APPENDIX A

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued December 11, 2014

Decided February 10, 2015

No. 14-5013

ELECTRONIC PRIVACY INFORMATION CENTER,
APPELLEE

v.

UNITED STATES DEPARTMENT OF
HOMELAND SECURITY,
APPELLANT

Appeal from the United States District Court
for the District of Columbia
(No. 1:13-cv-00260)

Adam C. Jed, Attorney, U.S. Department of Justice, argued the cause for appellant. With him on the brief were *Stuart F. Delery*, Assistant Attorney General, *Ronald C. Machen*, U.S. Attorney, and Sharon Swingle, Attorney.

Marc Rotenberg argued the cause and filed the brief for appellee.

Before: ROGERS, *Circuit Judge*, and SENTELLE and RANDOLPH, *Senior Circuit Judges*.

Opinion for the Court filed by *Circuit Judge* ROGERS.

ROGERS, *Circuit Judge*: Pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, the Electronic Privacy Information Center ("EPIC") requested release by the Department of Homeland Security of Standard Operating Procedure 303 ("SOP 303"), which the Department describes as a protocol for shutting down wireless networks during critical emergencies. When the Department released only a heavily redacted version, EPIC successfully sued to compel disclosure. See *Elec. Privacy Info. Ctr. v. Dep't of Homeland Sec.*, 999 F. Supp. 2d 24 (D.D.C. 2013) ("EPIC"). The Department appeals, invoking FOIA Exemption 7(F) on the ground that production of SOP 303 could reasonably be expected to endanger many individuals' lives or physical safety. Upon *de novo* review, we hold that the plain text of Exemption 7(F) protects law enforcement records the disclosure of which "could reasonably be expected to endanger the life or physical safety of any individual," 5 U.S.C. § 552(b)(7)(F), during a critical emergency, without requiring the withholding agency to specifically identify the individuals who would be endangered, and that much if not all of SOP 303 is exempt from disclosure. Accordingly, we reverse the grant of summary judgment to EPIC, and we remand the case for the district court to determine whether any reasonably segregable portions of SOP 303 can be disclosed.

I.

SOP 303 is an "Emergency Wireless Protocol" that codifies a "unified voluntary process for the orderly shut-down and restoration of wireless services during critical emergencies such as the threat of radio-activated improvised explosive devices." Decl. James Holzer, I, Senior Dir. FOIA Opns., Privacy Off., Dep't Homeland Sec., ¶ 20, June 28, 2013; *see Nat'l Sec. Telecomm. Advisory Comm., Termination of Cellular Networks During Emergency Situations*, NSTAC Issue Review 2006-07, at 139 (2007) ("NSTAC Issue Review").[1] After the 2005 bombings of the transportation system in London, England, in which cellular telephones were used to detonate explosives remotely, the President's National Security Telecommunications Advisory Committee identified 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; *see also* NSTAC Issue Review, at 139. The National Coordinating Center for Communications ("NCC", formerly known as the NCC for Telecommunications), part of the Department's National Cybersecurity and Communications Integration Center, developed SOP 303, under which the NCC "function[s] as the focal

---

[1] *Available at* http://www.dhs.gov/sites/default/files/publications/2006-2007%20 NSTAC%20Issue%20Review_0.pdf.

point for coordinating any actions leading up to and following the termination of private wireless network connections." NSTAC Issue Review, at 139. State Homeland Security Advisors, or their designees, or representatives of the Department's Homeland Security Operations Center make the decision to suspend cellular service. *Id*. Once one of these entities requests a shutdown, the NCC "operate[s] as an authenticating body, notifying the carriers in the affected area of the decision." *Id*. The NCC also "ask[s] the requestor a series of questions to determine if the shutdown is a necessary action." Id. "After making the determination that the shutdown is no longer required, the NCC * * * initiate[s] a similar process to reestablish service." *Id*.

On July 10, 2012, EPIC submitted a FOIA request to the Department seeking the full text of SOP 303, the series of questions used to determine whether a shutdown is necessary, and any related protocols or guidelines. The Department initially responded that it had conducted a comprehensive search, but was unable to locate or identify any responsive records. Following an administrative appeal, however, the Department conducted another search and located one responsive record: SOP 303. See Nat'l Coordinating Ctr. for Telecomm. Standard Operating Procedure 303 (Sept. 25, 2009) ("SOP 303"). The SOP included the full text of the predetermined series of questions that determines if a shutdown is necessary, and the executing protocols related to the implementation of SOP 303. Holzer Decl. ¶ 21.

Pursuant to FOIA Exemptions 6 and 7(C), which protect certain personal information, *see* 5

U.S.C. §§ 552(b)(6), (b)(7)(C), the Department withheld from EPIC the names, telephone numbers, and email addresses for state homeland security officials contained in SOP 303. Aside from a sentence explaining that SOP 303 "provides detailed procedures for the [NCC] to coordinate requests for the disruption of cellular service," certain subsection headings, and the title of Appendix E ("External Agency Cellular Service Disruption Implementation Instructions"), essentially all of SOP 303 was withheld pursuant to FOIA Exemptions 7(F) and 7(E), which permit non-disclosure of certain law-enforcement information that, respectively, "could reasonably be expected to endanger the life or physical safety of any individual," 5 U.S.C. § 552(b)(7)(F), or "would disclose techniques and procedures for law enforcement investigations or prosecutions," *id*. § 552(b)(7)(E).

On February 27, 2013, EPIC filed suit seeking the release of SOP 303 in its entirety. *See* 5 U.S.C. § 552(a)(4)(B). The parties filed cross motions for summary judgment. In support of summary judgment, the Department submitted the Holzer declaration asserting that SOP 303 was exempt from disclosure under FOIA Exemption 7(F) because "[m]aking SOP 303 public would, e.g., enable bad actors to insert themselves into the process of shutting down or reactivating wireless networks by appropriating verification methods and then impersonating officials designated for involvement in the verification process." Holzer Decl. ¶ 26. Such bad actors would, Holzer stated, then "be [able] to disable the protocol [and] freely use wireless networks to activate * * * improvised explosive devices," so "there is a reasonable expectation that disclosure could

reasonably endanger individuals' lives or physical safety." *Id*. Exemption 7(E) also applied because, according to Holzer, SOP 303 "contains a homeland security procedure primarily intended to efficiently and effectively deter the triggering of radio-activated improvised explosive devices," and during such critical emergencies "orderly deactivation of wireless networks may be the best option for preventing and/or mitigating explosions that would endanger life and property." *Id*. ¶ 25. Holzer repeated the "bad actor" explanation for non-disclosure, adding that SOP 303's production could "circumvent or interfere with a law enforcement strategy designed to prevent activation of improvised explosive devices by providing information about when shutdown procedures are used and how a shutdown is executed." *Id*.

The district court granted summary judgment for EPIC. *EPIC*, 999 F. Supp. 2d at 27, 29-34. Although concluding the Department had satisfied Exemptions 7's threshold requirement, by showing that SOP 303 was compiled for law enforcement purposes, id. at 29-30, the district court ruled that Exemption 7(F) was inapplicable because the Department had failed to "identify the individuals [endangered by disclosure of SOP 303] with some degree of specificity." *Id*. at 32. The district court acknowledged that an earlier version of Exemption 7(F) only protected records from disclosure if their production would endanger the life or physical safety of law enforcement personnel in particular, *see* Pub. L. No. 93-502, sec. 2(b), § 552(b)(7), 88 Stat. 1561, 1563-64 (1974), and that in 1986 Congress had amended the exemption to allow non-disclosure where production would endanger other persons, too,

but looking to the legislative history concluded Congress intended only a modest expansion of the exemption. *EPIC*, 999 F. Supp. 2d at 32-34; *see* Pub. L. No. 99-570, sec. 1802(a), § 552(b)(7), 100 Stat. 3207, 3255-56 (1986). The district court also ruled that Exemption 7(E) did not apply because SOP 303 was not a technique or procedure for law enforcement investigations or prosecutions. *EPIC*, 999 F. Supp. 2d at 30-31.

The Department appeals, and our review of the grant of summary judgment is de novo, viewing the evidence in the light most favorable to the non-moving party. *Pub. Emps. for Envtl. Responsibility v. U.S. Section, Int'l Boundary & Water Comm'n, U.S.-Mexico*, 740 F.3d 195, 200 (D.C. Cir. 2014) ("*PEER*").

II.

The FOIA "mandates that an agency disclose records on request, unless they fall within one of nine exemptions." *Milner v. Dep't of Navy*, 131 S. Ct. 1259, 1262 (2011); *see* 5 U.S.C. §§ 552(a)(3)(A), (b)(1)-(9). The basic purpose of the FOIA reflects "a general philosophy of full agency disclosure." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 152 (1989) (quotation omitted); *see also Nat'l Ass'n of Home Builders v. Norton*, 309 F.3d 26, 32 (D.C. Cir. 2002). The FOIA's exemptions "are explicitly made exclusive" and "must be narrowly construed." *Milner*, 131 S. Ct. at 1262 (internal quotation marks omitted). The burden is on the agency to justify withholding the requested documents, and the FOIA directs district courts to determine *de novo* whether non-disclosure was permissible. *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 755 & n.6 (1989) (citing 5 U.S.C. § 552(a)(4)(B)).

This court's analysis of the scope of Exemption 7 in *PEER*, 740 F.3d at 202-06, is highly instructive, if not largely dispositive, here.

A.

To fall within FOIA Exemption 7, "documents must first meet a threshold requirement: that the records were 'compiled for law enforcement purposes.'" *PEER*, 740 F.3d at 202-03 (quoting 5 U.S.C. § 552(b)(7)). "[T]he term 'compiled' in Exemption 7 requires that a document be created, gathered, or used by an agency for law enforcement purposes at some time before the agency invokes the exemption." *Id*. at 203 (citing *John Doe Agency*, 493 U.S. at 155). "Law enforcement entails more than just investigating and prosecuting individuals *after* a violation of the law," *id*. (emphasis in original), and "'includes * * * proactive steps designed to prevent criminal activity and to maintain security.'" *Id*. (alteration in original) (quoting *Milner*, 131 S. Ct. at 1272 (Alito, J., concurring)).

Applying these principles, the court held in PEER that emergency action plans and inundation maps created to prevent attacks on two dams on the U.S.-Mexico border and to maintain order and ensure dam security during emergencies satisfied Exemption 7's gateway requirement. *Id*. at 204. Here, too, the Department has shown that it compiled SOP 303 for law enforcement purposes. SOP 303 was developed after the 2005 bombings of London's transportation system to address deficiencies in the United States' ability to address and respond to such threats. The Holzer declaration explains that SOP 303 sets forth the steps taken to decide whether and when to disrupt wireless networks during critical emergencies

to, for example, "efficiently and effectively deter the triggering of radio-activated improvised explosive devices." Holzer Decl. ¶ 25. As so described, SOP 303 was created to prevent crime and keep people safe, which qualify as law enforcement purposes. *PEER*, 740 F.3d at 202-04. SOP 303 meets Exemption 7's threshold test.

B.

Even if a record satisfies Exemption 7's threshold test, an agency may only withhold the record pursuant to Exemption 7(F) if the record's release "could reasonably be expected to endanger the life or physical safety of any individual." 5 U.S.C. § 552(b)(7)(F); *see PEER*, 740 F.3d at 202. Our consideration of Exemption 7(F)'s scope begins and ends with its text. *Milner*, 131 S. Ct. at 1264, 1266-67.

Exemption 7(F) covers documents that "'could reasonably be expected to endanger the life or physical safety of any individual.'" *PEER*, 740 F.3d at 202 (quoting 5 U.S.C. § 552(b)(7)(F)). The scope of the exemption is broadly stated, see id. at 205, and consequently the government, once it has met Exemption 7's threshold test, "will ordinarily be able to satisfy Exemption 7(F) for documents relating to critical infrastructure, such as * * * emergency plans." *Id*. at 206. Here, the Department maintains that disclosure of SOP 303, according to the Holzer declaration, "would enable bad actors to circumvent or interfere with a law enforcement strategy designed to prevent activation of improvised explosive devices" and "to insert themselves into the process of shutting down or reactivating wireless networks by appropriating verification methods and then

impersonating officials designated for involvement in the verification process." Holzer Decl. ¶¶ 25-26. That explanation shows that SOP 303's production could reasonably be expected to place many individuals at risk and thus, the Department contends, SOP 303 falls within the scope of the plain text of Exemption 7(F).

EPIC maintains, however, that Exemption 7(F) requires the Department to identify with some specificity the individuals who would be endangered by SOP 303's disclosure. It relies on *American Civil Liberties Union v. Department of Defense*, 543 F.3d 59 (2d Cir. 2008) ("*ACLU*"), *vacated on other grounds*, 558 U.S. 1042 (2009). In that case, the Defense Department had refused to release twenty-one photographs depicting abusive treatment of detainees by United States soldiers in at least seven different locations in Afghanistan and Iraq, invoking Exemption 7(F) on the ground that release of the photographs could reasonably be expected to endanger the life and physical safety of U.S. and Coalition troops, as well as civilians in Iraq and Afghanistan. *ACLU*, 543 F.3d at 64-65. The Second Circuit observed that "[t]he phrase 'any individual' * * * may be flexible, but is not vacuous," *id*. at 67, and concluded, in view of the FOIA's structure and the obligation of the court to construe its exemptions narrowly, that it "cannot [be] read * * * to include individuals identified solely as members of a group *so large* that risks which are *clearly speculative* for any particular individuals become reasonably foreseeable for the group." *Id*. (emphases added). The court acknowledged that individuals could be identified in some other way 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." *Id.* at 67-68. But just being a member of a vast group was not enough, *see id.*, when the group referenced encompassed "a population the size of two nations and two international expeditionary forces combined." *Id.* at 71. The court rejected the argument "that the broad scope of the word 'any' relieve[d] the[] [Defense Department] of the burden of identifying, even roughly, an individual," *id.* at 68, noting that the Supreme Court has rejected wooden, uncritical capitulation to the word "any" without analysis of surrounding language and relevant legislative history. *See id.* at 68-69 (citing *Small v. United States*, 544 U.S. 385 (2005); *Gen. Dynamics Land Sys., Inc. v. Cline*, 540 U.S. 581 (2004)). The word "any" did not require such a broad interpretation in the FOIA context. *Id.* at 68. "[E]xemption 7(F), by conditioning its application on a reasonable expectation of danger to an individual, excludes from consideration risks that are speculative with respect to any individual." *Id.* at 71 (emphasis in original).

Our decision in *PEER* does not foreclose this interpretation of Exemption 7(F), for in *PEER* the court had no occasion to decide whether it agreed with it. The court stated that "*even if* we agreed with the Second Circuit's reading of Exemption 7(F), * * * the [agency] would prevail even under the Second Circuit's approach." *PEER*, 740 F.3d at 206 (emphasis added). Unlike in *PEER*, however, here the Department does not point to a "particularized threat to a discrete population," *id.*, but rather maintains its non-production falls within Exemption 7(F) because release of SOP 303 would endanger anyone in the United States who happens to be near

an unexploded bomb or frequents high value targets. In the Department's view, it would be anomalous if it could withhold SOP 303 if disclosure poses a danger to a small group of specifically identifiable people but not where many or most people would be endangered by production. Furthermore, the Department contends that, even under the Second Circuit's interpretation, it has identified the individuals most likely to be at risk with the requisite degree of specificity because "there are identifiable groups who are more likely to be harmed" from SOP 303's disclosure, including "people near unexploded bombs, people who frequent high value targets, and bomb squads and other first responders." Appellant's Br. 19. If viewed without regard to SOP 303's requirement that there be a critical emergency for a shutdown to take place, then the Department's interpretation may not accord with the Second Circuit's approach. *See ACLU*, 543 F.3d at 71. Significantly, however, the context addressed by the Second Circuit involved "vast" populations and the court disclaimed that it was confronting a case where there was a showing of a reasonable expectation of danger with respect to one or more individuals, see id., which we conclude there is here.

The court must both narrowly construe the FOIA's exemptions and apply the statute's plain text. *See Milner*, 131 S. Ct. at 1262, 1264, 1267; *see also John Doe Agency*, 493 U.S. at 152-53; *FBI v. Abramson*, 456 U.S. 615, 630-31 (1982). The Supreme Court has rebuffed lower courts' attempts to graft atextual glosses on the FOIA. *See Milner*, 131 S. Ct. at 1267; *cf. CIA v. Sims*, 471 U.S. 159, 169 & n.13 (1985). The FOIA provides no textual basis for requiring the Department, for purposes of Exemption

7(F), to identify the specific individuals at risk from disclosure, and to do so would be to "tak[e] a red pen" to the words chosen by Congress that are to be understood to have their ordinary meaning, *Milner*, 131 S. Ct. at 1264, absent indication to the contrary. Congress' use in Exemption 7(F) of the word "any" is instructive. Generally, "'the word 'any' has an expansive meaning, that is, 'one or some indiscriminately of whatever kind.'" *Ali v. Fed. Bureau of Prisons*, 552 U.S. 214, 219 (2008) (quoting *United States v. Gonzales*, 520 U.S. 1, 5 (1997) (quoting Webster's Third New International Dictionary 97 (1976))). Although there are statutory contexts in which "any" does not mean "any," see *Small*, 544 U.S. at 388-89, 391-93; *cf. Howard v. Pritzker*, — F.3d — , Nos. 12-5370 & 12-5392, slip op. at 10-11 (D.C. Cir. Jan. 6, 2015), in the context of Exemption 7(F) the word "any" demands a broad interpretation. Congress could have, but did not, enact a limitation on Exemption 7(F), such as "any specifically identified individual." *See Sims*, 471 U.S. at 169 n.13. By contrast, in the Privacy Act Congress afforded special treatment to certain law enforcement records associated with an "identifiable individual." *See* 5 U.S.C. §§ 552a(a)(6), (j)(2)(B), (l)(2); *cf. Sims*, 471 U.S. at 169 n.13. The language of Exemption 7(F), which concerns danger to the life or physical safety of any individual, suggests Congress contemplated protection beyond a particular individual who could be identified before the fact. Exactly who will be passing near an unexploded bomb when it is triggered somewhere in the United States may often be unknowable beyond a general group or method of approach (on foot, by car, etc.), but the critical emergency itself provides a limit (*e.g.*,

a situs on the London transportation system). To be effective in protecting those individuals endangered in a critical emergency, the Department advises, SOP 303 relies on protocols that could be corrupted if made available to the public.

EPIC maintains that Congress' choice to condition Exemption 7(F)'s availability on danger to an individual, rather than danger in general, indicates a requirement that the subject of the danger be identified with at least reasonable specificity. And according to EPIC, to reject its interpretation would read "individual" out of the statute, *see ACLU*, 543 F.3d at 70, thereby violating the anti-superfluity canon. *See Milner*, 131 S. Ct. at 1268; *Qi-Zhuo v. Meissner*, 70 F.3d 136, 139 (D.C. Cir. 1995). But understood in context, the phrase "any individual" makes clear that Exemption 7(F) now shields the life or physical safety of any person, not only the law enforcement personnel protected under the pre-1986 version of the statute. The district court took note of the 1986 amendment but went beyond the exemption's plain text to impose a requirement divorced from the language Congress enacted. *See EPIC*, 999 F. Supp. 2d at 32-34. Contrary to EPIC's suggestion that Congress could have made explicit that the government need not identify the individuals at risk with specificity, "the mere possibility of clearer phrasing cannot defeat the most natural reading of a statute." *Caraco Pharm. Labs., Ltd. v. Novo Nordisk A/S*, 132 S. Ct. 1670, 1682 (2012).

EPIC implies that its interpretation of Exemption 7(F) is rooted in the exemption's command that disclosure "*could reasonably be*

expected to endanger the life or physical safety of any individual." 5 U.S.C. § 552(b)(7)(F) (emphasis added). But EPIC does not explain why the release of records or information could reasonably be expected to endanger the life or physical safety of any individual only where the individual or individuals at risk can be identified specifically. Release of SOP 303, according to the Department, poses a concrete and non-speculative danger to numerous albeit unspecified individuals, *see* Holzer Decl. ¶¶ 25-26, and the Department thereby asserted a direct nexus between disclosure and a reasonable possibility of personal harm. *See PEER*, 740 F.3d at 206. The attacks in London that triggered the establishment of SOP 303 illustrate, as noted, that before-the-fact individual identification is unlikely to be practical. To the extent EPIC is suggesting that the Department has not satisfied Exemption 7(F)'s risk threshold, that suggestion is met by "[t]he confluence of Exemption 7(F)'s expansive text and [the court's] generally deferential posture when [it] must assess national security harms." *Id.* at 205 (citing *Milner*, 131 S. Ct. at 1272 (Alito, J., concurring)).

EPIC suggests that if there is a real danger from disclosure, then the Department should classify SOP 303, bringing it within FOIA Exemption 1, which protects materials that are classified pursuant to certain Executive orders. *See* 5 U.S.C. § 552(b)(1). The Second Circuit accepted a version of this argument in ACLU, explaining that

> [i]t would be anomalous if an agency that could not meet the requirements for classification of national security material could, by characterizing the

> material as having been compiled for law enforcement purposes, evade the strictures and safeguards of classification and find shelter in [E]xemption 7(F) simply by asserting that disclosure could reasonably be expected to endanger someone unidentified somewhere in the world.

543 F.3d at 73. But the possibility of classification and the concomitant protection from disclosure provided by Exemption 1 do not render Exemption 7(F) superfluous. The Department has plausibly identified "practical barriers" to classifying SOP 303, including the fact that it "must be shared with federal law enforcement officials, [S]tate homeland security officials, and national cellular carriers." Reply Br. 6. Nor does adhering to the plain text of Exemption 7(F) eviscerate Exemption 1, which applies even to records *not* compiled for law enforcement purposes.

The NCC is presumed to be aware of the need to restore service promptly, particularly in an age in which wireless communication is a critical component of peoples' lives. *See Riley v. California*, 134 S. Ct. 2473, 2484, 2489 (2014); *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *id.* at 963 (Alito, J., concurring in the judgment). It remains for EPIC and other litigants to seek additional judicial scrutiny by requesting findings on specific matters or in camera review. At some point, as our precedent indicates, the element of trust takes over where an agency has filed a sufficiently specific sworn declaration by a knowledgeable official. *See Juarez v. U.S. Dep't of Justice*, 518 F.3d 54, 60 (D.C.

Cir. 2008); *King v. U.S. Dep't of Justice*, 830 F.2d 210, 217 (D.C. Cir. 1987). Even if SOP 303's shutdown protocol is a matter of significant public interest, balancing when the value of producing certain categories of documents outweighs the government's generic justifications for non-disclosure is what the Congress has done in enacting and amending the FOIA. *See Milner*, 131 S. Ct. at 1265 n.5; *PEER*, 740 F.3d at 198; *Pratt v. Webster*, 673 F.2d 408, 416 & n.17 (D.C. Cir. 1982).

Finally, to the extent EPIC looks to Exemption 7(F)'s legislative history, the court's choice when "presented, on the one hand, with clear statutory language and, on the other, with dueling [congressional statements]," is foreordained. *See Milner*, 131 S. Ct. at 1267. Prior to the 1986 FOIA amendments, Exemption 7(F) protected records the release of which would "endanger the life or physical safety of law enforcement personnel." *See* Pub. L. No. 93-502, sec. 2(b), § 552(b)(7), 88 Stat. 1561, 1563-64 (1974). The exemption did not cover witnesses, interviewees, victims, informants, or families of law-enforcement personnel and thus, for example, undermined law enforcement officers' ability to enlist informants. 131 Cong. Rec. 253 (daily ed. Jan. 3, 1985) (statement of Hon. Carol E. Dinkins, Deputy U.S. Att'y Gen.). To remedy this omission, the Executive Branch asked that Exemption 7(F) be amended. *Id.* In response, Congress expanded Exemption 7(F) to protect law-enforcement documents if their release would endanger "any individual." 5 U.S.C. § 552(b)(7)(F); *see* Pub. L. No. 99-570, sec. 1802(a), § 552(b)(7), 100 Stat. 3207, 3255-56 (1986).

EPIC views Congress' amendment of Exemption 7(F) in 1986 to bring only witnesses, interviewees, victims, informants, and families of law-enforcement personnel within the exemption. There are statements of Members of Congress and the Executive Branch that reflect concern about those groups' prior omission. *See* 130 Cong. Rec. 3,502 (daily ed. Feb. 27, 1984) (statement of Sen. Hatch) ("The bill would * * * extend[] [E]xemption 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."); 130 Cong. Rec. 3,520 (daily ed. Feb. 27, 1984) (statement of Sen. Leahy) (describing certain changes to the FOIA as "narrowly aimed so that they will not interfere with the public's right to know where law enforcement is not seriously jeopardized"). Other Members' statements viewed the amendment to Exemption 7(F) as relatively broad. For instance, Senator Hatch, the principal sponsor of the amendment, remarked that the changes to Exemption 7 were "intended to * * * ease considerably a Federal law enforcement agency's burden in invoking" it. 132 Cong. Rec. 31,424 (daily ed. Oct. 15, 1986). Although General Dinkins stated that the language of Exemption 7 would be "modified slightly - not revised wholesale," 131 Cong. Rec. 248, she also expressed concern that the prior version of the exemption did not protect "the life of any other person" besides law enforcement personnel. *Id.* at 253. And her explanation that the 1986 amendments expanded Exemption 7(F) "to include *such* persons as witnesses, potential witnesses, and family members," *id.* (emphasis added), is reasonably understood as illustrative not exclusive. In any event, what

Congress enacted was broad language that was not limited to protection of law enforcement personnel and related persons. *See PEER*, 740 F.3d at 205. "We will not . . . allow[] ambiguous legislative history to muddy clear statutory language." *Milner*, 131 S. Ct. at 1266. "All we hold today is that Congress has not enacted the FOIA exemption [EPIC] desires. We leave to Congress, as is appropriate, the question whether it should do so." *Id.* at 1271.

Accordingly, we hold that the Department permissibly withheld much, if not all of SOP 303, because its release, as described in the Holzer declaration, could reasonably be expected to endanger individuals' lives or physical safety, and we reverse the grant of summary judgment. As such, we need not now decide whether Exemption 7(E) applies. *See Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice*, 331 F.3d 918, 925 (D.C. Cir. 2003). We will remand the case, however, for the district court to address, in the first instance, the issue of segregability, *see* 5 U.S.C. § 552(b); *Stolt-Nielsen Transp. Grp. Ltd. v. United States*, 534 F.3d 728, 734 (D.C. Cir. 2008); *Trans-Pac. Policing Agreement v. U.S. Customs Serv.*, 177 F.3d 1022, 1028 (D.C. Cir. 1999), leaving it to determine "whether more detailed affidavits are appropriate or whether an alternative such as *in camera* review would better strike the balance between protecting [exempted] information and disclosing nonexempt information as required by the FOIA." *Stolt-Nielsen*, 534 F.3d at 734-35 (alteration in original) (quotation omitted); *see* 5 U.S.C. § 552(a)(4)(B); *Neill v. U.S. Dep't of Justice by Reno*, No. 93-5292, 1994 WL 88219, at *1 (D.C. Cir. Mar. 9, 1994).

APPENDIX B

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 14-5013 **September Term, 2014**
1:13-cv-00260-JEB
Filed On: May 13, 2015

Electronic Privacy Information Center,
Appellee

v.

United States Department of Homeland Security,
Appellant

BEFORE: Garland, Chief Judge; Henderson, Rogers, Tatel, Brown, Griffith, Kavanaugh, Srinivasan, Millett, Pillard, and Wilkins, Circuit Judges; Sentelle and Randolph, Senior Circuit Judges

ORDER

Upon consideration of appellee's petition for rehearing en banc, the response thereto, and the absence of a request by any member of the court for a vote, it is

ORDERED that the petition be denied.

Per Curiam

FOR THE COURT: Mark J. Langer, Clerk

BY: /s/ Ken R. Meadows, Deputy Clerk

APPENDIX C

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Civil Action No. 13-260 (JEB)

ELECTRONIC PRIVACY
INFORMATION CENTER,

Plaintiff,

v.

DEPARTMENT OF HOMELAND SECURITY,

Defendant.

MEMORANDUM OPINION

This case concerns efforts of the Electronic Privacy Information Center under the Freedom of Information Act to obtain documents related to the Department of Homeland Security's Standard Operating Procedure 303. This protocol governs the shutdown of wireless networks in emergencies to, *inter alia*, prevent the remote detonation of explosive devices. After DHS withheld the lion's share of the one responsive document it found, EPIC brought this action. DHS now moves for summary judgment, arguing that its search for documents was adequate, that it properly withheld the bulk of SOP 303 under applicable FOIA exemptions, and that no other non-exempt parts of the document could be released. EPIC cross-moves for summary judgment, contending that the two exemptions DHS relied on to withhold

most of the document, 7(E) and 7(F), do not apply here. As the Court believes EPIC has the better of this argument, it will dispose of the Motions accordingly.

I. Background

Standard Operating Procedure 303 is an "Emergency Wireless Protocol[] . . . codifying a shutdown and restoration process for use by commercial and private wireless networks during national crises." National Security Telecommunications Advisory Committee, NSTAC Issue Review 2006-07 at 139 (2007), http://www.dhs.gov/sites/default/files/publications/2006- 2007%20NSTAC%20Issue%20Review_0.pdf. The wireless networks could be shut down in certain emergency situations to, *inter alia*, "deter the triggering of radio-activated improvised explosive devices." See Def. Mot., Exh. 2 (Declaration of James V.M.L. Holzer), ¶ 25.

On July 10, 2012, EPIC submitted a FOIA request to DHS seeking: "(1) the full text of Standard Operating Procedure 303 (SOP 303), which describes a shutdown and restoration process for use by 'commercial and private wireless networks' in the event of a crisis; (2) the full text of the pre-determined 'series of questions' that determines if a shutdown is necessary; and (3) any executing protocols or guidelines related to the implementation of SOP 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations." Id., ¶ 9. DHS responded to EPIC on August 21, 2012, saying that it "had conducted comprehensive searches for records that would be responsive to the

request[, but] . . . that [DHS was] unable to locate or identify any responsive records." Id., ¶ 16. EPIC administratively appealed on October 2, 2012, and on March 25, 2013, the United States Coast Guard, Office of the Chief Administrative Law Judge – the office that reviews these FOIA appeals – "remanded the matter back to DHS Privacy for further review." Id., ¶¶ 17-18.

Upon additional inspection, DHS located one responsive record, the very document EPIC had requested: Standard Operating Procedure 303. Id., ¶¶ 19-20. "Included as part of SOP 303 itself are the two other categories of records that EPIC seeks, *i.e.*, the full text of the predetermined series of questions that determines if a shutdown is necessary, and the executing protocols related to the implementation of SOP 303." Id., ¶ 21. DHS "determined that the SOP is the only responsive document because there are no other documents that contain the full text of the questions or any executing protocols." Id.

Portions of SOP 303 – "names, direct-dial telephone numbers, and email addresses for state homeland security officials" – were withheld from EPIC under Exemptions 6 and 7(C), which generally permit withholding of personal information. Id., ¶¶ 23-24. The remainder of the document was withheld under Exemptions 7(E) and 7(F), which permit withholding of certain law-enforcement information if it, respectively, would "disclose techniques and procedures for law enforcement investigations or prosecutions" or "could reasonably be expected to endanger the life or physical safety of any individual." 5 U.S.C. § 552(b)(7); Holzer Decl., ¶¶ 25-26.

On February 27, 2013, EPIC filed this lawsuit seeking the release of the withheld portions of SOP 303. Both parties have now cross-moved for summary judgment.

II. Legal Standard

Summary judgment may be granted if "the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A genuine issue of material fact is one that would change the outcome of the litigation. See Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986) ("Only disputes over facts that might affect the outcome of the suit under the governing law will properly preclude the entry of summary judgment."). In the event of conflicting evidence on a material issue, the Court is to construe the evidence in the light most favorable to the non-moving party. See Sample v. Bureau of Prisons, 466 F.3d 1086, 1087 (D.C. Cir. 2006). Factual assertions in the moving party's affidavits or declarations may be accepted as true unless the opposing party submits his own affidavits, declarations, or documentary evidence to the contrary. Neal v. Kelly, 963 F.2d 453, 456 (D.C. Cir. 1992).

FOIA cases typically and appropriately are decided on motions for summary judgment. See Defenders of Wildlife v. Border Patrol, 623 F. Supp. 2d 83, 87 (D.D.C. 2009); Bigwood v. U.S. Agency for Int'l Dev., 484 F. Supp. 2d 68, 73 (D.D.C. 2007). In FOIA cases, the agency bears the ultimate burden of proof. See U.S. Dep't of Justice v. Tax Analysts, 492 U.S. 136, 142, n.3 (1989). The Court may grant summary judgment based solely on information

provided in an agency's affidavits or declarations when they describe "the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not 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). Such affidavits or declarations are accorded "a presumption of good faith, which cannot be rebutted by 'purely speculative claims about the existence and discoverability of other documents.'" SafeCard Servs., Inc. v. SEC, 926 F.2d 1197, 1200 (D.C. Cir. 1991) (quoting Ground Saucer Watch, Inc. v. CIA, 692 F.2d 770, 771 (D.C. Cir. 1981)).

III. Analysis

Congress enacted FOIA in order to "pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny." Dep't of Air Force v. Rose, 425 U.S. 352, 361 (1976) (citation omitted). "The basic purpose of FOIA 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." John Doe Agency v. John Doe Corp., 493 U.S. 146, 152 (1989) (citation omitted). The statute provides that "each agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules . . . shall make the records promptly available to any person." 5 U.S.C. § 552(a)(3)(A). Consistent with this statutory mandate, federal courts have jurisdiction to order the production of records that an agency improperly withholds. See 5 U.S.C. §

552(a)(4)(B); Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 755 (1989). "Unlike the review of other agency action that must be upheld if supported by substantial evidence and not arbitrary and capricious, FOIA expressly places the burden 'on the agency to sustain its action' and directs the district courts to 'determine the matter de novo.'" Reporters Comm., 489 U.S. at 755 (quoting 5 U.S.C. § 552(a)(4)(B)). "At all times courts must bear in mind that FOIA mandates a 'strong presumption in favor of disclosure' . . . ." Nat'l Ass'n of Home Builders v. Norton, 309 F.3d 26, 32 (D.C. Cir. 2002) (quoting Dep't of State v. Ray, 502 U.S. 164, 173 (1991)).

In moving for summary judgment, DHS first contends that its search was adequate. EPIC does not contest this point. DHS next maintains that its withholding of personal identifying information under Exemptions 6 and 7(C) was appropriate. EPIC makes no challenge here either. See Opp. at 5 n.1. Instead, it saves its ammunition for DHS's claim that it properly withheld the bulk of SOP 303 under both Exemption 7(E) and 7(F). Because the Court ultimately finds that the agency's invocation of these exemptions was not proper, it need not address the last issue EPIC raises – namely, whether DHS performed an appropriate segregability analysis. The Court will begin with a discussion of 7(E) and then move to a consideration of 7(F).

A. Exemption 7(E)

Exemption 7 authorizes the Government to withhold "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or

information" meets one of six requirements. 5 U.S.C. § 552(b)(7); see Keys v. Dep't of Justice, 830 F.2d 337, 340 (D.C. Cir. 1987) ("[Exemption 7] exempts such documents from disclosure only to the extent that production of the information might be expected to produce one of six specified harms."). The fifth subparagraph – 7(E) – permits withholding where production "would disclose techniques and procedures for law enforcement investigations or prosecutions." 5 U.S.C. § 552(b)(7)(E). The agency here must thus satisfy two requirements: First, the record must be compiled for law-enforcement purposes; and second, production must disclose techniques and procedures for law-enforcement investigations.

DHS clearly surpasses the first hurdle. "Steps by law enforcement officers to prevent terrorism surely fulfill 'law enforcement purposes.'" Milner v. Dep't of Navy, 131 S. Ct. 1259, 1272 (2011) (Alito, J., concurring). DHS need only make "a colorable claim" of a rational nexus "between the agency's activity [that created the document] and its law enforcement duties." Keys, 830 F.2d at 340. DHS created SOP 303 to "establish[] a protocol for verifying that circumstances exist that would justify shutting down wireless networks" "to efficiently and effectively deter the triggering of radio-activated improvised explosive devices." Holzer Decl., ¶ 25. There is, accordingly, a rational nexus between SOP 303's protocol for preventing the triggering of radio-activated IEDs and DHS's law-enforcement purpose of keeping the country safe.

DHS's trouble comes at the second step, which requires that the disclosure would reveal "techniques and procedures for law enforcement investigations or prosecutions." 5 U.S.C. § 552(b)(7)(E). The key

question is whether the agency has sufficiently demonstrated how SOP 303, which articulates protective measures, is a technique or procedure "for law enforcement investigations or prosecutions." Id.

The Court must begin by "presum[ing] that a legislature says in a statute what it means and means in a statute what it says there." Connecticut Nat'l Bank v. Germain, 503 U.S. 249, 253-54 (1992). Of particular relevance here, Congress amended FOIA in 1986. See PL 99-570, Oct. 27, 1986, 100 Stat 3207. Prior to the 1986 amendments, to merit withholding, Exemption 7 first required "investigatory records compiled for law enforcement purposes," and subparagraph (E) then required that the records would "disclose investigative techniques and procedures." See PL 93-502, Nov. 21, 1974, 88 Stat 1561. The 1986 amendments "delet[ed] any requirement [in the first step] that the information be 'investigatory,'" Tax Analysts, 294 F.3d at 79, and broadened the permissible withholding to "records or information compiled for law enforcement purposes." See PL 99-570, Oct. 27, 1986, 100 Stat 3207. Congress, however, retained the investigatory requirement in 7(E). See id. (slightly modifying subparagraph (E), but keeping requirement that information be "for law enforcement investigations or prosecutions"). Congress thus specifically and intentionally chose to remove the investigatory requirement from the first step and to leave it in the second step. The Court, therefore, will apply "the usual rule that 'when the legislature uses certain language in one part of the statute and different language in another, the court assumes different meanings were intended.'" Sosa v. Alvarez-Machain, 542 U.S. 692, 711 n.9 (2004) (quoting 2A N. Singer,

Statutes and Statutory Construction § 46:06, p. 194 (6th rev. ed. 2000)).

Looking at the amended language, the Court agrees with the Government that Exemption 7's mention of "law enforcement purposes" may certainly include preventive measures. See Mot. at 9-10. The problem is that 7(E)'s reference to "law enforcement investigations and prosecutions" does not. This distinction finds support in Justice Alito's concurrence in Milner, a case that dealt with the applicability of Exemption 2. In his opinion, Justice Alito explained that "[t]he ordinary understanding of law enforcement [purposes] includes not just the investigation and prosecution of offenses that have already been committed, but also proactive steps designed to prevent criminal activity and to maintain security." Milner, 131 S. Ct. at 1272 (Alito, J., concurring). Justice Alito went on to explain how, in context, Exemption 7's reference to "law enforcement purposes" "involve[s] more than just investigation and prosecution," which he describes as "narrower activities" confined to Exemption 7's subparagraphs. See id. at 1273 ("Congress' decision to use different language to trigger Exemption 7 confirms that the concept of 'law enforcement purposes' sweeps in activities beyond [subparagraph (E)'s] investigation and prosecution.")

If "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. Reading Exemption 7(E) as such, moreover, is in keeping with FOIA's "basic policy that

disclosure, not secrecy, is the dominant objective of the Act," Pub. Citizen, Inc. v. Rubber Mfrs. Ass'n, 533 F.3d 810, 813 (D.C. Cir. 2008) (internal quotation marks omitted), and the well-settled practice of reading FOIA exemptions narrowly. See Milner, 131 S. Ct. at 1265 ("We have often noted 'the Act's goal of broad disclosure' and insisted that the exemptions be 'given a narrow compass.'") (quoting Dep't of Justice v. Tax Analysts, 492 U.S. 136, 151 (1989)).

In arguing against such an interpretation, DHS relies on a nearly 30-year-old case from this district that upheld the Secret Service's invocation of Exemption 7(E) to shield "records pertaining to . . . two armored limousines for the President." U.S. News & World Report v. Dep't of Treasury, 1986 U.S. Dist. LEXIS 27634, at *1 (D.D.C. March 26, 1986). In that case, the court rejected plaintiff's argument – similar to the one EPIC makes here – "that the information at issue [] would reveal 'protective' not 'investigative' techniques and procedures" and concluded that "[i]t is inconceivable . . . that Congress meant to afford these [preventive] activities any less protection from disclosure simply because they do not fit within the traditional notion of investigative law enforcement techniques." Id. at *6. This case, however, was decided before the 1986 amendments changed the language of the relevant clauses, making it not "inconceivable," but in fact probable that Congress intended to differentiate between preventive and investigative activities. U.S. News also predates Milner's insistence on reading the exemptions narrowly. See 131 S. Ct. at 1265; see also Dep't of Justice v. Landano, 508 U.S. 165, 181 (1993) (noting Court's "obligation to construe FOIA exemptions narrowly in favor of disclosure"). The

Court, therefore, does not believe U.S. News dictates a different result.

The agency's last gambit is a *post hoc* attempt in its Reply to classify SOP 303 as an investigative technique. It claims that "[p]reventing explosives from detonating preserves evidence . . . and, thereby, facilitates the investigation into who built and placed the bomb." See Def's Reply at 5-6. This is too little, too late. As EPIC notes, "[N]o ordinary speaker of the English language" would describe SOP 303 – "a protocol for verifying that circumstances exist that would justify shutting down wireless networks" "to efficiently and effectively deter the triggering of radio-activated improvised explosive devices," Holzer Decl., ¶ 25 – as an evidence gathering technique. Pl's Reply at 3.

The Court will thus read Exemption 7(E) in a manner that harmonizes with FOIA's purpose of disclosure, the canons of statutory construction, and the Supreme Court's guidance to read FOIA's exemptions narrowly.

B. Exemption 7(F)

DHS next argues that SOP 303 was also properly withheld under Exemption 7(F). This exemption authorizes the Government to withhold "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to endanger the life or physical safety of any individual." 5 U.S.C. § 552(b)(7)(F). As the Court explained in relation to Exemption 7(E), the agency easily clears the "law enforcement purposes" hurdle. See Section III.A, *supra*.

Yet again, though, the second requirement leads to DHS's undoing. DHS must show that production would "endanger the life or physical safety of any individual." 5 U.S.C. § 552(b)(7)(F) (emphasis added). The agency argues that SOP 303's "disclosure could reasonably be expected to endanger the physical safety of individuals near unexploded bombs." Mot. at 13. DHS's thinking goes like this: 1) SOP 303 "describes a procedure for shutting down wireless networks to prevent bombings"; 2) "[r]eleasing information regarding this protocol would enable 'bad actors' to blunt its usefulness"; and 3) this "could reasonably be expected to endanger the physical safety of those near a bomb by increasing the chances that the process will fail and the bomb will explode." Id. In other words, the "any individual" test is satisfied because those endangered are any individuals near a bomb. Although this interpretation holds some appeal, the Court must conclude that the agency reads the "any individual" standard too broadly.

While DHS is correct that Exemption 7(F) is not limited to protecting law-enforcement personnel from harm, see Amuso v. Dep't of Justice, 600 F. Supp. 2d 78, 101 (D.D.C. 2009), the agency still must identify the individuals at risk with some degree of specificity. See ACLU v. Dep't of Defense, 543 F.3d 59, 66-72 (2d Cir. 2008) ("The phrase 'any individual' in exemption 7(F) may be flexible, but is not vacuous."), vacated on other grounds, 558 U.S. 1042 (2009).

The Second Circuit in ACLU considered a similar question to the one raised here, and its opinion is instructive. The Government there wished to apply the "any individual" standard to prevent the

release of photographs "depict[ing] abusive treatment of detainees by United States soldiers in Iraq and Afghanistan" on the ground that "the release of the disputed photographs will endanger United States troops, other Coalition forces, and civilians in Iraq and Afghanistan." Id. at 63. In an extensive examination of the phrase "any individual" – in light of the Supreme Court's admonition to interpret FOIA exemptions narrowly – the court rejected the Government's argument "that it could reasonably be expected that out of a population the size of two nations and two international expeditionary forces combined, someone somewhere will be endangered as a result of the release of the Army photos." Id. at 71. It concluded that "an agency must identify at least one individual with reasonable specificity and establish that disclosure of the documents could reasonably be expected to endanger that individual." Id.

Central to the ACLU court's holding was its thorough examination of the legislative history of 7(F), which this Court also finds significant. Prior to the 1986 FOIA amendments, Exemption 7(F) protected records, the release of which would "endanger the life or physical safety of law enforcement personnel." See PL 93-502, Nov. 21, 1974, 88 Stat 1561 (emphasis added). The exemption served to withhold "information which would reveal the identity of undercover agents, State or Federal, working on such matters as narcotics, organized crime, terrorism, or espionage." Edward A. Levi, Attorney General's Memorandum on the 1974 Amendments to the Freedom of Information Act, pt. I.B (1975), available at http://www.justice.gov/oip/74agmemo.htm, cited in

ACLU, 543 F.3d at 77-78. The exemption did not cover witnesses, interviewees, victims, informants, or families of law-enforcement personnel; as a result, among other impairments, it "harmed the ability of law enforcement officers to enlist informants." Statement of the Chair of the Senate Committee on the Judiciary's Subcommittee on the Constitution (the subcommittee with jurisdiction over FOIA), 131 Cong. Rec. S263 (daily ed. Jan. 3, 1985), cited in ACLU, 543 F.3d at 78.

To remedy this omission, the Government asked for an amendment to "modif[y] slightly – not revise[] wholesale" – the scope of 7(F). Statement of Carol E. Dinkins, Deputy Attorney General, 131 Cong. Rec. S263 (daily ed. Jan. 3, 1985), cited in ACLU, 543 F.3d at 79. As the Government stated in support of the amendment:

> The current language in Exemption 7(F) exempts records only if their disclosure would endanger the life of a law enforcement officer. However, the exemption does not give similar protection to the life of any other person. [The proposed amendment] expands 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

Id., cited in ACLU, 543 F.3d at 78. Congress complied, passing "only modest changes to the FOIA . . . , [a]nd slight[ly] expan[ding] . . . exemption[] . . . (7)(F)." Statement of the Chair of the House Committee on Government Operations, Subcommittee on Government Information, Justice,

and Agriculture (the subcommittee with jurisdiction over FOIA), 132 Cong. Rec. H9455 (daily ed. Oct. 8, 1986), cited in ACLU, 543 F.3d at 79.

Congress ultimately settled on the broader term of "any individual," as opposed to, for example, "any individual connected to or assisting law enforcement." The Court, therefore, would be overly restrictive if it defined "any individual" in the latter, cabined manner. Yet, bearing in mind the modest expansion intended and the prescription that exemptions must be read narrowly, the Court must require some specificity and some ability to identify the individuals endangered.

Against this backdrop, the Government here nonetheless seeks a broader interpretation of "any individual" than was rejected in ACLU. The individuals that DHS claims satisfy the standard are anyone "within the blast radius of a remotely detonated bomb." See Def's Mot. at 12-13; Def's Reply at 11. As EPIC notes, "These hypothetical bombs" – like the hypothetical danger to troops and civilians in ACLU – "could materialize at any time, in any place, and affect anyone in the United States." Pl's Reply at 9. These individuals, therefore, are "identified only as a member of a vast population." ACLU, 543 F.3d at 68. In fact, the population is vaster here because it encompasses all inhabitants of the United States, while in ACLU it only covered people in Iraq and Afghanistan. Indeed, 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. This expansive interpretation of "any

individual" is far broader than what the Government had in mind when it requested a "slight[]" enlargement of 7(F) in 1985, and far more than Congress approved in its "slight expansion of exemption[] . . . (7)(F)" in 1986. See 131 Cong. Rec. at S263; 132 Cong. Rec. at H9455.

The primary case DHS relies on for the proposition that anyone near unexploded bombs is a specific-enough group, Living Rivers, Inc. v. U.S. Bureau of Reclamation, 272 F. Supp. 2d 1313 (D. Utah 2003), is easily distinguishable. In that case, the court upheld the Government's invocation of Exemption 7(F) to withhold inundation maps that showed downstream communities that would be at risk in the event of dam failure. Id. at 1315, 1321-22. The danger was that terrorists could use the maps to better plan prospective attacks. Id. at 1321. There is a critical difference, however, between the populations in danger in that case and this one. In Living Rivers, the Government contended that "disclosure of the inundation maps 'could reasonably place at risk the life or physical safety of those individuals who occupy the downstream areas that would be flooded by a breach of Hoover Dam or Glen Canyon Dam.'" Id. (emphasis added) (internal citation omitted). Here, the individuals at risk include anyone near any unexploded bomb, which could include anyone anywhere in the country. See Mot. at 12-13, Def's Reply at 11. As the Living Rivers population was clearly specified and limited, the case, even were it binding, does not affect the Court's decision.

The additional cases DHS cites in its Reply for the proposition that individuals need not be specifically identified all involve far narrower groups

with readily identifiable members than those at risk here. See Zander v. Dep't of Justice, 885 F. Supp. 2d 1, 7 (D.D.C. 2012) (upholding 7(F) withholding where Government identified class of people at risk as police officers working in prisons while forcibly removing prisoners from their cells); Pub. Employees for Envtl. Responsibility v. U.S. Section Int'l Boundary & Water Comm'n, 839 F. Supp. 2d 304, 327-28 (D.D.C. 2012) (upholding 7(F) withholding of inundation maps for similar reasons as those in Living Rivers); Peter S. Herrick's Customs & Int'l Trade Newsletter v. U.S. Customs & Border Prot., No. 04-00377, 2006 WL 1826185, at *8-9 (D.D.C. June 30, 2006) (upholding 7(F) withholding relating to, *inter alia*, customs officials' seized contraband because information's release would "put[] Customs' officials at risk from individuals who would seek to acquire such items").

Reading 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. See Milner, 131 S. Ct. at 1265 ("We have often noted 'the Act's goal of broad disclosure' and insisted that the exemptions be 'given a narrow compass.'") (quoting Dep't of Justice v. Tax Analysts, 492 U.S. 136, 151 (1989)); Landano, 508 U.S. at 181 (noting Court's "obligation to construe FOIA exemptions narrowly in favor of disclosure"); Rose, 425 U.S. at 361 (noting "basic policy that disclosure, not secrecy, is the dominant objective of the Act"). Exemption 7(F), therefore, cannot be read as expansively as the Government proposes, and thus cannot justify withholding SOP 303. The Court does not dispute that it will be difficult in some cases to decide whether endangered

individuals have been sufficiently identified, but such hardship does not exist here.

* * *

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. . . . All we hold today is that Congress has not enacted the FOIA exemption the Government desires. We leave to Congress, as is appropriate, the question whether it should do so." Milner, 131 S. Ct. at 1271. Indeed, in issuing guidance on FOIA exemptions in a post-Milner world, the Department of Justice's Office of Information Policy concluded that "it seems inevitable that there will be some sensitive records that will not satisfy the standards of any of the Exemptions." OIP Guidance, Exemption 2 After the Supreme Court's Ruling in Milner v. Department of the Navy 15 available at http://www.justice.gov/oip/foiapost/milner-navy.pdf. Standard Operating Procedure 303 is such a record.

IV. Conclusion

For the foregoing reasons, the Court will issue a contemporaneous Order granting judgment in Plaintiff's favor and ordering DHS to turn over SOP 303 – with redactions related only to Exemptions 6 and 7(C) – to Plaintiff within 30 days. Mindful of the

national-security implications involved, and appreciating that disclosure of SOP 303 would effectively moot any appeal, this Opinion and accompanying Order will be stayed for 30 days in order to allow for either appeal, should the Government wish to file one, or 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. If DHS notices an appeal by December 12, 2013, the stay shall remain in effect until the Court of Appeals rules on such appeal.

/s/ James E. Boasberg
JAMES E. BOASBERG
United States District Judge

Date: November 12, 2013

APPENDIX D

DECLARATION OF JAMES V.M.L. HOLZER, I, IN SUPPORT OF DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

I, James V.M.L. Holzer declare and state as follows:

1. I am the Senior Director of FOIA Operations for the Department of Homeland Security Privacy Office (DHS Privacy). I am the Department official immediately responsible for responding to requests for records under the Freedom of Information Act (FOIA), 5 U.S.C. §552 (the FOIA), the Privacy Act, 5 U.S.C. § 552a (the Privacy Act), and other applicable records access Statutes and Regulations. I have held this position since November 7, 2012. Prior to that, I held the position of Director of Disclosure and FOIA Operations. I have been with the Department since 2009. I make the following statements based upon my personal knowledge, which in turn is based on a personal review of the records in the files established for processing FOIA requests and upon information furnished to me in the course of my official duties. Through the exercise of my official duties, I have also become familiar with the background of this case and have read a copy of the complaint.

2. The purpose of this declaration is to provide an overview of the FOIA process at DHS and to explain how the FOIA request that is the subject of the instant litigation was processed This declaration is submitted in support of defendant's motion for summary judgment.

3. The Department of Homeland Security's (DHS) FOIA operations is carried out by the DHS Privacy Office. FOIA requests directed to DHS are reviewed by DHS Privacy, and that office also refers those requests to the DHS offices and components likely to possess responsive documents. DHS Privacy also oversees FOIA and Privacy Act operations throughout DHS.

4. After DHS Privacy receives a FOIA request, that request receives a unique identification number. DHS Privacy uses the unique identification number to track the status of all FOIA requests that it receives. DHS Privacy then reviews the request to determine which DHS office or component is likely to possess responsive documents. This review may include conversations with DHS component FOIA offices to determine if they had received the same request directly from the public and if the component has responsive documents.

5. In addition to DHS Privacy, DHS components maintain offices that handle FOIA requests. These offices also use an automated case tracking systems which assigns case control numbers to all FOIA requests received by that component. Components log all incoming FOIA requests into an automated case tracking system, and input information about each request into the system (including, but not limited to, the requester's name and/or organization and, in the case of FOIA requests, the request's topic). These numbers are used to track the status of incoming FOIA requests.

6. The mission of DHS's National Protection and Programs Directorate (NPPD) is to assure a safe, secure, and resilient infrastructure. There are four subcomponents within NPPD, which are the Federal

Protective Service (FPS), Office of Cybersecurity and Communications (CS&C), Office of Infrastructure Protection (IP), and Office of Biometric Identity Management (OBIM). FPS provides security and law enforcement services to federally owned and leased buildings, facilities, properties. CS&C's mission is to assure the security, resiliency, and reliability of the nation's cyber and communications infrastructure. IP leads a coordinated national effort to reduce risk to our critical infrastructure. OBIM uses innovative technological solutions to provide decision-makers with accurate biometric-based information.

7. NPPD also has a FOIA Office, which processes FOIA requests received directly from the general public by postal delivery or email, and those referred to it by DHS Privacy, DHS component FOIA offices and federal agencies. The NPPD FOIA office processes FOIA requests for all NPPD subcomponents and offices.

8. When the NPPD FOIA office personnel receive a referral or tasking from DHS Privacy or some other source, NPPD FOIA personnel make a determination regarding which NPPD subcomponent or program office may have responsive documents, and then refer the request to the appropriate subcomponent or office.

EPIC'S JULY 10, 2012 FOIA REQUEST

9. On July 18, 2012, DHS Privacy received a FOIA request from EPIC dated July 10, 2012. EPIC requested the following categories of records: (1) the full text of Standard Operating Procedure 303 (SOP 303), which describes a shutdown and restoration process for use by "commercial and private wireless networks" in the event of a crisis; (2) the full text of the predetermined "series of questions" that

determines if a shutdown is necessary; and (3) any executing protocols or guidelines related to the implementation of SOP 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

10. When DHS Privacy received EPIC's FOIA request it had to determine which offices at DHS would be most likely to have records responsive to the request. EPIC specifically mentioned the National Communications System (NCS) and the National Coordinating Center for Communications (NCC) in its request, each of which was or is an NPPD organization. The NCS was formerly an organization within NPPD that was established to provide the Federal Government with national security and emergency preparedness communications as well as formulate and implement policies in this area. By Executive Order 13618 on July 6, 2012, the NCS was eliminated, and replaced with an alternate structure for performing the same functions.

11. The NPPD FOIA office believed that there were no responsive records. As discussed more fully below, the NPPD FOIA Office was incorrect, in that NPPD indeed had responsive documents, namely SOP 303. The NPPD FOIA office learned of its mistake later. The mistake was due in part to confusion regarding a similar FOIA request from another requester seeking certain records relating to the activation of SOP 303, but not the SOP itself, as EPIC had requested. Because the two FOIA requests were pending within the same timeframe and dealt with the same general subject matter area, NPPD did not fully appreciate the difference between EPIC's

request, which sought only three specific categories of documents (i.e., the full text of SOP 303, the full text of the series of questions used to determine the necessity of shutdown, and any executing protocols or guidelines), and the other FOIA request, which sought records related to particular security events where the SOP may have been implemented and activated.

12. In addition to referring EPIC's request to NPPD, DHS Privacy also directed the DHS Management Directorate (MGMT), the Office of the Chief Information Officer (OCIO) and the Under Secretary for Management (USM) to search for responsive documents. DHS Privacy believed that these offices would be likely to have documents related to communications policy, such as SOP 303. The DHS Management Directorate is the office responsible for Department budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements. Because of its broad portfolio, MGMT often will know about a policy, procedure or initiative, and DHS Privacy often directs MGMT to search for responsive documents.

13. DHS Privacy directed that OCIO conduct a search because the request related to communications. OCIO is often involved in, and consulted on, information and communication issues, which might have had some information about the subject matter of the request. USM also was tasked to conduct a search because, like MGMT, it has a broad portfolio. The office oversees (i) the promulgation of policy, (ii) operations and (iii)

oversight, for each of the critical management lines-of-business. These lines of business include: acquisition, human capital, budget and finance, information technology, capital assets, and security.

14. DHS Privacy sent an acknowledgement to EPIC on July 24, 2012, assigning the matter file number DHS/OS/PRIV 12-0598 and indicated that DHS Privacy had tasked MGMT, OCIO, and USM with a search based on the opinion that those offices would be most likely to have records responsive to the request.

15. Each office conducted a search for documents related to the SOP, using the search terms "Standard Operating Procedure 303" and "SOP 303." These offices do not have one database to search for records that are responsive to Freedom of Information and/or Privacy Act requests. Consequently, each of the component offices was tasked to search for records. In this instance, for purposes of coordination, search requests were sent to the Chief of Staffs in each of the three Offices mentioned above. In each case, the offices searched shared computer drives, Share Point sites, and emails for information about the requested records. These are the storage places where DHS employees would typically place information about the products they are working on as well as copies of any final products that are proposed for dissemination or are actually disseminated. In each case, the Offices reported no records responsive to the request.

16. DHS Privacy sent its final response to EPIC on August 21, 2012. In the final response, DHS Privacy said that MGMT, OCIO, and USM, had conducted comprehensive searches for records that would be responsive to the request. DHS Privacy also

said that these offices were unable to locate or identify any responsive records.

17. On October 2, 2012, DHS Privacy received an appeal from EPIC dated September 13, 2012. DHS Privacy acknowledged the appeal on October 25, 2012. DHS Privacy forwarded the appeal to the United States Coast Guard, Office of the Chief Administrative Law Judge (ALJ), as that office reviews FOIA appeals on behalf of DHS' Office of the General Counsel.

18. By the letter dated March 25, 2013, the ALJ notified DHS Privacy that it had reviewed the appeal, and it remanded the matter back to DHS Privacy for further review.

19. On April 19, 2013, DHS Privacy reached out to various offices, including MGMT, OCIO, and USM at DHS Headquarters to again inquire as to whether these offices might have responsive documents. DHS Privacy also contacted NPPD again, at which point, the NPPD FOIA Office realized that there was confusion about the nature of EPIC's request. The NPPD FOIA Office realized that NPPD would have one or possibly more records responsive to the EPIC request. NPPD conducted a search and quickly identified, in the files of the NCC, the only document that is responsive to the request. Specifically, NPPD consulted with the NCC because the NCC is the author of the SOP and implements the SOP. According to the NCC, there are no other documents that contain either the full text of the questions or any executing protocols or guidelines.

20. SOP 303 was drafted by the NCC and approved by CS&C on March 17, 2006. It has been periodically updated so that names and contact information contained therein remains current. The

SOP was compiled for a law enforcement purpose, which includes activities related to national security and homeland security. It was inspired by the Letter to the President on Emergency Wireless Protocol and Recommendations, dated March 1, 2006, and generated by the National Security Telecommunications Advisory Committee (NSTAC), an industry-led Presidential advisory committee established by Executive Order 12382. In the aftermath of the 2005 bombings in the London transportation system, the NSTAC perceived 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. Consistent with the NSTAC's recommendation, the NCC developed SOP 303 as a unified voluntary process for the orderly shut-down and restoration of wireless services during critical emergencies such as the threat of radio-activated improvised explosive devices. The SOP establishes a procedure by which state homeland security officials can directly engage with wireless carriers, and it establishes factual authentication procedures for decision-makers.

21. Included as part of SOP 303 itself are the two other categories of records that EPIC seeks, *i.e.*, the full text of the pre-determined series of questions that determines if a shutdown is necessary, and the executing protocols related to the implementation of SOP 303. Again, DHS Privacy, in conjunction with the NCC, determined that the SOP is the only responsive document because there are no other

documents that contain the full text of the questions or any executing protocols.

22. Portions of the SOP are being withheld pursuant to FOIA Exemptions b(6), b(7)(c), b(7)(e), and b(7)(f), as the SOP contains security procedures and related information regarding the shutdown of cell phone service during various types of homeland security incidents, and personal information about certain law enforcement officials. After a review for segregability, NPPD FOIA Office determined that some information in the SOP could be released without compromising law enforcement or privacy objectives. DHS Privacy agrees with the assessment.

23. FOIA Exemption b(6) protects from disclosure information about individuals when the disclosure of the information "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552 (b)(6). DHS applied the b(6) exemption to protect the names, direct dial telephone numbers, and email addresses for state homeland security officials who have an expectation of privacy. The redacted information does not directly shed light on the operations or activities of the government. The release of this information would constitute an unwarranted invasion of personal privacy, possibly subject the persons to harassment by the public and inquiries by the media, and potentially facilitate targeting of these officials by bad actors.

24. FOIA Exemption b(7)(c) permits the withholding of personal information in law enforcement records. DHS applied the b(7)(c) exemption to protect the names, direct-dial telephone numbers and e-mail addresses of high-ranking officials within each state's homeland security agency. The release of this information would not

shed lights on the agency's operations or activities and would constitute an unwarranted invasion of personal privacy, possibly subject the persons to harassment by the public and inquiries by the media, and potentially facilitate targeting of these officials by bad actors.

25. FOIA Exemption b(7)(e) permits the withholding of law enforcement information that "would disclose techniques and procedures for law enforcement investigations." The b(7)(e) exemption applies because the requested document contains a homeland security procedure primarily intended to efficiently and effectively deter the triggering of radio-activated improvised explosive devices. During the course of incidents involving the potential for improvised explosive devices to be dispersed over a wide geographic area, orderly deactivation of wireless networks may be the best option for preventing and/or mitigating explosions that would endanger life and property. SOP 303 establishes a protocol for verifying that circumstances exist that would justify shutting down wireless networks. It also ensures that decision makers consider potential public safety hazards when deciding whether to shut-down a wireless network, such as the inability of first-responders and the public to use wireless phones for calls, including 911 calls. In addition, SOP 303 provides a step-by-step process for the orderly shut-down of wireless networks following verification of the facts and appropriate weighing of the circumstances. Finally, SOP 303 coordinates orderly resumption of wireless service. Making SOP 303 public would enable bad actors to circumvent or interfere with a law enforcement strategy designed to prevent activation of improvised explosive devices by

providing information about when shutdown procedures are used and how a shutdown is executed.

26. FOIA Exemption b(7)(F) permits the withholding of records necessary to protect the physical safety of "any individual." Making SOP 303 public would, e.g., enable bad actors to insert themselves into the process of shutting down or reactivating wireless networks by appropriating verification methods and then impersonating officials designated for involvement in the verification process. The aim of such bad actors would be to disable the protocol so that they could freely use wireless networks to activate the improvised explosive devices. Given that disclosure of the requested information could reasonably lead to circumvention of or interference with a procedure aimed at preventing the triggering of improvised explosive devices, there is a reasonable expectation that disclosure could reasonably endanger individuals' lives or physical safety.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 28th day of June, 2013.

_____

James V.M.L. Holzer

APPENDIX E

5 U.S.C. § 552(b) provides that:

Public information; agency rules, opinions, orders, records, and proceedings

(a) Each agency shall make available to the public information as follows:

* * *

(3)

(A) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, and except as provided in subparagraph (E), each agency, upon any request for records which

(i) reasonably describes such records and

(ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

* * *

(b) This section does not apply to matters that are—

* * *

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information

* * *

(F) could reasonably be expected to endanger the life or physical safety of any individual;