re Applications of U.S. for Orders Authorizing Disclosure of Cell Cite Information*, 2005 WL 3658531 (D.D.C. 2005). Courts have also been cognizant of the serious constitutional issues such tracking raises. The court in *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) agreed that "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."

As far as plaintiffs have been able to determine, all but two of the published decisions on cell phone tracking arose at the application stage.[9] The extent to which individuals who are the subjects of cell phone tracking are subsequently prosecuted is unknown. There is no information on how often cell phone tracking allows law enforcement agents to apprehend criminals, in what sorts of circumstances cell phone tracking is an advantageous law enforcement technique, and whether any resulting prosecutions are successful. There is little information about whether motions to suppress evidence obtained through warrantless cell phone tracking have been filed or granted.

Despite a dearth of public information, there has been a high level of public interest in cell phone tracking and the attendant privacy concerns.[10]

---

[9] The two that did not are *U.S. v. Bermudez*, 2006 WL 3197181 (S.D. Ind. June 30, 2006); *U.S. v. Suarez-Blanca*, 2008 WL 4200156 (N.D.Ga. April 21, 2008).

[10] *See, e.g. Cellphone Data Raises New Questions in Safety vs. Privacy Debate*, Seattle Post-Intelligencer, July 8, 2009, *available at* 2009 WLNR 13063554; Anne Barnard, *Growing Presence in the Courtroom: Cellphone Data as Witness*, New York Times, July 6, 2009, at A16, *available at* 2009 WLNR 12835882; Nancy Remsen, *Free Speech Faces New Challenges From Technology*, Burlington Free Press, June 29, 2009; Al Gidari, *NPR On the Media: Where I'm Calling From*, National Public Radio Interview, May 8, 2009, *transcript available at* http://www.onthemedia.org/transcripts/2009/05/08/05; Peter J. Sampson and Claire Heininger,

PROCEDURAL BACKGROUND

On November 29, 2007, the ACLU filed FOIA requests with the Drug Enforcement Administration (DEA) and the Executive Office For United States Attorneys (EOUSA). Dkt. No. 26-4 (Letter from C. Crump to EOUSA, dated November 29, 2007), and Dkt. No. 26-5 (Letter from C. Crump to DEA, dated November 29, 2007). The requests sought, *inter alia*:

> 1. Policies, procedures, and practices followed to obtain mobile phone location information for law enforcement purposes;
>
> * * *
>
> 5. The case name, docket number, and court of all criminal prosecutions, current or past, of individuals who were tracked using mobile location data, where the government did not first secure a warrant based on probable cause for such data.

Id. EOUSA is in charge of FOIA compliance for United States Attorneys' Offices. Dkt. No. 26-7 (Declaration of Karen Finnegan) at ¶ 1. In addition to asking EOUSA to search for responsive records within its own offices, plaintiffs asked it to search for responsive records in the United States Attorneys' Offices in six states and the District of Columbia. Dkt. No. 26-4.

On July 1, 2008, plaintiffs sued to enforce their request. Dkt. No. 1 ¶ 24. On November 3, 2008, defendant filed a scheduling report, proposing to complete processing of Category 1 by November 30, 2008 and to produce any non-exempt material by December 31, 2008. Dkt. No. 17 at 2-3. Defendant proposed to respond to Category 5 by creating a list of the case names and docket numbers (including court) of cases in which individuals were prosecuted subsequent to

---

ACLU Claims Christie OK'd GPS Tracking, New Jersey Record, April 24, 2009, at A06, *available at* 2009 WLNR 9109948; Ryan Singel, *Cops Need Warrant for Cellphone Location Data, Judge Rules*, Wired, Sept. 11, 2008, *at* http://www.wired.com/threatlevel/2008/09/cops-need-warra/; *Justice Department Defends Use of Cell-Phone Tracking Data*, Fox News, Nov. 24, 2007, *at* http://www.foxnews.com/story/0,2933,312647,00.html; *Who's Tracking Your Cell Calls: Enhanced 911, and Other Services are Turning Phones into a Location Device*, The Post-Tribune, Nov. 23, 2007, at A12, *available at* 2007 WLNR 24406529; Ellen Nakashima, *Cellphone Tracking Powers on Request*, Washington Post, Page A01, Nov. 23, 2007; Editorial, *Phone Tech Raises Privacy Concerns*, United Press International, Nov. 23, 2007 *at* http://www.upi.com/Top_News/2007/11/23/Phone-tech-raises-privacy-concerns/UPI-24661195824144/.

warrantless cell phone tracking, which it would then withhold pursuant to Exemptions 6 and 7(C). *Id.* at 4-5.

The Court approved the proposal. Dkt. No. 18. After certain records were produced, on March 20, 2009, the parties filed a joint motion stating that, "the sole issue remaining for adjudication in this action is whether the exemption[s] . . . have been applied correctly to the records responsive to Category 1 of plaintiffs' FOIA request dated November 27, 2007, and the information responsive to Category 5 of plaintiff's request." Dkt. No. 24. On May 29, 2009, defendant filed its motion for summary judgment.

Category 5: The Records Now at Issue

With regard to Category 5 ("The case name, docket number, and court of all criminal prosecutions, current or past, of individuals who were tracked using mobile location data, where the government did not first secure a warrant based on probable cause for such data"), defendant has generated a list of responsive information, which it claims is exempt from disclosure under Exemptions 6 and 7(C). *See* Dkt. No. 26-7 (Finnegan Decl.) at ¶ 5.

Category 1: The Records Now At Issue

With regard to Category 1 ("Policies, procedures, and practices followed to obtain mobile phone location information for law enforcement purposes"), defendant has produced a revised *Vaughn* index. Exh. 4.[11] Of the 72 documents listed on the *Vaughn*, plaintiffs seek only 27.[12] These 27 documents can be grouped as follows:

[11] Whenever plaintiffs refer to defendant's *Vaughn*, they are referring to the revised *Vaughn* index defendant provided plaintiffs, which is attached to the Sahl Decl. as Exh. 4. The pages of the index are not numbered; citations are to the numbers in the left hand column ("Entries.")

[12] Consequently, this Court need not consider the arguments presented by defendant on the following pages of its memorandum: 8-10 (discussing Exemption 3), 10-14 (discussing Exemption 5), and 23-24 (discussing Exemption 7(D)).

- **Case names and docket numbers of applications.** While Category 5 sought case names and docket numbers of *prosecutions*, this category encompasses case names and docket numbers of *applications,* which defendant has also withheld.

- **Application for cell phone tracking.** Defendant withheld a final application to engage in cell phone tracking. Exh. 4 at Entry 67. Plaintiffs seek the release of the portion of the application stating the legal standard defendant thinks is applicable in the jurisdiction at issue.

- **Withheld portions of template applications**. According to defendant's *Vaughn*, some of the Category 1 documents consist of template applications that Assistant United States Attorneys fill out and submit to courts when requesting cell phone tracking authority. *Vaughn* Index at Entries 2, 3, 26-29, 32-24, 68-71. Plaintiffs challenge defendant's decision to withhold these templates in part.

Finally, as to Category 1, review of the *Vaughn* raises substantial questions about whether defendant conducted an adequate search. Plaintiffs ask the Court to order defendants to conduct a further, narrowly targeted search for final versions of 13 draft documents.

ARGUMENT

I. THE FREEDOM OF INFORMATION ACT AND STANDARD OF REVIEW

The Freedom of Information Act is intended to safeguard the right of the American people to know "what their Government is up to." *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 773 (1989). Grounded in the "fundamental principle of public access to Government documents," *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151 (1989), the central purpose of the statute is "to ensure 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." *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978).

A court may grant summary judgment where the pleadings, affidavits and declarations show that there is no genuine issue of material fact and that the moving party is entitled to judgment as a matter of law. FRCP 56(c). In considering a motion for summary judgment under FOIA, the Court must conduct a *de novo* review of the exemptions claimed by the government. 5 U.S.C. § 552(a)(4)(B). In the FOIA context, "*de novo* review requires the court to ascertain whether the agency has sustained its burden of demonstrating that the documents requested . . . are exempt from disclosure under the FOIA." *Assassination Archives & Research Ctr. v. Cent. Intelligence Agency*, 334 F.3d 55, 57 (D.C. Cir. 2003) (internal quotation marks omitted).

In a FOIA matter, if a court is to grant summary judgment solely on the basis of information provided by the agency in affidavits or declarations, these documents must satisfy the following requirements: first, they must describe "the documents and the justifications for nondisclosure with reasonably specific detail" and must be non-conclusory; second, they must "demonstrate that the information withheld logically fall within the claimed exemption;" and finally they must not be "controverted by either contrary evidence in the record nor by evidence of agency bad faith." *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981). Summary judgment is appropriate only where an agency proves it has fully discharged its FOIA obligations. *Moore v. Aspin*, 916 F. Supp 32, 35 (D.D.C. 1996).

Records requested under FOIA must be disclosed unless they fall squarely within one of the statute's exemptions, which "must be narrowly construed." *Rose*, 425 U.S. at 361. An agency's declaration and *Vaughn* index will be deemed adequate only to the extent they provide "reasonable specificity of detail rather than merely conclusory statements, and if they are not

called into question by contradictory evidence in the record or by evidence of agency bad faith." *Gallant v. N.L.R.B.*, 26 F.3d 168, 171 (D.C. Cir. 1994). Even where a FOIA exemption is found to apply, "[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." 5 U.S.C. § 552(b).

II. PLAINTIFFS ARE ENTITLED TO THE CATEGORY 5 INFORMATION.

In Category 5 of their FOIA request, plaintiffs sought "[t]he case name, docket number, and court of all criminal prosecutions, current or past, of individuals who were tracked using mobile location data, where the government did not first secure a warrant based on probable cause for such data." Dkt. No. 26-5. Pursuant to defendant's agreement, a list of such case names and docket numbers now exists. That list is what is at issue under Category 5. Defendant claims the information can be withheld pursuant to Exemptions 6 and 7(C).

A. Defendant Cannot Withhold Case Names and Docket Numbers Pursuant To Exemption 7(C).

Exemption 7(C) permits the government to withhold "records or information compiled for law enforcement purposes" that "could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C).[13] Determining whether this exemption applies requires balancing the privacy interest of the individual implicated by the record in question against the public interest in the release of the record. *Reporters Comm.*, 489 U.S. at 776. The burden is on the agency to prove that disclosure would constitute an invasion of personal privacy, and that such invasion would be unwarranted. *See Fed. Bureau of Investigation v. Abramson*, 456 U.S. 615, 632 (1982). Where the public interest outweighs the privacy interest, the invasion of that interest is not unwarranted and the records cannot be

[13] Plaintiffs concede that the records at issue here were "compiled for law enforcement purposes."

withheld. *Fed. Labor Relations Auth. v. U.S. Dep't of Veterans Affairs*, 958 F.2d 503, 509-10 (2d Cir. 1992).

1. Disclosure Of The Requested Information Would Not Invade Any Legitimate Privacy Interest.

Defendant argues that its list of case names and docket numbers is properly withheld because "[b]eing linked with any law enforcement investigation carries a strong negative connotation. To release the identities of those individuals to the public as subject or suspects of a criminal investigation could subject them to harassment or embarrassment, as well as undue public attention." Dkt. No. 26-7 (Finnegan Decl.) at ¶ 91. This argument has nothing to do with the information plaintiffs are seeking. Plaintiffs are not seeking information about people of mere "investigative" interest, or who are mere "subjects or suspects of a criminal investigation." *Id.* Plaintiffs seek information about criminal cases that have been filed in federal courts.

The considerable privacy interest of an individual in the fact that he was once of investigative interest is categorically different from the minimal privacy interest of an individual in the fact that he was actually the subject of a public prosecution.[14] Criminal defendants become "public persons" by virtue of their arrest or indictment. *Tennessean Newspaper, Inc. v. Levi*, 403 F. Supp. 1318, 1321 (M.D. Tenn. 1975) ("Since an individual's right of privacy is essentially a protection relating to his or her private life, this right becomes limited and qualified for arrested or indicted individuals, who are essentially public personages."). Disclosing identifying information, such as a defendant's name or the circumstances of his arrest, "does not

[14] Plaintiffs acknowledge that individuals have, as a categorical matter, some privacy interest when their names are mentioned in law enforcement records. *Reporters Committee*, 489 U.S. at 780. When the proffered privacy interest is that of a criminal defendant in the case name and docket number of his prosecution, however, that interest is at its nadir.

involve substantial privacy concerns." *Id.* Defendant is well aware of this, as it regularly holds press conferences and issues press releases naming the defendants when it files criminal cases.[15]

Concluding that the interest in disclosure outweighs the privacy interest here makes sense given the purpose of Exemption 7(C), which is not to protect against the disclosure of all records that may have any impact on the privacy interest of an individuals, but only against the disclosure of records where disclosure may result in an "*unwarranted* invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C) (emphasis added). Here, the government can hardly argue that the association with criminal activity is unwarranted. By definition, the government believes beyond a reasonable doubt that these individuals are not only associated with criminal activity, but are perpetrators of it.

The requested information reveals no more than the fact of a criminal prosecution against a person, which is already a matter of public record. "The interests in privacy fade when the information involved already appears on the public record." *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 494-495 (1975). Although plaintiffs cannot know for certain that each of the case names and docket numbers they seek is publicly available, it seems highly unlikely that any of them are not because, absent extraordinary circumstances, criminal prosecutions in this country are public. *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 573 (1980).

With respect to the closely analogous Exemption 6, which protects "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," 5. U.S.C. § 552(b)(6), the D.C. Circuit has held that the FOIA

---

[15] *See, e.g.*, the following recent press releases from the office of the United States Attorney for the District of Columbia:
http://www.usdoj.gov/usao/dc/Press_Releases/2009%20Archives/April/09-105.pdf
http://www.usdoj.gov/usao/dc/Press_Releases/2009%20Archives/April/09-103.pdf
http://www.usdoj.gov/usao/dc/Press_Releases/2009%20Archives/April/09-093.pdf

analysis "must include consideration of any interest the individual might have in the release of the information, particularly when the individuals who are 'protected' under this exemption are likely unaware of the information that could benefit them." *Lepelletier v. FDIC*, 164 F.3d 37, 48 (D.C. Cir. 1999). In *Lepelletier*, the circuit considered a FOIA request for the names of depositors with unclaimed funds at banks for which the Federal Deposit Insurance Corporation was the receiver. *Id.* at 39. The circuit ordered the names released, stating, "it is overly paternalistic to insist upon protecting an individual's privacy interest when there is good reason to believe that he or she would rather have both the publicity and the money than have neither."

The principle is equally applicable to Exemption 7(C), and is an additional reason the documents at issue here should be disclosed. Some of the prosecuted individuals may be able to vindicate their Fourth Amendment rights through motions to suppress evidence, petitions for post-conviction relief, or *Bivens* suits for money damages. As in *Lepelletier*, it is "overly paternalistic" for the government to insist on protecting the privacy rights of individuals it has chosen to publicly prosecute for crimes where there is "good reason to believe" that they would rather have both the publicity and the information that their constitutional rights were violated than neither. *Id.*

Defendant's arguments to the contrary are unavailing. Defendant first cites four cases to support the proposition that "courts have recognized the considerable stigma and potential for harassment and embarrassment inherent in being associated with law enforcement proceedings and criminal activity." Dkt. No. 26-2 (Def.'s Br.) at 17. All four cases are inapposite because they involve the privacy interests of individuals who were uncharged subjects of investigations or who were merely mentioned in records. *Fitzgibbon v. Cent. Intelligence Agency*, 911 F.2d 755, 767 (D.C. Cir. 1990); *Lesar v. U.S. Dep't of Justice*, 636 F.2d 472, (D.C. Cir. 1980); *Morley*

v. Cent. Intelligence Agency, 453 F. Supp. 2d 137, 153 (D. D.C. 2006); *Palacio v. U.S. Dep't of Justice*, Civil Action No. 00-1564, U.S. Dist. LEXIS 2198 at *20 (D.D.C. Feb. 11, 2002). For such individuals, who were never charged with any crime, association with criminal activity might be unwarranted. But where, as here, the government has taken initiated a public criminal prosecution, the government itself has concluded that the association is no longer unwarranted.

Defendant next maintains that "it is settled law that parties mentioned in law enforcement materials have a presumptive privacy interest in having their names and other personal information withheld from public disclosure." Dkt. No. 26-2 (Def.'s Br.) at 18. While plaintiffs have no quarrel with this general proposition, the individuals whose names would be released here were not just "mentioned in law enforcement materials," they were *indicted*. Again, none of the cases defendant cites involved criminal defendants. *See SafeCard Services, Inc. v. SEC*, 926 F.2d 1197, 1205 (D.C. Cir. 1991); *Bast v. DOJ*, 665 F.2d 1251, 1254 (D.C. Cir. 1981); *Nation Magazine Washington Bureau v. U.S. Customs Serv.*, 71 F.3d 885, 894 (D.C. Cir. 1995).

Finally, defendant argues that "a substantial privacy interest can exist for the purpose of Exemption 7(C) even in law enforcement records that have been made public at some place and point in time." Dkt. No. 26-2 (Def.'s Br.) at 19. While an individual *can* sometimes have a privacy interest in publicly revealed information, that does not mean that individuals necessarily *do* have a privacy interest in such information. The defendant has not explained why there is any such interest here. Defendant cites two cases on this point. In the first, the Court found that an individual has a substantial interest in the privacy of his rap sheet (a list of his arrests, charges, convictions and incarcerations), because while the individual items of information on the rap sheet were publicly available, "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local policy stations

throughout the country and a computerized summary located in a single clearinghouse of information." *Reporters Comm.*, 489 U.S. at 764. Plaintiffs here do not seek any government compilation of information about any individual. They seek only the names (e.g., "United States v. David Addington") and docket numbers (e.g., "09-cr-9999 (D.D.C.)") of criminal prosecutions subsequent to warrantless cell phone tracking. This is not the sort of compilation of hard-to-find information about an individual that concerned the Court in *Reporters Committee*.

Defendant's second case involved a pro se federal inmate's request for information about a federal magistrate judge who had previously served as an Assistant United States Attorney, including a list of every case prosecuted by the magistrate as an AUSA. *Harrison v. Executive Office For United States Attorneys*, 377 F. Supp. 2d 141 (D. D.C. 2005). The court noted that the plaintiff had identified no public interest in disclosure and on that basis upheld the government's invocation of Exemption 7(C), citing without elaboration a string of FOIA cases none of which involved case names or docket numbers. Judge Lamberth's decision in *Harrison* may have been motivated by the identity of the requester and the creepy nature of his request. In any event, to the extent that it is relevant here, *Harrison* merely demonstrates that a very minimal privacy interest may satisfy the balancing test when the public interest is nonexistent.

2. The Public Has A Strong Interest In Learning About Prosecutions Resulting From Cell Phone Tracking.

The other side of the balancing test is the public interest in disclosure. *Davis v. DOJ*, 968 F.2d, 1276, 1281 (D.C. Cir. 1992). Defendant asserts "there is no relevant public interest." Dkt. No. 26-2 (Def.'s Br.) at 20. Quite the opposite is true.

There is a substantial public interest in understanding to what extent and to what end the government is engaged in cell phone tracking, to what extent these surveillance activities lead to prosecutions, and to what extent these prosecutions are successful. Currently the public has no

idea who is prosecuted as a result of cell phone tracking, or for what kinds of crimes. The case names and docket numbers are necessary in order to be able to see to what uses this surveillance is being put. This is a classic example of an interest in learning what the government is "up to," the central public interest FOIA was intended to satisfy. *Reporters Comm.*, 489 U.S. at 773.

In addition, courts have recognized a heightened public interest in the disclosure of government records that relate to potential government misconduct. *See, e.g., Perlman v. U.S. Dep't of Justice*, 380 F.3d 110, 111-12 (2d Cir. 2004); *SafeCard Services, Inc.*, 926 F.2d at 1206. Such an interest exists where, as here, judges across the country have expressed concern that warrantless tracking of cell phones without probable cause may violate both statutory law and the Fourth Amendment. *See supra* at pp. 6-7.

The public interest in disclosure is also strong because it implicates the public's right of access to court proceedings. *See Richmond Newspapers*, 448 U.S. at 573 ("a presumption of openness inheres in the very nature of a criminal trial under our system of justice"). Because the vast majority of applications and orders remain under seal and published decisions exist in only a handful of districts, plaintiffs need the requested information to access court proceedings.

Defendant relies on three cases to argue that "courts have typically found no public interest in knowing the names of individuals mentioned in law enforcement records." Dkt. 26-2 (Def.'s Br.) at 18. But these cases are inapposite because they all involved names in investigatory files of people who were not subsequently prosecuted. *SafeCard*, 926 F.2d at 1205; *Puerto Rico v. DOJ*, 823 F.2d 574, 575 (D.C. Cir. 1987); *Blanton v. DOJ*, 63 F. Supp. 2d 35, 36 (D. D.C. 1999). In other cases, courts *have* found a public interest in knowing information about specific individuals and have concluded that the public interest trumps the

privacy interest. *See, e.g.*, *Bennett v. Drug Enforcement Admin.*, 55 F. Supp. 2d 36, 43 (D.D.C. 1999); *Hidalgo v. FBI*, 541 F. Supp. 2d 250, 255-56 (D.D.C. 2008).

Here, the public interest in disclosure is at its highest, given that the interest motivating the requests is concern with what an agency is up to, and is amplified by the possibility that the agency is engaged in wrongdoing. The privacy interest is at its lowest, because the individuals concerned have been prosecuted, the material is in the public domain, and widely available.

B. Defendant Improperly Withheld Responsive Records Pursuant to Exemption 6.

Because withholding is improper under Exemption 7(C), it is also improper under Exemption 6. Exemption 7(C), which permits withholding when disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy," is more easily satisfied than Exemption 6, which permits withholding only when disclosure "would constitute a *clearly* unwarranted invasion of personal privacy." 552 U.S.C. § 552(b)(6), (7)(C) (emphasis added). Where information that has been compiled for law enforcement purposes is not exempt pursuant to Exemption 7(C), it will necessarily fail to be exempt under the more demanding standard of Exemption 6. *See U.S. Dep't of Defense v. Federal Labor Relations Authority*, 510 U.S. 487, 496 n.6 (1994) ("Exemption 7(C) is more protective of privacy than Exemption 6").

III. PLAINTIFFS ARE ENTITLED TO CERTAIN OF THE WITHHELD CATEGORY 1 DOCUMENTS.

In Category 1, plaintiffs sought "Policies, procedures, and practices followed to obtain mobile phone location information for law enforcement purposes." Defendant produced a *Vaughn* index listing 72 documents it concedes are responsive to Category 1 of plaintiffs' FOIA request. To narrow the issues before the Court, plaintiffs seek the release of only 27 of them.

A. Plaintiffs Are Entitled To The Case Names And Docket Numbers In the Applications.

Defendant has withheld the case names and docket numbers (with court) in draft and final applications for surveillance. *Vaughn* Index, at Entries 19-24, 29 30, 31, 35, 36, 48, and 65-67. This information is different from the information plaintiffs sought in Category 5, because that Category encompassed the case names and docket number of *prosecutions* (i.e. United States v. David Addington, 09-cr-9999 (D.D.C.)), whereas what plaintiffs seek here are the case names and docket numbers of *applications* (i.e. *In re: Application For Cell Site Authority*, No. 09-8888 (D.D.C.)). Defendant claims that Exemptions 6 and 7(C) cover this information, but because the case names of *applications* do not include the surveillance target's name, and the applications are filed under seal, the case names and docket numbers do not reveal any personally identifying information and therefore do not implicate Exemptions 6 and 7(C) at all. To the extent this Court applies these exemptions, plaintiffs incorporate by reference their arguments above regarding Exemptions 6 and 7(C).

B. Plaintiffs Are Entitled To Portions of Document 67.

Defendant's brief states that Document 67 is a "sealed application and a court order to obtain historical cell cite information in a criminal investigation involving death threats made against a federal employee," and that the underlying law enforcement proceedings are still pending. Dkt. No. 26-2 (Def.'s Br.) at 15-16. Defendant's *Vaughn* states:

> Withheld this document because it is protected by the attorney work product privilege; and, the name and cell phone numbers related to third party of investigative interest to the government to protect against harassment or stigmatizing public attention; the names and business affiliations of three third parties merely mentioned to protect against harassment and unwanted public attention; and the name of an FBI Special Agent to protect against harassment an annoyance in the conduct of official duties and in private life. There is no reasonably segregable information contained in this document. The withheld information is not appropriate for discretionary disclosure

Exh. 4 at Entry 67. Plaintiffs do not challenge the withholding of (1) the name and cell phone numbers related to an investigative interest to the government, (2) the names and business affiliates of three third parties, or (3) the name of an FBI special agent.[16] However, it is highly likely that this application also states the legal standard pursuant to which defendant seeks cell phone tracking authority in the district in which it was filed. Defendant has provided no justification for withholding this portion of the application and proposed order.

Nor could it. None of the three exemptions asserted by defendant (Exemptions 6, 7(C), and 7(A)) justifies withholding legal arguments. As discussed above, Exemptions 6 and 7(C) protect information that impacts personal privacy. Disclosing the portion of the application consisting of legal argument will not reveal any personally identifying information.

Exemption 7(A) permits withholding of law enforcement records where disclosure could reasonably be expected to "interfere with law enforcement proceedings." 5 U.S.C. § 552(b)(7)(A). "[T]o withhold documents pursuant to Exemption 7(A), an agency must show that they were compiled for law enforcement purposes and that their disclosure (1) could reasonably be expected to interfere with (2) enforcement proceedings that are (3) pending or reasonably anticipated." *Mapother v. U.S. Dep't of Justice*, 3 F.3d 1533, 1540 (D.C. Cir. 1993) (emphasis omitted). Defendant has not explained how releasing the portion of the application and order setting out the legal standard could imperil an ongoing investigation. The portion plaintiffs seek should be released.

C. Plaintiffs Are Entitled To The Withheld Portions Of The Template Applications

Finally, plaintiffs also seek portions of template applications and orders that defendant

[16] Although defendant initially asserted in its *Vaughn* that Exemption 5 is applicable to this document, defendant has subsequently withdrawn that claim. Exh. 5 (Letter from V. Desai to C. Crump, dated July 20, 2009) at 1.

has withheld pursuant to Exemption 2, 7(E), or both.[17] As plaintiffs understand defendant's use of the term "template," these documents are model applications that Assistant United States Attorneys fill out when they want to track individuals' cell phones.

1. Defendant Improperly Withheld Portions Of Template Orders Pursuant To Exemption 2.

Defendant has withheld portions of documents 2, 69, and 71 pursuant to Exemption 2 on the ground that they relate to internal agency practices and contain information that, if released, could risk circumvention of the law by providing details of how to avoid detection. Dkt. No. 26-2 (Def.'s Br.) at 8.

Exemption 2 provides that the FOIA does not apply to matters that are "related solely to the internal personnel rules and practices of an agency." 5 U.S.C. § 552(b)(2). Despite the use of the word "solely," the D.C. Circuit has interpreted Exemption 2 to cover documents that are "predominantly internal." *Crooker v. Bureau of Alcohol, Tobacco & Firearms*, 670 F.2d 1051, 1074 (D.C. Cir. 1981). The D.C. Circuit has explained that records are not "predominantly internal" if they affect the public or another agency. *Crooker*, 670 F.2d at 1073. "The word 'internal' in Exemption 2 plainly limits the exemption to those rules and practices that affect the internal workings of an agency." *Id*. The templates at issue here have significant external effects on members of the public because they are used to advocate the tracking of individuals' cell phones. They are therefore not "predominantly internal" and Exemption 2 is inapplicable.

Even if the templates were deemed "predominantly internal," defendant would still not be able to withhold the records. To qualify for Exemption 2, the documents must also be either "trivial administrative matters of no genuine public interest," *Schiller v. NLRB*, 964 F.2d 1205,

[17] Defendant asserts Exemption 2 to withhold documents 2, 69, and 71, and asserts Exemption 7(E) to withhold these documents as well as 2, 3, 26, 27, 28, 29, 32, 33, 34, 68, 69, 70 and 71.

1207 (D.C. Cir. 1992), or else their disclosure must "significantly risk[] circumvention of agency regulations or statutes, *Stolt-Nielson Transp. Group Ltd. v. U.S.*, 534 F.3d 728, 732 (D.C. Cir. 2008). Defendant does not contend that the former criterion applies. It contends that the latter (known as "High 2") does. Dkt. 26-2 (Def.'s Br.) at 7.

To qualify for "High 2," it is "the Government's burden to prove the 'significant risk'" of circumvention of the law if the record were provided. *Hidalgo*, 541 F. Supp. 2d at 253 (quoting *Crooker*, 670 F.2d at 1074). This burden "cannot be met by mere conclusory statements; the agency must show how release of the particular material would have the adverse consequence that the Act seeks to guard against." *Washington Post Co. v. U.S. Dep't of Justice*, 863 F.2d 96, 101 (D.C. Cir. 1988).

Defendant has not shown with reasonable specificity that disclosure of these records would risk circumvention of the law. With respect to Document 2, defendant's sole explanation for withholding is that it contains "information regarding how investigating agents use the cell phone information, which if released could risk circumvention of the law by providing details of how to avoid detection, thereby negatively impacting the effectiveness of the technique." Exh. 4 (*Vaughn* Index) at Entry 2. But this boilerplate does little more than restate the language of the exemption. It is unclear whether the withheld information extends beyond what is commonly known, and whether it would in fact enable circumvention. The public has some knowledge about "how investigative agents use cell phone information." *See supra* pp. 6 to 7. Without some more specific justification, plaintiffs have no way to present argument as to whether the particular use at issue is one that, if known, would increase the risk of circumvention.

With respect to Document 69, the *Vaughn* asserts that "information regarding the investigative agency's interest in continuation of service on a target's cell phone account" could

"risk circumvention of the law by providing details of how to avoid detection, thereby negatively impacting the effectiveness of this technique." Exh. 4 at Entry 69. Again, plaintiffs and this Court are left to guess as to whether the exemption applies, which is improper. *Washington Post Co.*, 863 F.2d at 101. If defendant is merely redacting information related to the fact that law enforcement may request a carrier continue service beyond the contract date, the release of this information would not create a significant risk of circumvention because it is too obvious. To the extent the redacted information makes some other point, defendant's *Vaughn* index is inadequately informative.

With respect to Document 71, the *Vaughn* asserts that information regarding "the geographic range for pinpointing a target's cell phone… could risk circumvention of the law by providing details of how to avoid detection." Exh. 4 at Entry 71. That cell phones permit law enforcement to identify the location of the cell phone user is public knowledge. *See supra* pp. 6-7. Defendant therefore must establish that knowledge by investigative targets of some aspect of the precision which is obtainable would facilitate circumvention. Defendant does not explain how that could be true. The millions of people who have used GPS devices know that they locate themselves with considerable precision ("turn left *now*").

Defendant's only other discussion of why application of High 2 is appropriate is contained in the Finnegan Declaration. Dkt. No. 26-7 at ¶¶ 59, 60. Ms. Finnegan writes:

> Specifically, EOUSA has asserted Exemption (b)(2)(high) in conjunction with Exemption (b)(7)(E) to protect the details associated with the geographic and physical limitations of a caller identification feature and of a Global Positioning System ("GPS") feature, the conditions under which a subject's cell phone activity will be captured, the conditions under which cell site information will not be collected, and the ways in which co-conspirators can be identified by using information related to a target's cell phone activity.

Finnegan Decl. at ¶ 59. However, defendant fails to indicate which document (2, 69, or 71) contains which of the five pieces of information that defendant claims will lead to circumvention. This Court should not grant summary judgment until defendant specifies which types of information are featured in each of the documents under dispute, and plaintiffs have an opportunity to respond.

2. Defendant Improperly Withheld Responsive Records Pursuant to Exemption 7(E).

Defendant claims that Exemption 7(E) permits it to withhold portions of the template applications. Exh. 4 (*Vaughn* Index) at Entries 2, 3, 26-29, 32-34, and 68-71 (the portions of these documents released by defendant are attached to the Sahl Decl. as Exhibits 6-18). Exemption 7(E) allows agencies to withhold information "compiled for law enforcement purposes, but only to the extent that production . . . (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E).

The standard for applying Exemption 7(E) is identical to the Exemption 2 standard: whether "disclosure significantly risks circumvention of agency regulations or statutes." *Crooker*, 670 F.2d at 1074. *See also PHE, Inc. v. U.S. Dep't of Justice*, 983 F.2d 248, 250 (D.C. Cir. 1993) ("under both the (b)(2) and the (b)(7)(E) exemptions, the agency must establish that releasing the withheld materials would risk circumvention of the law"); *Hidalgo*, 541 F. Supp. 2d at 253 (same). The exemption does not protect techniques which are already known to the public. *Nat'l Sec. Archive v. Fed. Bureau of Investigation*, 759 F. Supp. 872, 885 (D.D.C. 1991). It properly applies only to information regarding those techniques which are "obscure or secret." *Jaffe v. Cent. Intelligency Agency*, 573 F. Supp. 377, 387 (D.D.C. 1983).

Defendant uses the same boilerplate, conclusory language regarding circumvention here that it used in asserting Exemption (b)(2). *Compare* Finnegan Decl. at ¶ 104 (regarding Exemption 7(E): "The possession of this information by individuals involved in criminal activity would allow them to take evasive actions in order to avoid detection, to destroy or tamper with evidence, and to coordinate false exculpatories.") *with Id.* at ¶ 60 (regarding Exemption 2: "The release of these techniques would equip lawbreakers with information that would allow them to take evasive actions in order to avoid detection, to destroy or tamper with evidence, and to coordinate false exculpatories.").

Furthermore, the Finnegan Declaration lists 13 types of information that are withheld pursuant to Exemption 7(E), Finnegan Decl. at ¶ 102, and explains that it is withholding information from 30 different documents pursuant to Exemption 7(E), *id.*, but never explains which of the 13 types of information are contained in which of the 30 documents. Plaintiffs seek some of the 30 documents but not others. Rather than accept this improper kitchen sink approach to exemption analysis, this Court should either deny defendant's exemption claims or require defendant to indicate, on a document-by-document basis, what information is withheld and why the withheld information poses a risk of circumvention.

Defendant's *Vaughn* does not help matters because, with respect to its withholdings pursuant to Exemption 7(E), defendant does not even allege that there is a substantial risk of circumvention. *See, e.g*, Exh. 4 at Entry 3 ("Withheld portions of pages 1-5 of the Order and pages 2-8 of the Application to protect the details of techniques and procedures for law enforcement investigations and prosecutions that relate to information/cellular phone technology, that are not generally known to the public and the methods of obtaining cell phone use

information."). Defendant's *Vaughn* uses similarly vacuous language for the other twelve records under consideration here.

As with Exemption 2, defendant's burden "cannot be met by mere conclusory statements; the agency must show how release of the particular material would have the adverse consequence that the Act seeks to guard against." *Washington Post Co. v. U.S. Dep't of Justice*, 863 F.2d 96, 101 (D.C. Cir. 1988). Yet conclusory statements are all defendant has provided.

Defendant appears to argue that, under Exemption 7(E), demonstrating a risk of circumvention is unnecessary. Defendant writes, "Exemption 7(E) does not require a particular determination of harm that would result from disclosure of specific records or information; rather, the exemption categorically protects information related to law enforcement techniques." Ex. 26-2 (Def.'s Br.) at 24. Although a few district court decisions have followed this approach, Circuit precedent is to the contrary. *See PHE, Inc.*, 983 F.2d at 250 ("under both the (b)(2) and the (b)(7)(E) exemptions, the agency must establish that releasing the withheld materials would risk circumvention of the law"). *See also Hidalgo*, 541 F. Supp. 2d at 253 ("the standard under Exemptions 2 and 7(E) is substantially the same: whether disclosure significantly risks circumvention of agency regulations or statutes") (internal citation omitted); *Coleman v. Fed. Bureau of Investigation.*, 13 F. Supp. 2d 75, 83 (D.D.C. 1998) (same); *Billington v. U.S. Dep't of Justice*, 69 F. Supp. 2d 128, 140 (D.D.C. 1999) (same), *aff'd in relevant part*, 233 F.3d 581, 583 (D.C. Cir. 2000). Accordingly, withholding under 7(E) is proper only if defendant demonstrates that disclosure "significantly risks" circumvention of the law, *Hidalgo*, 541 F. Supp. 2d at 253, which it has failed to do.

Because neither Exemption 2 nor Exemption 7(E) permits withholding of the template applications, the Court should order their release.

D. Defendant Failed To Conduct An Adequate Search For Certain Category 1 Documents.

Defendant's *Vaughn* index raises serious questions regarding the adequacy of defendant's search for Category 1 records, and precludes summary judgment for defendant. Defendant's search has been demonstrably inadequate with respect to the following records which were neither released nor listed in defendant's *Vaughn* index: a) the final versions of numerous "draft" applications and orders (Documents 19-24, 30, 31, 35, 36, 48, 65, and 66); and b) the Hodor and Kischer declarations, which are referred to in defendant's *Vaughn* Index at Entries 26-28. Exh. 4. at Entries 19-24, 26-28, 30, 31, 35, 36, 48, 65, and 66.

"It is elementary that an agency responding to a FOIA request must conduct[] a search reasonably calculated to uncover all relevant documents." *Truitt v. Department of State*, 897 F.2d 540, 542 (D.C. Cir. 1990) (internal quotation marks omitted). In assessing the reasonableness of an agency's search, a court may look to "positive indications of overlooked materials." *Founding Church of Scientology of D.C., Inc. v. Nat'l Sec. Agency*, 610 F.2d 824, 837 (D.C. Cir. 1979).

The adequacy of defendant's search is in issue in this case because of the following "positive indications of overlooked materials":

1. Final Versions Of Withheld "Draft" Applications And Orders

Defendant withheld in full Documents 19-24, 30, 31, 35, 36, 48, 65, and 66, which defendant describes in its *Vaughn* index as "draft" applications and proposed orders, "(Under Seal)." Defendant represents it does not know whether final versions of these applications were ever submitted to courts. Exh. 5 (Letter from V. Desai to C. Crump, dated July 20, 2009) at 2. Defendant stated that it would have to search individual case files to determine whether finals exist, and that "having to search through individual case files would be unduly burdensome." *Id.*

This Court should reject defendant's argument. In listing the draft versions of these documents on its *Vaughn* index, defendant has conceded that they are responsive to plaintiffs' request. Defendant must either search for these documents or explain to this Court why this search would constitute an undue burden. *Nation Magazine*, 71 F.3d at 892. "If the reasonableness of a search is questioned, the burden is on the agency to provide sufficient explanation why a search .... would be unreasonably burdensome." *People for Am. Way Found. v. U.S. Dep't of Justice*, 451 F.Supp.2d 6, 12 (D.D.C. 2006) (ellipsis in original; internal quotation omitted).

The case law makes clear that, wherever the threshold for imposing an undue burden may lie, the search necessary to retrieve these documents would not approach it. *See, e.g., Pub. Citizen, Inc. v. U.S. Dep't of Educ.*, 292 F.Supp.2d 1, 6-7 (D.D.C.2003) (finding reasonable a search of 25,000 files for data irregularly kept in the agency's database); *Nation Magazine*, 937 F.Supp. at 42 (finding reasonable a search for a single memorandum among unindexed chronological files). Instances in which courts have found that searches would be legitimately unduly burdensome are sharply distinguishable. *See, e.g., People for Am. Way Found*., 451 F.Supp.2d at 13 (finding unduly burdensome a manual search of 44,000 files) *Nation Magazine*, 71 F.3d at 891-92 (finding unduly burdensome a search of 23 years of unindexed files); *Am. Fed'n of Gov't Employees, Local 2782 v. U.S. Dep't of Commerce*, 907 F.2d 203, 208-09 (D.C.Cir.1990) (finding unduly burdensome a request to locate "every chronological office file and correspondent file, internal and external, for every branch office [and] staff office ...."). As a matter of common sense, it would take defendant less time to look through 13 files to retrieve the final versions of documents it has already identified than it will take defendant to brief its refusal to do so.

2. The Hodor and Kischer Declarations

Certain documents released by defendant refer to the "Hodor" and "Kischer" declarations, but neither of those declarations was released or listed on defendant's *Vaughn* index. Exh. 4 at Entries 26-28. These declarations appear to be components of application packages that Assistant United States Attorneys submit to courts when seeking to track cell phones. In response to plaintiffs' inquiry, defendant has located the declarations and is determining "whether they are responsive to Plaintiff's FOIA request and whether any or all of the information they contain is exempt from disclosure." Exh. 5 at 3. This Court may need to intervene if defendant does not timely process these declarations or does not release them in full. Summary judgment is therefore inappropriate.

CONCLUSION

For the foregoing reasons, the Court should grant plaintiffs' motion for summary judgment; defendant's motion should be granted in part and denied in part. The Court should further order that defendant shall:

1. Release the Category 5 information (case names and docket numbers);
2. With regard to Category 1 information:
    a. Release the case names and docket numbers contained in documents 19-24, 29-31, 35, 36, 48, and 65-67;
    b. Release the legal argument portion of document 67;
    c. Release the withheld portions of "template" documents 2, 3, 26, 27, 28, 29, 32, 33, 34, 68, 69, 70 and 71; and
    d. Search for the final versions of draft documents 19-24, 30, 31, 35, 36, 48, 65, and 66. If found, defendant should be ordered to release these records or file a supplemental

Vaughn index and supplemental legal memorandum with respect to any that are withheld. If not found, defendant should be ordered to submit an affidavit setting forth why the search was adequate.

3. With regard to the Hodor and Kischer declarations, this Court should order that defendants to disclose them in full or file a supplemental *Vaughn* index and supplemental legal memorandum with respect to any records or portions that are withheld.

July 24, 2009

Respectfully submitted,

/s/ *Catherine Crump*
Catherine Crump
Benjamin Sahl
American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004
Tel: (212) 549-2500
Fax: (202) 452-1868

/s/ *Arthur B. Spitzer*
Arthur B. Spitzer (D.C. Bar No. 235960)
American Civil Liberties Union
of the National Capital Area
1400 20th Street, N.W., Suite 119
Washington, D.C. 20036
Tel: (202) 457-0800
Fax: (202) 452-1868

David L. Sobel (D.C. Bar No. 360418)
Electronic Frontier Foundation
1875 Connecticut Avenue, N.W., Suite 650
Washington, DC 20009
Tel: (202) 797-9009
Fax: (202) 797-9066

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AMERICAN CIVIL LIBERTIES UNION, *et al.* Plaintiffs, v. UNITED STATES DEPARTMENT OF JUSTICE Defendant.	No. 08-cv-1157 (JR)

PLAINTFFS' STATEMENT OF UNDISPUTED AND DISPUTED MATERIAL FACTS

Pursuant to Local Civil Rules 7(h) and 56.1, plaintiffs submit the following statement of undisputed and disputed material facts.

Response to Defendant's Statement of Material Facts

Paragraphs numbered 1- 7 and 9 accurately state undisputed facts.

Paragraphs 8 and 10 are not statements of fact but legal opinions or conclusions about the issues before the Court, and are disputed.

Plaintiffs' Statement of Undisputed Material Facts

Plaintiffs submit the following additional material facts as to which plaintiffs contend there is no genuine issue or dispute.

1. As of December 2008, 270 million people—87 % of the United States population—carried a wireless electronic communication device. CTIA, *CTIA's Semi-Annual Wireless Industry Survey*, *available at* http://files.ctia.org/pdf/CTIA_Survey_Year-End_2008_Graphics.pdf (last viewed July 9, 2009).

2. Cell phone carriers (i.e. Verizon, T-Mobile, etc.) are technically capable of tracking cell phones. DOJ, *Electronic Surviellance Manual* (2005) at 41, *available at* http://www.usdoj.gov/criminal/foia/docs/elec-sur-manual.pdf (last viewed July 13, 2009).

3. In order to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular phone, the portion of the tower facing the phone, and often the signal strength of the phone. *Id.*

4. If a cell phone has GPS capability—GPS is a device which communicates with a network of satellites, generating information about the location of the phone—the carrier may also be able to collect information about the phone's location via GPS. Exh. 1, Mark Eckenweiler, Associate Director, Office Of Enforcement Operations, *Current Legal Issues In Wireless Phone Location* (undated) (hereinafter Eckenweiler Presentation), at 4.

5. The government distinguishes between two types of tracking data it can obtain through carriers. The government generally refers to the first type as Cell Site data. S*ee, e.g., In Re Application Of The United States Of America For An Order For Disclosure Of Telecommunications Records And Authorizing The Use Of A Pen Register And Trap And Trace*, 405 F.Supp.2d 435 (S.D.N.Y. 2005).

6. When the government seeks Cell Site data, it asks the carrier to tell it which cell phone tower the target phone is nearest, as well as which portion of the tower the phone is facing. *See, e.g., In the Matter of the Application of the United States of*

America for an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp.2d 947 (E.D. Wis. 2006).

7. Sometimes the government requests only the phone's location at the beginning and end of phone calls. S*ee, e.g.*, *In Re Application Of The United States Of America For An Order For Disclosure Of Telecommunications Records And Authorizing The Use Of A Pen Register And Trap And Trace*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005),

8. At other times the government requests the phone's location during the course of phone calls. S*ee, e.g.*, *In The Matter Of An Application Of The United States For An Order (1) Authorizing The Use Of A Pen Register And A Trap And Trace Device And (2) Authorizing Release Of Subscriber Information And/Or Cell Site Information*, 396 F.Supp.2d 294, 295 (E.D.N.Y. 2005).

9. In still other cases, the government requests the phone's location whenever it is turned on. *See, e.g.*, *In The Matter Of The Application Of The United States Of America For An Order Authorizing The Installation And Use Of A Pen Register And A Caller Identification System On Telephone Numbers [Sealed] And [Sealed] And The Production Of Real Time Cell Site Information*, 402 F. Supp.2d 597 (D. Md. 2005).

10. The precision of Cell Site data depends on how closely grouped the towers are in a given area. Exh.1 (Eckenweiler Presentation) at p.4.

11. Cell tower service radius ranges from 200 meters to 30 km. *Id.*

12. Defendant can obtain both historical and real-time Cell Site data. *Id.*

13. The second type of cell phone tracking information defendant can obtain is Latitude/Longitude or "Lat/Long" data. *Id.* at 12.

14. There are two distinct forms of Lat/Long data. *Id.*

15. The first is GPS. FCC rules require GPS to be accurate within 50 meters for 67% of calls and to 150 meters for 95% of calls. *Id.*

16. The second form of Lat/Long Data is "network solution" data, derived from triangulation. *Id.* at 6.

17. This data is acquired by the service provider by measuring the signal characteristics of the phone relative to one or more towers. *Id.*

18. FCC rules require accuracy to 100 m for 67% of calls and to 300 m for 95% of calls. *Id.*

19. Lat/Long Data is generally only available in real time. *Id.* at 10.

20. For Lat/Long data, defendant's Office of Enforcement Operations "recommends invoking Rule 41 [probable cause] to obtain lat-long data" because "[a]nything less presents significant risks of suppression." *Id.* at 15.

21. The USAOs for the District of New Jersey and Southern District of Florida are obtaining court permission to engage in GPS or similarly precise cell phone tracking without a warrant. Exh. 2 at p.1 and Exh. 3 at p.1 (letters dated December 31, 2008 from W. G. Stewart, II, to C. Crump).

22. Magistrate judges in at least twelve districts have rejected the government's position and held that the government needs to show probable cause to engage in Cell Site tracking. Exh. 1 (Eckenweiler Presentation) at 9.

July 24, 2009

Respectfully submitted,

/s/ *Catherine Crump*
Catherine Crump
Benjamin Sahl

American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004
Tel: (212) 549-2500
Fax: (202) 452-1868

/s/ *Arthur B. Spitzer*
Arthur B. Spitzer (D.C. Bar No. 235960)
American Civil Liberties Union
of the National Capital Area
1400 20th Street, N.W., Suite 119
Washington, D.C. 20036
Tel: (202) 457-0800
Fax: (202) 452-1868

David L. Sobel (D.C. Bar No. 360418)
Electronic Frontier Foundation
1875 Connecticut Avenue, N.W., Suite 650
Washington, DC 20009
Tel: (202) 797-9009
Fax: (202) 797-9066