ORAL ARGUMENT NOT YET SCHEDULED

No. 14-5013

IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER
Plaintiff-Appellee,

v.

DEPARTMENT OF HOMELAND SECURITY
Defendant-Appellant.

On Appeal from the
United States District Court
for the District of Columbia

BRIEF FOR PLAINTIFF-APPELLEE

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
GINGER MCCALL
JULIA HORWITZ
DAVID HUSBAND
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Plaintiff-Appellee
Electronic Privacy Information Center

CERTIFICATE AS TO PARTIES, RULINGS AND RELATED CASES

CORPORATE DISCLOSURE STATEMENT

Pursuant to F.R.A.P. 26.1 and D.C. Cir. Rules 27(a)(4) and 28(a)(1)(A), Appellee certifies as follows:

A. Parties and Amici

The Defendant-Appellant is the Department of Homeland Security ("DHS"). DHS is a federal agency subject to the Freedom of Information Act ("FOIA").

Plaintiff-Appellee is the Electronic Privacy Information Center ("EPIC"). EPIC is a 501(c)(3) non-profit corporation. EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.

B. Ruling Under Review

Appellant seeks review of the Memorandum Opinion of Judge James E. Boasberg of the United States District Court for the District of Columbia in case number 1:13-cv-00260. The Opinion, issued on November 12, 2013, granted EPIC's cross-motion for summary judgment in full. The Order and Opinion are reproduced in the Joint Appendix at JA 41 and JA 42 respectively.

C. Related Cases

This case has not previously been before this or any other court. Appellee is not aware of any related cases.

D. Corporate Disclosure Statement

EPIC is a 501(c)(3) non-profit corporation. EPIC has no parent, subsidiary, or affiliate. EPIC has never issued shares or debt securities to the public.

/s/ Marc Rotenberg

TABLE OF CONTENTS

Page

CERTIFICATE AS TO PARTIES, RULINGS AND RELATED CASES

GLOSSARY

STATEMENT OF ISSUE FOR REVIEW 1

PERTINENT STATUTES AND REGULATIONS 2

STATEMENT OF THE CASE.....2

I. Factual Background.....3

II. Procedural History 5

A. The EPIC FOIA Request 5

B. EPIC v. DHS, No. 13-cv-00260.....6

C. The District Court Decision and Docketing of the Appeal.....8

SUMMARY OF THE ARGUMENT 10

ARGUMENT.....11

I. THE DISTRICT COURT PROPERLY RULED THAT SOP 303 CANNOT BE WITHHELD UNDER EXEMPTION 7(F) 11

A. In Exemption 7(F) "Any Individual" Refers to an Ascertainable Person or Group; Any Other Reading of the Phrase Produces an Insufficient Nexus to the Harm Asserted 11

B. The District Court's Decision is Consistent with This Court's Recent Ruling in PEER 14

A. The Legislative History and Structure of FOIA Supports the District Court's Construction of "Any Person" 18

II. THE DISTRICT COURT PROPERLY RULED THAT SOP 303 CANNOT BE WITHHELD UNDER EXEMPTION 7(E) 20

A. SOP 303 Is Used for "Coordination," Not "Investigations" or "Prosecutions" 21

B. DHS's Proposed Interpretation of 7(E) is Contrary to Established Principles of Statutory Construction.....24

C. The District Court's Interpretation of Exemption 7(E) Is Consistent With PEER 26

III. DHS FAILED TO DISCLOSE REASONABLY SEGREGABLE, NON-EXEMPT MATERIAL IN SOP 303 27

CONCLUSION.....32

CERTIFICATE OF COMPLIANCE.....33

CERTIFICATE OF SERVICE 34

TABLE OF AUTHORITIES*

Cases

* *ACLU v. Dep't of Def.*, 543 F.3d 59 (2d Cir. 2008), *vacated on other grounds*, 558 U.S. 1042 (2009) 12, 16, 19
Blackwell v. FBI, 646 F.3d 37 (D.C. Cir. 2011) 22, 30
Boehm v. FBI, 948 F. Supp. 2d 9 (D.D.C. 2013) 11
Brestle v. Lappin, 950 F. Supp. 2d 174 (D.D.C. 2013) 13
Conn. Nat'l Bank v. Germain, 503 U.S. 249 (1992) 24
Ctr. for Auto Safety v. EPA, 731 F.2d 16 (D.C. Cir. 1984) 27
Ctr. for Nat'l Sec. Studies v. DOJ, 331 F.3d 918 (D.C. Cir. 2003) 25
DOJ v. Tax Analysts, 492 U.S. 136 (1989) 11
Donnelly v. FAA, 411 F.3d 267 (D.C. Cir. 2005) 25
Edmonds v. FBI, 272 F. Supp. 2d 35 (D.D.C. 2003) 23
EPA v. Mink, 410 U.S. 73 (1973) 26
Hidalgo v. FBI, 541 F. Supp. 2d 250 (D.D.C. 2008) 30
James v. CBP, 549 F. Supp. 2d 1 (D.D.C. 2008) 30
Johnson v. Exec. Office for U.S. Attorneys, 310 F.3d 771 (D.C. Cir. 2002) 27
Juarez v. DOJ, 518 F.3d 54 (D.C. Cir. 2008) 25
Judicial Watch, Inc. v. DHS, No. 11-00604, 2012 WL 251914 (D.D.C. Jan. 27, 2012) 29
Judicial Watch, Inc. v. U.S. Secret Serv., 579 F. Supp. 2d 182 (D.D.C. 2008) 24
Lewis-Bey v. DOJ, 595 F. Supp. 2d 120 (D.D.C. 2009) 23
* *Living Rivers v. U.S. Bureau of Reclamation*. 272 F. Supp. 2d 1313 (D. Utah 2003) 15, 17, 23
Long v. DOJ, 450 F. Supp. 2d 42 (D.D.C. 2006), *order amended on reconsideration*, 457 F. Supp. 2d 30 (D.D.C. 2006), *order amended*, 479 F. Supp. 2d 23 (D.D.C. 2007) 11, 12, 24
Mead Data Cent., Inc. v. Dep't of Air Force, 566 F.2d 242 (D.C. Cir. 1977) 28, 29
Milner v. Dep't of Navy, 131 S. Ct. 1259 (2011) 11
Oglesby v. United States Dep't of the Army, 79 F.3d 1172 (D.C. Cir. 1996) 27, 28
Pratt v. Webster, 673 F.2d 408 (D.C. Cir. 1982) 22
* *Pub. Emps. for Envtl. Responsibility v. U.S. Section, Int'l Boundary & Water Comm'n, U.S.-Mexico,* 740 F.3d 195 (D.C. Cir. 2014) 14, 15, 16, 17, 26
Qi-Zhuo v. Meissner, 70 F.3d 136 (D.C. Cir. 1995) 17
Quinto v. DOJ, 711 F. Supp. 2d 1 (D.D.C. 2010) 13

* Authorities upon which we chiefly rely are marked with asterisks.

Riley v. California, 573 U.S. ___ (2014) 10
Symons v. Chrysler Corp. Loan Guarantee Bd., 670 F.2d 238 (D.C. Cir. 1981) 24, 25
Tax Analysts v. IRS, 294 F.3d 71 (D.C. Cir. 2002) 21, 22
Trans-Pac. Policing Agreement v. U.S. Customs Serv., 177 F.3d 1022 (D.C. Cir. 1999) 28

Statutes

The Freedom of Information Act, 5 U.S.C. § 552 (2012) 6
552(b) 31
552(b)(7) 24
552(b)(7)(A) 29
* 552(b)(7)(E) 24
* 552(b)(7)(F) 12

Legislative Materials

130 Cong. Rec. 3502 (1984) 21
131 Cong. Rec. 248 (1985) 21
132 Cong. Rec. 29,616 (1986) 21
Freedom of Information Act: Hearings Before the Subcommittee on the Constitution, United States Senate, 97th Cong., 1st Sess. 178, 189 (1981) 20

Other Authorities

Black's Law Dictionary (5th ed. 1979) 22
President's Nat'l Sec. Advisory Comm., *Termination of Cellular Networks During Emergency Situations*, 139 (2006) 21
Webster's Ninth New Collegiate Dictionary (1985) 30

GLOSSARY

BART	Bay Area Rapid Transit
DHS	Department of Homeland Security
EPIC	Electronic Privacy Information Center
FOIA	Freedom of Information Act
JA	Joint Appendix
NCC	National Coordinating Center
NCS	National Communications System
NSTAC	National Security Telecommunications Advisory Committee
SOP 303	Standard Operating Procedure 303

ORAL ARGUMENT NOT YET SCHEDULED

No. 14-5013

IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER
Plaintiff-Appellee,

v.

DEPARTMENT OF HOMELAND SECURITY
Defendant-Appellant.

On Appeal from the
United States District Court
for the District of Columbia

BRIEF FOR PLAINTIFF-APPELLEE

STATEMENT OF ISSUE FOR REVIEW

Whether the Department of Homeland Security's policy for coordinating the "disruption" of wireless communications networks during a peaceful protest is exempt from disclosure under Exemptions 7(E) or 7(F) of the Freedom of Information Act, 5 U.S.C. § 552(b) (2012).

PERTINENT STATUTES AND REGULATIONS

All applicable statutes are contained in the addendum to the Brief for Appellant DHS.

STATEMENT OF THE CASE[1]

This case involves a Freedom of Information Act request for the document that describes the circumstances under which the federal government may "disrupt" communications networks. EPIC sought this policy from DHS following the shutdown of a telephone network during a peaceful protest of public transit authorities in California. Government "disruption" of communications networks implicates not only lawful protests and other First Amendment protected activities but also access to 9-1-1 and other critical emergency services. Public release of this policy is necessary to protect constitutional rights, public safety, and public trust in communications services. DHS claims that this document may be withheld as an investigative technique or method and because release would endanger the physical safety of an individual. But Judge Boasberg correctly held that neither FOIA exemption 7(E) nor 7(F) applies to the document at issue in this case. His decision should be affirmed.

[1] EPIC is grateful for the work of EPIC Clerks Natasha Duarte, Cody Duncan, Eric Glatt, Krister Johnson, Aimee Thomson, and Alex Vlisides, who contributed to the preparation of this brief.

I. Factual Background

On July 3, 2011, a Bay Area Rapid Transit ("BART") officer in San Francisco shot and killed a homeless man named Charles Hill. The officer later alleged that Hill had attacked him with a knife and that he acted in self-defense. The death sparked a major protest against BART on July 11, 2011. Though the protests disrupted service at several transit stations, no one was injured. A second protest was planned one month later, but ended after BART officials cut off all cellular service inside four transit stations for a period of three hours. This act by public officials prevented everyone in the transit stations from sending or receiving phone calls, messages, emergency notifications, and other transmissions.

The protocol for public officials to "disrupt" communication services is derived from Standard Operating Procedure 303 ("SOP 303"). According to DHS, "SOP 303 establishes a protocol for verifying that circumstances exist that would justify shutting down wireless networks." Holzer Decl. ¶ 25. (JA 18.) SOP 303 "establishes a procedure by which state homeland security officials can directly engage with wireless carriers, and it establishes factual authentication procedures for decision-makers." *Id.* ¶ 20. (JA 16-17.) SOP 303 was developed by the National Coordinating Center for Communications ("NCC") and approved by the Office of Cybersecurity and Communications ("CS&C"), a subcomponent of

DHS's National Protection and Programs Directorate ("NPPD") in 2005—2006. Holzer Decl. ¶¶ 6, 10, 20. (JA 11, 13, 16.)

According to the President's National Security Telecommunications Advisory Committee ("NSTAC"), SOP 303 responded to the

> need for a single governmental process to coordinate determinations of if and when cellular shutdown activities should be undertaken in light of the serious impact on access by the public to emergency communications services during these situations and the need to preserve the public trust in the integrity of the communications infrastructure.

Holzer Decl. ¶ 20. (JA 16.) The NCC developed SOP 303 consistent with this recommendation "as a unified voluntary process" for the shutdown of wireless networks, that would include coordination with state and local officials. *Id.*

At the time the BART shutdown occurred in 2011, SOP 303 was in effect and would have governed the decision by California state officials to disrupt the cell phone network during the protest. *See* NCC Standard Operating Procedure (SOP) 303 [hereinafter "Redacted SOP 303"] (Pl's Cross Mot. Sum. J., Ex. 2, ECF No. 11-2). The action required communications with the relevant wireless service providers, coordination with the DHS, and compliance with certain factual authentication procedures. *See* Holzer Decl. ¶20. (JA 16.)

II. Procedural History

A. The EPIC FOIA Request

On July 10, 2012, EPIC submitted a FOIA request to DHS for SOP 303 and related documents. *See* EPIC FOIA Req. 1. (JA 24.) SOP 303 codifies a "shutdown and restoration process for use by commercial and private wireless networks during national crisis." *EPIC v. DHS*, ____ F. Supp. 2d ____, No. 13-260, slip op. at 2 (D.D.C. Nov. 12, 2013) (JA 43.) EPIC explained that the government's deactivation of entire communication networks raises substantial First Amendment and public safety concerns, and that such a policy should be subject to public debate. EPIC FOIA Req. 2. (JA 26.) To that end, EPIC requested three specific records from DHS:

1. The full text of Standard Operating Procedure 303;
2. The full text of the pre-determined "series of questions" that determines if a shutdown is necessary;
3. Any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

Id. at 3. (JA 27.)

DHS acknowledged the request on July 24, 2012, conditionally granting a fee waiver and assigning the request Reference Number DHS/OS/PRIV 12-0598. DHS Ack. of EPIC FOIA Req. 1. (JA 31.) DHS then granted itself a 10-day extension due to the "unusual circumstance" that EPIC's FOIA Request is "of substantial interest" to two or more components of DHS or another agency. *Id.*

On August 21, 2012, DHS provided the agency's final response, claiming that it was "unable to locate or identify any responsive records." DHS Final Det. of EPIC FOIA Req. 1. (JA 34.) EPIC appealed the adequacy of DHS's search on September 13, 2012, setting forth in detail the evidence for the existence of SOP 303 and for its location within one or more DHS subcomponents. EPIC Appeal 1. (JA 20.) DHS acknowledged EPIC's appeal on October 25, 2012, but failed to make a determination within twenty days, as required by the FOIA.

B. EPIC v. DHS, No. 13-cv-00260

On February 27, 2013, EPIC filed suit under the FOIA, 5 U.S.C. § 552. EPIC Compl. 1. (JA 1.) After filing the complaint, EPIC received a letter from the United States Coast Guard Office of the Chief Administrative Law Judge. Def. Mot. Sum. J., ECF No. 10-5. (JA 36.) The judge found that the agency failed "to demonstrate that the Privacy Office conducted an adequate search for responsive records" and remanded the request for further review. *Id.*

On June 28, 2013, DHS provided to EPIC an almost entirely redacted copy of SOP 303 and then filed a motion for summary judgment. With the exception of a few headings, and an appendix of agency contacts, the document was entirely redacted. The agency cited FOIA exemptions 6, 7(C), 7(E), and 7(F).[2] *See* Redacted SOP 303, ECF No. 11-2. EPIC opposed the government's motion for

[2] EPIC did not challenge the assertion of Exemptions 6 and 7(C).

summary judgment and cross-moved for summary judgment. DHS filed an opposition and reply on August 9, 2013, and EPIC filed a reply on August 23, 2013.

The version of SOP 303 that DHS released to EPIC appears to consist of seven pages of main text and 23 pages of appendices. *See* Redacted SOP 303, ECF No. 11-2. Nearly all of the main text was withheld under both Exemptions 7(E) and 7(F). *See id*. at 1-7. The first sentence of the document is unredacted and states: "Purpose. This SOP provides detailed Procedures for the National Coordinating Center for Telecommunications (NCC) to coordinate requests for the disruption of cellular service." *Id.* at 1. The text of the document as released contains only a few other unredacted portions, such as the headings for "Restoration" and "Notification" sub-sections and a few short sentences about fax confirmations and annual reviews of the procedure. *Id.* at 3, 5, 7.

After the main text of SOP 303 is a heavily redacted Appendix. *Id.* at 7-30. Appendix A, titled "Points of Contact," lists an emergency response agency in each state with contact information for each. *Id.* at 8-18. Each state agency listing includes information redacted under both Exemptions 6 and 7(C). EPIC did not challenge these exemptions concerning personal privacy. The agency withheld all other appendices under Exemptions 7(E) and 7(F), except for the title of Appendix

E, which stated "External Agency Cellular Disruption Implementation Instructions." *Id.* at 19-30.

C. The District Court Decision and Docketing of the Appeal

The District Court issued a Memorandum Opinion and Order on November 12, 2013. *EPIC v. DHS*, slip op. at 16 (D.D.C. Nov. 12, 2013). (JA 57.) In the Opinion, Judge Boasberg granted EPIC's Motion for Summary Judgment, ordering DHS to turn over SOP 303 without redactions for material previously withheld under Exemptions 7(E) or 7(F). *Id*.

In rejecting DHS's assertion of Exemption 7(E), Judge Boasberg found that "techniques and procedures for law enforcement investigations or prosecutions" apply only to acts by law enforcement officials and only "after or during the commission of a crime." *Id*. at 8. (JA 49.) Although the court found that SOP 303 met the threshold requirement of being "compiled for law-enforcement purposes," the court found that the procedure did not include "techniques and procedures for law enforcement investigations or prosecutions." *Id*. at 6, 8. (JA 47, 49.) The court underscored the distinction between "law enforcement purposes" and "law enforcement investigations," noting that Congress deliberately chose to make the latter category narrower than the former. *Id*. at 7-8. (JA 48-49.) In so holding, the court emphasized the need to follow FOIA's basic principle of promoting disclosure over secrecy. *Id.* at 8. (JA 49.) Finally, Judge Boasberg dismissed

DHS's *post hoc* attempt to characterize SOP 303 as an investigative method, finding that "'no ordinary speaker of the English language' would describe SOP 303 . . . as an evidence-gathering technique." *Id*. at 9 (internal citation omitted). (JA 50.)

Judge Boasberg also held that SOP 303 is not exempt under 7(F) because release of the document cannot "reasonably be expected to endanger the life or physical safety of any individual." *Id*. at 10. (JA 51.) The court found that DHS failed to "identify the individuals at risk with some degree of specificity" as required by the FOIA. *Id*. at 10. (JA 51.) The court held that DHS's claim was "too broad[]," and that Exemption 7(F) requires "some specificity and some ability to identify the individuals endangered." *Id*. at 10, 12. (JA 51, 53.) As a result, Exemption 7(F) does not cover "anyone anywhere in the United States within the blast radius of a hypothetical unexploded bomb." *Id*. at 14. (JA 55.)

The court stayed its order to allow DHS to appeal or implement another type of cure. *Id*. at 16. (JA 57.) On January 13, 2014, DHS timely filed notice of appeal. The appeal was docketed on January 15, 2014, and DHS filed its brief on June 4, 2014.

SUMMARY OF THE ARGUMENT

The government procedure at issue in this case is used to "disrupt" cellular networks operated by private carriers. These communications networks are the backbone of our society. Hundreds of millions of Americans rely upon cell phone service every day to conduct business, communicate with family, organize politically, and obtain emergency services. 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*, 573 U.S. ___, slip op. at 9 (2014). The decision to shut down one of these networks, even temporarily, would have a significant impact on the surrounding population, and could itself threaten public safety. Furthermore, shutdowns have been used to suppress lawful protest activities, both in the United States and abroad. The protocol governing the shutdown decision is therefore a matter of significant public interest and should be released.

Judge Boasberg concluded that SOP 303 is not exempt from disclosure under FOIA. The court ruled that DHS's Exemption 7(F) claim fails because the government must show a threat of harm to a *specific and discrete* group of identifiable individuals. The court also held that DHS's Exemption 7(E) claim fails because SOP 303 does not facilitate law enforcement investigations or prosecutions. Judge Boasberg emphasized the Supreme Court's recent

determination that FOIA "exemptions be 'given a narrow compass'" because of "the Act's goal of broad disclosure." *Milner v. Dep't of Navy*, 131 S. Ct. 1259, 1265 (2011) (citing *DOJ v. Tax Analysts*, 492 U.S. 136, 151 (1989)).

ARGUMENT

I. THE DISTRICT COURT PROPERLY RULED THAT SOP 303 CANNOT BE WITHHELD UNDER EXEMPTION 7(F)

A. In Exemption 7(F) "Any Individual" Refers to an Ascertainable Person or Group; Any Other Reading of the Phrase Produces an Insufficient Nexus to the Harm Asserted

Under Exemption 7(F), information can be withheld under the FOIA where disclosure could "endanger the life or safety of any individual." 5 U.S.C. § 552(b)(7)(F). When evaluating a 7(F) claim, courts look for some "nexus between disclosure and possible harm and whether deletions were narrowly made to avert the possibility of such harm." *Boehm v. FBI*, 948 F. Supp. 2d 9, 22 (D.D.C. 2013). While Exemption 7(F) "may be invoked to protect 'any individual' reasonably at risk of harm," the agency must focus its redactions narrowly. *Long v. DOJ*, 450 F. Supp. 2d 42, 79 (D.D.C. 2006), *order amended on reconsideration*, 457 F. Supp. 2d 30 (D.D.C. 2006), *order amended*, 479 F. Supp. 2d 23 (D.D.C. 2007).

Courts have maintained a narrow construction of Exemption 7(F) by applying it only in cases where the at-risk individuals can be identified with specificity. As the Second Circuit recently stated, "the phrase 'any individual' in Exemption 7(F) may be flexible, but it is not vacuous." *ACLU v. Dep't of Def.*, 543

F.3d 59, 67 (2d Cir. 2008), *vacated on other grounds*, 558 U.S. 1042 (2009). The court held that:

> the statute does not read 'any *named* individual,' and we thus understand it to include individuals identified in some way other than by name – such as, for example, being identified as family members or coworkers of a named individual, or some similarly small and specific group. This does not, however, mean that the individual contemplated by exemption 7(F) need not be identified at all, or may be identified as a member of a vast population.

Id. at 67-68. The court reasoned that, "by requiring a showing of danger to an individual, Congress provided a constraint limiting Exemption 7(F) to its intended scope—the protection of individuals subject to a *non-speculative* risk of harm incident to a law enforcement investigation." *Id*. at 80.

Thus, where an agency "fail[s] to demonstrate with sufficient specificity that releasing [extensive] information reasonably could be expected to endanger the life or physical safety of any individual," the agency is not permitted to assert Exemption 7(F). *Long*, 450 F. Supp. 2d at 79-80. Records are improperly withheld where an agency "offers little more than conclusory assertions that disclosure will increase the chances that third parties will be harmed in some way. Such unsupported speculation cannot serve as a justification for withholding information under Exemption 7(F)." *Id*. at 80.

Exemption 7(F) "affords broad protection to the identities of individuals mentioned in law enforcement files . . . including any individual reasonably at risk

of harm." *Brestle v. Lappin*, 950 F. Supp. 2d 174, 184 (D.D.C. 2013) (*citing Quinto v. DOJ*, 711 F. Supp. 2d 1, 8 (D.D.C. 2010)). Thus, courts have found that 7(F) was properly asserted where the withheld information would have revealed the identity of police informants, who might then be at risk of retaliation by either the plaintiff or some member of the public. *Brestle*, 950 F. Supp. 2d at 185; *Quinto*, 711 F. Supp. 2d at 8; *Boehm*, 948 F. Supp. 2d at 22. The key in these cases was the "nexus between disclosure and possible harm," meriting "narrow deletions to avert the possibility of such harm." *Boehm*, 948 F. Supp. 2d at 22.

DHS cannot establish a "nexus between disclosure and possible harm" here because both the risks and the "persons" referred to in the agency affidavit are purely speculative. The "individuals" that DHS puts forward are "people near unexploded bombs, people who frequent high value targets, and bomb squads and other first responders." Br. of Appellant at 19, *EPIC v. DHS*, No. 14-5031 (D.C. Cir. June 4, 2014). This recitation is not sufficient to satisfy the 7(F) standard. There are no identified individuals "mentioned in law enforcement files" whom the agency seeks to protect by invoking Exemption 7(F). DHS cannot establish the required link since the agency has no identifiable group of individuals whom it seeks to protect.

Exemption 7(F) was intended to protect individuals from risk of harm when their actual participation in law enforcement activities was exposed; it should not

extend to any harm that might occur in any place as a possible result of the disclosure of an agency document. Such an interpretation of Exemption 7(F) would create a boundless rationale to withhold agency records that should otherwise be disclosed to the public.

B. The District Court's Decision is Consistent with This Court's Recent Ruling in PEER

This Court recently examined the application of 7(F) in *PEER*, considering whether records relating to two dams along the U.S.-Mexican border, the Amistad and Falcon Dams, should be released under the FOIA. *Pub. Emps. for Envtl. Responsibility v. U.S. Section, Int'l Boundary & Water Comm'n, U.S.-Mexico,* 740 F.3d 195, 199 (D.C. Cir. 2014) [hereinafter *"PEER"*]. The plaintiffs sought disclosure of an expert report concerning structural deficiencies in the dams' foundations, a set of emergency action plans for dam-related evacuations, and inundation maps showing the "downstream areas and populations that would be affected if the dams were to break." *Id*.

This Court determined that the inundation maps were exempt under 7(F) because they would "give anyone seeking to cause harm the ability to deduce the zones and populations most affected by dam failure." *Id*. at 206. The Court also found that "[t]errorists or criminals could use that information to determine whether attacking a dam would be worthwhile, which dam would provide the most attractive target, and what the likely effect of a dam break would be." *Id*. This

threat was further confirmed by the prior issuance of an "intelligence alert from the Department of Homeland Security," which described a "plot by drug traffickers to blow up the Falcon Dam." *Id*.

In an earlier case, *Living Rivers v. U.S. Bureau of Reclamation*, 272 F. Supp. 2d 1313, 1321-22 (D. Utah 2003), a court similarly held that release of inundation maps posed a threat justifying exemption under 7(F). The maps identified the effects an attack on the Hoover Dam and Glen Canyon Dam would have on the downstream areas. *Id.* at 1314. As in *PEER*, the specifics of the threat posed by disclosure of the *Living Rivers* inundation maps were clear: the "individuals" at risk were the downstream inhabitants of the dam regions, and the location of the attacks were the dams themselves.

PEER and other "inundation maps" cases involve risks to specific and discrete groups of people — the inhabitants downstream of specific dams. The crucial inquiry when assessing Exemption 7(F) is not whether the government seeks to protect a *narrow* group of individuals but instead whether the government seeks to protect a group of *specific and discrete* individuals. Thus, in *PEER* this Court found that the defendant met this burden because "a threat to the population living downstream of a dam would be sufficiently specific to satisfy the exemption." *PEER*, 740 F.3d at 206.

The specificity with which the government defined the at-risk individuals in *Living Rivers* and *PEER* led this Court to find that disclosure of inundation maps would be properly exempted under the Second Circuit's analysis in *ACLU v. DOD*. *PEER*, 740 F.3d at 206 (citing *ACLU v. DOD*, 543 F.3d at 71). In *ACLU*, the court held that proper application of Exemption 7(F) requires the government to "identify at least one individual with reasonable specificity and establish that disclosure of the documents could reasonably be expected to endanger that individual." *ACLU*, 543 F.3d at 71. In *PEER*, this Court found that "the U.S. Section points to the same kind of potential harm to a similarly circumscribed population, meaning that the U.S. Section would prevail even under the Second Circuit's approach. In short, the U.S. Section has connected the release of the inundation maps to a reasonable threat of harm to the population downstream of the dams." *PEER*, 740 F.3d at 206.

In *ACLU*, the Second Circuit found that if the phrase "any individual" was given the expansive interpretation proffered by the government — any individual anywhere — it would have the effect of reading the word "individual" out of the statute. *Id.* at 70. "[I]n effect, it would convert the phrase 'endanger the life or physical safety of any individual' into 'endanger life or physical safety.'" *Id*. This reasoning applies here. To grant DHS's expansive reading, wherein any unidentified persons could be subject to hypothetical harms, would be to read the

word "individual" out of the text. This would violate the statutory canon against surplusage, which is "an endlessly reiterated principle of statutory construction [that] all words in a statute are to be assigned meaning." *Qi-Zhuo v. Meissner*, 70 F.3d 136, 139 (D.C. Cir. 1995).

This Court held in *PEER* that individuals "living downstream of a dam" constitute a "circumscribed population," thus allowing the government to identify, with "reasonable specificity," a "particularized threat to a discrete population." *PEER*, 740 F.3d at 206 (citing *ACLU*, 543 F.3d at 71). In *ACLU*, the population was less specific (the civilian populations of Iraq and Afghanistan and the two American expeditionary forces deployed in combat inside their borders) and the harm was equally diffuse (the threat that publication of photographs would lead to "enlistments and violent acts.") *Id.* at 65. As a result, the Second Circuit held that "it is plainly insufficient to claim that releasing documents could reasonably be expected to endanger some unspecified member of a group so vast as to encompass all United States troops, coalition forces, and civilians in Iraq and Afghanistan." *Id.* at 71.

Judge Boasberg stressed this central conclusion, emphasizing that "the Government here nonetheless seeks a broader interpretation of 'any individual' than was rejected in *ACLU*," because "if the Government's interpretation were to hold, there is no limiting principle to prevent 'any individual' from expanding

beyond the roughly 300 million inhabitants of the United States, as the Government proposes here, to the seven billion inhabitants of the earth in other cases." *EPIC v. DHS*, slip op. at 13. (JA 54.) Therefore, the court held that "[r]eading 7(F) to encompass possible harm to anyone anywhere in the United States within the blast radius of a hypothetical unexploded bomb also flies in the face of repeated Supreme Court direction to read FOIA exemptions narrowly." *Id.* at 14. (JA 55.)

A. The Legislative History and Structure of FOIA Supports the District Court's Construction of "Any Person"

This common-sense reading of the FOIA is supported by the fact that there is no evidence that Congress intended the 1986 FOIA amendments to allow the term "any individual" to include speculative threats to unidentifiable persons. Congress' modifications to Exemption 7(F), were slight and in response to a discrete need. Prior to the 1986 amendments, Exemption 7(F) provided protection only for law enforcement personnel, not their family members or police informants. Thus, Congress revised the exemption to bring these discrete and specific categories of individuals within the scope of 7(F). *Freedom of Information Act: Hearings Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 97th Cong., 1st Sess. 178 (1981); *see also*, 130 Cong. Rec. 3502 (1984) (statement of Sen. Hatch) ("The bill would . . . extend[] exemption 7(F) to include such persons as witnesses, potential witnesses, and family members whose

personal safety is of central importance to the law enforcement process"). This history, reveals that Congress intended only to relax "the category of covered persons, extending its protection to individuals who were not themselves law enforcement personnel, but who faced similarly specific threats of violence." *ACLU*, 543 F.3d at 80.

Judge Boasberg's determination that the 1986 amendments to 7(F) were intended to be "slight" is consistent with the legislative history. The Deputy Attorney General at the time of the amendments emphasized that "the provisions of Exemption 7 would be modified slightly—not revised wholesale as some observers have asserted." 131 Cong. Rec. 248 (1985) (statement of Carol E. Dinkins, Deputy Att'y Gen. of the United States); *see also* 132 Cong. Rec. 29,616 (1986) (statement of Rep. Glenn English) (expressing his approval that the proposed amendments "represent an overall improvement" by making "only modest changes to the FOIA" and a "slight expansion" to 7(F)); *accord ACLU*, 543 F.3d at 79 (finding the legislative history showed that the government did not intend to dramatically expand the scope of Exemption 7(F)). It is clear that Congress did not repeal the requirement of specificity with the amendment to 7(F) in 1986.

Furthermore, DHS has alternative means of protecting SOP 303 without unnecessarily straining the meaning of Exemption 7. The court below stated:

> In reaching its conclusion, the Court is not unaware of the potential adverse use to which this information could be put. Its ruling, furthermore, is no judgment on whether it is in the national interest for SOP 303 to be disclosed. If in fact, the Government believes release will cause significant harm, it has other options to pursue. As the Supreme Court explained in *Milner*, 'If these or other exemptions do not cover records whose release would threaten the Nation's vital interests, the Government may of course seek relief from Congress.'

EPIC v. DHS, slip op. at 15 (internal citations omitted). (JA 56.)

The district court issued a 30-day stay to allow the government to appeal or seek "another type of cure — e.g., classification of the document to exempt it from disclosure under Exemption 1 or legislation exempting it from FOIA under Exemption 3." *Id.* at 16. (JA 57.) But the Government has never asserted that the document is properly classified and has not sought special Congressional protection. If the disclosure of SOP 303 would pose a danger nationwide, the agency could have relied upon one of these other FOIA provisions. Instead, DHS chose to assert an interpretation of Exemption 7(F) that is supported by neither caselaw, nor the text of the provision, nor legislative history.

II. THE DISTRICT COURT PROPERLY RULED THAT SOP 303 CANNOT BE WITHHELD UNDER EXEMPTION 7(E)

SOP 303 is a procedure for disrupting wireless communications, implemented by the National Coordinating Center for Telecommunications ("NCC"). The NCC does not have any law enforcement investigatory powers or responsibilities. Instead, the NCC is a "joint government/industry operation" that

coordinates "national security and emergency preparedness communications" between affiliated government agencies and private entities. Holzer Decl. ¶ 10. (JA 13.) When an authorized governmental authority requests a wireless network shutdown, "the NCC will operate as an authenticating body, notifying the carriers in the affected area of the decision." President's Nat'l Sec. Advisory Comm., *Termination of Cellular Networks During Emergency Situations*, 139 (2006). (JA 39.) Thus, SOP 303 is a coordinating document used to assist the NCC. SOP 303 is not a law enforcement technique, nor is it implemented by a law enforcement agency.

A. SOP 303 Is Used for "Coordination," Not "Investigations" or "Prosecutions"

An agency seeking to withhold records under Exemption 7(E) must satisfy two primary statutory elements. First, the record must be "compiled for law enforcement purposes." 5 U.S.C. § 552(b)(7). This Court has referred to this element as "the threshold requirement of Exemption 7." *See Tax Analysts v. IRS*, 294 F.3d 71, 77 (D.C. Cir. 2002). Second, disclosure of the record must result in the harm recognized by Exemption 7(E): it must reveal either "techniques and procedures for law enforcement investigations or prosecutions," or "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).

These elements are separate, and the agency must establish each one independently to lawfully assert 7(E). *See Blackwell v. FBI*, 646 F.3d 37, 40-42 (D.C. Cir. 2011) (analyzing first whether FBI files regarding the requester's prosecution were compiled for a law enforcement purpose, then whether their disclosure would reveal techniques or procedures for investigations or prosecutions). The threshold requirement of a law enforcement "purpose" is typically easier to establish than the requirement that disclosure reveal "techniques and procedures for law enforcement investigations or prosecutions." *See Pratt v. Webster*, 673 F.2d 408, 420 (D.C. Cir. 1982) (finding that "Congress intended that 'law enforcement purpose' be broadly construed"); *Tax Analysts*, 294 F.3d at 79 (noting that in 1986, Congress broadened Exemption 7's threshold requirement by "deleting any requirement that the information be 'investigatory'"). Accordingly, the Exemption 7 threshold covers law enforcement records unconnected to investigations or prosecutions. *See Tax Analysts,* 294 F.3d at 79.

However, in order to be exempt under 7(E), a record must also be used specifically *for investigations or prosecutions*. To investigate is "to examine and inquire into with care and accuracy" and involves "the taking of evidence." *Black's Law Dictionary* 740 (5th ed. 1979) (definition contemporaneous with amendments to Exemption 7). Accordingly, Exemption 7(E) has been applied to protect records related to the process of an inquiry, such as methods of gathering or organizing

information. *See, e.g.*, *Lewis-Bey v. DOJ*, 595 F. Supp. 2d 120, 137 (D.D.C. 2009) (details of electronic surveillance techniques); *Edmonds v. FBI*, 272 F. Supp. 2d 35, 56 (D.D.C. 2003) (polygraph information).

In the decision below, Judge Boasberg found that "[i]f 'techniques and procedures for law enforcement investigations or prosecutions' is given its natural meaning, it cannot encompass the protective measures discussed in SOP 303. This term refers only to acts by law enforcement after or during the commission of a crime, not crime-prevention techniques." *EPIC v. DHS*, slip op. at 8. (JA 49.) The court also found that this reading of Exemption 7(E) aligned with the FOIA's purpose to promote disclosure and the "well-settled practice of reading FOIA exemptions narrowly." *Id*.

DHS's proposed interpretation of the term "investigation" in 7(E) would create another boundless exemption. From the perspective of a law enforcement agency, almost anything preserved could be said to "support" or "facilitate" investigations. The fact that a technique might indirectly create conditions conducive to a future investigation does not automatically convert it into a technique *for* investigation. In order to be used "for" investigation, there must be a "direct relation to the [government's] law enforcement mandate." *Living Rivers, Inc. v. U.S. Bureau of Reclamation*, 272 F. Supp. 2d 1313, 1320-1321 (D. Utah 2003).

B. DHS's Proposed Interpretation of 7(E) is Contrary to Established Principles of Statutory Construction

In addition to showing that the withheld records were compiled for law enforcement purposes, the government must also show that release of those records would "disclose techniques and procedures for law enforcement investigations or prosecutions." *See, e.g.*, *Judicial Watch, Inc. v. U.S. Secret Serv.*, 579 F. Supp. 2d 182, 187-88 (D.D.C. 2008) ("The Court agrees with defendant that [Sensitive Security Records] are compiled for law enforcement purposes. However, the Court cannot see how disclosure of the information plaintiff seeks would reveal techniques, procedures, or guidelines used by the Secret Service"); *Long*, 450 F. Supp. 2d at 79 (finding that certain program category fields from databases of criminal investigations were compiled for law enforcement purposes but were not exempt under 7(E) because "the Department has failed to identify any law enforcement technique or procedure that would be disclosed upon release of the information").

None of FOIA's "other important interpretive principles" exempt it from the "cardinal canon" of statutory interpretation: that "courts must presume that a legislature says in a statute what it means and means in a statute what it says there." *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992). Even in the FOIA context, "proper deference must be paid to the plain meaning rule." *Symons v. Chrysler Corp. Loan Guarantee Bd.*, 670 F.2d 238, 241 (D.C. Cir. 1981) (citing

Consumers Union of the U.S., Inc., v. Heimann, 589 F.2d 531, 533 (D.C. Cir. 1978)).

Here, Exemption 7(E) plainly requires that the "technique" in question be used "for investigations"—that is, for the process of inquiring into or tracking down through inquiry. Whenever possible, statutes must be interpreted to avoid redundancy. *See Donnelly v. FAA*, 411 F.3d 267, 271 (D.C. Cir. 2005) ("We must strive to interpret a statute to give meaning to every clause and word, and certainly not to treat an entire subsection as mere surplusage"). Exemption 7(E) requires that techniques and procedures be "for law enforcement investigations or prosecutions," and the Court must give effect to these words because "[o]rdinarily, courts will give effect to the plain meaning of the words used by the legislature." *Symons*, 670 F.2d at 241. DHS's expansive reading of Exemption 7(E) would violate this principle, rendering other FOIA exemptions superfluous in the process.

Exemption 7(A), for example, protects law-enforcement records if disclosure "could reasonably be expected to interfere with enforcement proceedings." 5 U.S.C. § 552(b)(7)(A). Courts have interpreted Exemption 7(A) to permit withholding in order to preserve evidence. *See, e.g.*, *Juarez v. DOJ*, 518 F.3d 54, 58 (D.C. Cir. 2008) (protecting records under Exemption 7(A) where disclosure "would compromise the investigation as it could lead to destruction of evidence"); *Ctr. for Nat'l Sec. Studies v. DOJ*, 331 F.3d 918, 929 (D.C. Cir. 2003)

(reviewing cases that have found "evidence tampering" concerns sufficient to justify Exemption 7(A)). But under DHS's reading, there would be no need for Exemption 7(A) because any record that tends to facilitate a subsequent investigation would be protected under Exemption 7(E).

DHS's theory would also invalidate the holdings of numerous Exemption 7(E) cases, render other exemptions superfluous, and transform FOIA from a "disclosure statute" into a "withholding statute." *EPA v. Mink*, 410 U.S. 73, 79 (1973).

C. The District Court's Interpretation of Exemption 7(E) Is Consistent With PEER

This Court recently considered the application of Exemption 7(E) to law enforcement guidelines in *PEER*. 740 F.3d 195, 204-205 (D.C. Cir. 2014). The Court found that guidelines describing "the surveillance and detection of the cause of an emergency dam failure as well as the process for evaluating the dam failure when the emergency subsides," and the "precautions that law enforcement personnel should implement around the dams during emergency conditions" were properly exempt under 7(E). *Id*. at 205.

Unlike the guidelines in *PEER*, the Standard Operating Procedure at issue in this case is used to coordinate activities between government agencies and private parties, not to facilitate the investigation of a threat or emergency. SOP 303 is not executed in connection with an investigation or prosecution, and it is not an

evidence-gathering technique; it is simply a protocol for shutting down a communications network. There is also no similar risk that the release of SOP 303 will hinder investigations. According to the DHS affidavit, the agency's main concern is that the release of certain portions of SOP 303 would allow individuals to "appropriat[e] verification methods and then impersonat[e] officials designated for involvement in the verification process." Holzer Decl. ¶ 26. (JA 19.) But these concerns are relevant only to minor, segregable portions of the document (like the identifying information in Appendix 1 that EPIC has not challenged).

III. DHS FAILED TO DISCLOSE REASONABLY SEGREGABLE, NON-EXEMPT MATERIAL IN SOP 303

The FOIA requires the government to disclose any "reasonably segregable portion of a record." 5 U.S.C. § 552(b); *see Oglesby v. United States Dep't of the Army*, 79 F.3d 1172, 1176 (D.C. Cir. 1996) ("If a document contains exempt information, the agency must still release 'any reasonably segregable portion' after deletion of the nondisclosable portions"). "The 'segregability' requirement applies to all documents and all exemptions in the FOIA." *Ctr. for Auto Safety v. EPA*, 731 F.2d 16, 21 (D.C. Cir. 1984). Under the FOIA, the government bears the burden of providing "a detailed justification for its non-segregability." *Johnson v. Exec. Office for U.S. Attorneys*, 310 F.3d 771, 776 (D.C. Cir. 2002). This includes "a statement of [the government's] reasons," and a "descri[ption of] what proportion of the information in a document is non-exempt and how that material is dispersed

throughout the document." *Mead Data Cent., Inc. v. Dep't of Air Force*, 566 F.2d 242, 261 (D.C. Cir. 1977). Simply claiming that a segregability review has been conducted is insufficient. *Oglesby*, 79 F.3d at 1180. Finally, district courts have an "affirmative duty to consider the segregability issue *sua sponte*." *Trans-Pac. Policing Agreement v. U.S. Customs Serv.*, 177 F.3d 1022, 1028 (D.C. Cir. 1999).

DHS has failed to conduct an adequate segregability analysis in this case or to justify its redaction of nearly every line of SOP 303. The version of SOP 303 that DHS released to EPIC was 30 pages long, but the only text consisted of a section entitled "Emergency Wireless Protocols" consisting of fewer than 70 words, an appendix listing state emergency management contact information (Appendix A), and the title of Appendix E: "External Agency Cellular Disruption Implementation Instructions." *See* Redacted SOP 303, ECF No. 11-2. Even most of the headings of the document are redacted, which makes it impossible to understand how it is organized. The only unredacted lines in SOP 303 are:

1. Purpose. This SOP provides detailed procedures for the National Coordinating Center for Telecommunications (NCC) to coordinate requests for the disruption of cellular service.

[REDACTED]

5. Fax Confirmation. [REDACTED] This fax transmission will be scanned to a file for electronic distribution upon receipt.

[REDACTED]

b. Restoration

[REDACTED]

ii. Notification

[REDACTED]

6. Review. Review annually and following any instance where these procedures are implemented.

7. Supersession. This is the initial issue of the SOP.

Id. DHS has not explained why the outline and headings, or any other organizational elements of SOP 303, are not reasonably segregable.

To justify these redactions, the DHS declaration states that "[n]o other segments of the document could be released without compromising the interests protected by the exemptions invoked by DHS." Holzer Decl. ¶ 22. (JA 17.) But this statement is a conclusion, not an explanation. "[U]nless the segregability provision of the FOIA is to be nothing more than a precatory precept, agencies must be required to provide *the reasons behind their conclusions* in order that they may be challenged by FOIA plaintiffs and reviewed by the courts." *Mead Data Cent., Inc.*, 566 F.2d at 261 (emphasis added). DHS has provided nothing more than "empty invocation[s] of the segregability standard" that the Court should reject. *Judicial Watch, Inc. v. DHS*, 841 F. Supp. 2d 142, 161 (D.D.C. 2012).

Although EPIC does not bear the burden of finding segregable material, it appears that the predetermined shutdown questions contained within SOP 303 should be segregated and released. This portion of SOP 303 consists of a "pre-determined series of questions that determines if a shutdown is necessary." Holzer Decl. ¶ 21. (JA 17.) These questions are plainly not law enforcement techniques. A

"technique" is "a method of accomplishing a desired aim" and a "procedure" is "a particular way of accomplishing something or of acting." *Webster's Ninth New Collegiate Dictionary*, 1211, 937 (1985) (definition contemporaneous with enactment of amendments to Exemption 7). The shutdown questions, however, are not a means of accomplishing a shutdown; they are the means of determining whether to employ a shutdown. In other words, they describe policy criteria, not techniques or procedures.

Even if a technique or procedure were both compiled for law enforcement purposes and used for investigation or prosecution, the government would still need to demonstrate that harm would result from its disclosure. In the D.C. Circuit, this harm typically occurs where disclosure would allow bad actors to evade, defeat, or otherwise circumvent the techniques, thereby reducing their effectiveness. *See, e.g.*, *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011); *Hidalgo v. FBI*, 541 F. Supp. 2d 250, 254 (D.D.C. 2008) (explaining that Exemption 7(E) only allows "information about law enforcement techniques to be withheld when publication would allow perpetrators to avoid them"); *James v. CBP*, 549 F. Supp. 2d 1, 10 (D.D.C. 2008) (withholding the specific search techniques used on requester because disclosure would "assist in subverting the effectiveness of a particular investigative technique . . . and could enable

smugglers of contraband to employ measures to neutralize those techniques" (internal quotation marks omitted)).

SOP 303 contains multiple sub-parts, including (1) the predetermined series of questions that determine if a shutdown is necessary, (2) authentication methods, and (3) the step-by-step shutdown process itself. *See* Holzer Decl. ¶ 25. (JA 18.) Releasing the predetermined shutdown questions would disclose only one part of SOP 303, but without the "verification methods" or identities of "officials designated for involvement," there would be no way for "bad actors to insert themselves into the process of shutting down or reactivating wireless networks." *Id*. ¶ 26 (JA 19.)

Based on the Government's description, the risks created by disclosing SOP 303 are tied directly to the "verification methods" and identities of "officials" involved in the verification process. *Id.* But DHS did not release the other segregable portions of SOP 303 or explain why those portions would not be reasonably segregable. As a result, DHS has not met its burden of showing that all reasonably segregable portions of the record have been disclosed.

CONCLUSION

For the foregoing reasons, this Court should affirm the decision of the District Court.

Respectfully submitted,

/s/ Marc Rotenberg

MARC ROTENBERG
ALAN BUTLER
GINGER MCCALL
JULIA HORWITZ
DAVID HUSBAND
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Appellant Electronic Privacy Information Center

Dated: July 7, 2014

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Rule 32(a)(6) because it is composed in a 14-point Times New Roman, a proportionally spaced font. I further certify that the brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B)(iii) because it contains 6,907 words, excluding the parts of the brief exempted under Rule 32(a)(7)(B)(iii).

/s/ Marc Rotenberg
MARC ROTENBERG

CERTIFICATE OF SERVICE

I hereby certify that on July 7, 2014, I electronically filed the foregoing brief with the Clerk of the Court of the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system.

/s/ Marc Rotenberg
MARC ROTENBERG