Exemption 7(E)

Exemption 7(E) of the Freedom of Information Act affords protection to law enforcement information that "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law."[1]

Techniques and Procedures

The first clause of Exemption 7(E) protects "techniques and procedures for law enforcement investigations or prosecutions."[2] The phrase "techniques and procedures" refers to the means by which agencies conduct investigations.[3] Specifically, a "technique" is "'a technical method of accomplishing a desired aim'" and a "procedure" is "'a particular way of doing or of going about the accomplishment of something'" in the context of a law enforcement investigation or prosecution.[4]

---

[1] 5 U.S.C. § 552(b)(7)(E) (2018).

[2] 5 U.S.C. § 552(b)(7)(E) (2018); see Mayer Brown LLP v. IRS, 562 F.3d 1190, 1192-93 (D.C. Cir. 2009) (discussing meaning of phrase "could reasonably be expected to risk circumvention of the law" found in second clause of Exemption 7(E)).

[3] See Allard K. Lowenstein Int'l Hum. Rts. Project v. DHS, 626 F.3d 678, 682 (2d Cir. 2010) [hereinafter Lowenstein II] (noting as example if investigators are given instructions on manner in which to investigate those suspected of tax evasion, such details constitute techniques and procedures); see also Fams. for Freedom v. U.S. Customs & Border Prot., 837 F. Supp. 2d 287, 296-97 (S.D.N.Y. 2011) [hereinafter Fams. for Freedom II] (relying on definition set forth in Allard to state that techniques and procedures constitute how, where, and when law enforcement methods are carried out, while policy and budgetary decisions about law enforcement staffing patterns arguably constitute "guidelines" under Exemption 7(E)).

[4] Lowenstein II, 626 F.3d at 682 (quoting Webster's Third New International Dictionary (1986)).

Exemption 7(E) has been found to authorize the withholding of law enforcement "techniques" or law enforcement "procedures," whenever they are used "for law enforcement investigations or prosecutions," both civil and criminal.[5]

Historically, courts have reached differing conclusions as to whether a showing that disclosure could risk circumvention of the law is required to satisfy the first clause of Exemption 7(E).[6] Some courts have required a showing of circumvention of the law to withhold techniques and procedures under the first clause,[7] while other courts have

---

[5] See Elec. Priv. Info. Ctr. v. U.S. Customs & Border Prot., No. 17-5058, 2017 WL 4220339, at *1 (D.C. Cir. Aug. 1, 2017) (per curiam) (holding that Exemption 7(E)'s scope "is not limited to records the release of which would disclose techniques, procedures or guidelines for *criminal* law enforcement investigations or prosecutions"); Gordon v. FBI, 388 F. Supp. 2d 1028, 1036 (N.D. Cal. 2005) (rejecting plaintiff's "narrow[]" reading of the "law enforcement purpose" requirement of Exemption 7(E), and noting that it "is not limited to documents created in connection with a criminal investigation"); cf. Cozen v. U.S. Dep't of Treasury, 570 F. Supp. 2d 749, 782 (E.D. Pa. 2008) (noting that in context of Exemption 7, protection for "law enforcement" records or information "is not limited to documents involving criminal proceedings").

[6] See Associated Press v. FBI, 265 F. Supp. 3d 82, 99 (D.D.C. 2017) (noting that courts are divided on whether circumvention requirement applies to law enforcement techniques and procedures); Citizens for Resp. & Ethics in Wash. v. DOJ, 160 F. Supp. 3d 226, 241-42 (D.D.C. 2016) ("There is some disagreement in the courts as to the proper reading of Exemption 7(E).").

[7] See, e.g., Garza v. U.S. Marshals Serv., No. 18-5311, 2020 WL 768221, at *1 (D.C. Cir. Jan. 22, 2020) (per curiam) (unpublished disposition) (approving invocation of Exemption 7(E) to protect information concerning the effectiveness of investigative techniques and internal filing codes because public disclosure "might increase the risk that a law will be violated or that past violators will escape legal consequences"); Blackwell v. FBI, 646 F.3d 37, 42 (D.C. Cir. 2011) (applying, without analysis, "risk of circumvention" standard to law enforcement techniques and procedures); Catledge v. Mueller, 323 F. App'x 464, 466-67 (7th Cir. 2009) (requiring showing of risk of circumvention for techniques and procedures); Davin v. DOJ, 60 F.3d 1043, 1064 (3d Cir. 1995) (declaring that "Exemption 7(E) applies to law enforcement records which, if disclosed, would risk circumvention of the law"); PHE, Inc. v. DOJ, 983 F.2d 248, 250 (D.C. Cir. 1993) (stating that under Exemption 7(E), agency "must establish that releasing the withheld materials would risk circumvention of the law"); Elec. Frontier Found. v. DOD, No. 09-05640, 2012 WL 4364532, at *3 (N.D. Cal. Sept. 24, 2012) (requiring that agency satisfy "risk of circumvention" standard without distinguishing between first and second prongs of Exemption 7(E)); Bloomer v. DHS, 870 F. Supp. 2d 358, 369 (D. Vt. 2012) (applying "risk of circumvention" standard to "'internal instructions, codes, and guidance [that] would reveal both a law enforcement technique and an internal investigative practice'") (quoting agency declaration); Muslim Advocs. v. DOJ, 833 F. Supp. 2d 106, 109 (D.D.C. 2012) [hereinafter Muslim Advocs. II] (citing prior case in which court required circumvention showing under first clause of Exemption 7(E), and finding that agency made adequate showing of circumvention harm for certain techniques and

applied a circumvention standard without clarifying which clause of Exemption 7(E) was being applied,[8] and yet other courts have not required any circumvention showing under Exemption 7(E)'s first clause.[9] However, the FOIA Improvement Act of 2016 codified a

---

procedures); Riser v. U.S. Dep't of State, No. 09-3273, 2010 WL 4284925, at *5 (S.D. Tex. Oct. 22, 2010) (holding that "risk of circumvention" analysis must be applied to withholdings of law enforcement techniques and procedures); Council on Am.-Islamic Rels., Cal. v. FBI, 749 F. Supp. 2d 1104, 1123 (S.D. Cal. 2010) (stating that agency can withhold techniques or guidelines whose release could risk circumvention of law); Unidad Latina En Accion v. DHS, 253 F.R.D. 44, 49 (D. Conn. 2008) (stating that for Exemption 7(E) to apply, court must find disclosure "could reasonably be expected to risk circumvention of the law").

[8] See, e.g., Frank LLP v. Consumer Fin. Prot. Bureau, 327 F. Supp. 3d 179, 185 (D.D.C. 2018) (endorsing protection of methods of questioning individuals because agency demonstrated "a risk of circumvention, whether it was required to or not"); Hasbrouck v. U.S. Customs & Border Prot., No. 10-3793, 2012 WL 177563, at *3-4 (N.D. Cal. Jan. 23, 2012) (allowing withholding of certain identifiers used to retrieve personal information from law enforcement databases due to government's showing of plausible circumvention harms, but failing to identify whether first or second clause of Exemption 7(E) was at issue); Kortlander v. BLM, 816 F. Supp. 2d 1001, 1014 (D. Mont. 2011) (endorsing withholding of records regarding techniques and procedures associated with undercover operations because disclosure could allow criminals to circumvent such efforts and because such techniques are unknown to public); Skinner v. DOJ, 744 F. Supp. 2d 185, 214 (D.D.C. 2010) [hereinafter Skinner I] (recognizing cases that allowed withholding of law enforcement techniques or procedures where disclosure could lead to circumvention of the law).

[9] See, e.g., Hamdan v. DOJ, 797 F.3d 759, 778 (9th Cir. 2015) (finding agency need not show risk of circumvention as to disclosure of law enforcement techniques); Lowenstein II, 626 F.3d at 681-82 (finding "no ambiguity" in Exemption 7(E)'s application of risk of circumvention standard to "guidelines" prong, but not "techniques and procedures" prong of Exemption 7(E)); ACLU of Mich. v. FBI, No. 11-13154, 2012 WL 4513626, at *9 (E.D. Mich. Sept. 30, 2012) (holding that no showing of harm is required to withhold law enforcement "techniques and procedures"), aff'd, 734 F.3d 460 (6th Cir. 2013); McRae v. DOJ, 869 F. Supp. 2d 151, 168 (D.D.C. 2012) (contrasting "techniques and procedures" prong of Exemption 7(E), which provides "categorical" protection, to "guidelines" prong of Exemption 7(E), which requires showing of risk of circumvention); Fams. for Freedom II, 837 F. Supp. 2d 287, 296-97 (S.D.N.Y. 2011) (noting that because certain information at issue constituted techniques and procedures rather than guidelines, any circumvention risks were irrelevant under FOIA); Jordan v. DOJ, No. 07-2303, 2009 WL 2913223, at *16 (D. Colo. Sept. 8, 2009) (adopting magistrate's recommendation) ("The court is not required to make any particular finding of harm or circumvention of the law when evaluating applications of Exemption 7(E) involving law enforcement techniques."), aff'd, 668 F.3d 1188 (10th Cir. 2011); cf. ACLU of Mich., 2012 WL 4513626, at *9 (finding that law enforcement techniques and procedures receive "categorical protection" from disclosure if such techniques and procedures are not well known to public); McRae, 869 F. Supp. 2d at 168 (applying "categorical" protection for law enforcement techniques and procedures); Citizens for Resp. & Ethics in Wash. v. DOJ, 870 F. Supp. 2d 70, 85 (D.D.C. 2012) (declaring that "longstanding precedent" supports categorical protection for law enforcement techniques and procedures), rev'd and remanded on other grounds, 746 F.3d 1082, 1102

"foreseeable harm" standard which requires that an agency shall withhold information under the FOIA only if "the agency reasonably foresees that disclosure would harm an interest protected by an exemption" or if "disclosure is prohibited by law."[10] As to the showing of harm that must be made, the D.C. Circuit has stated on multiple occasions that the FOIA sets a "relatively low bar" for withholding under this exemption.[11]

For the first clause of Exemption 7(E) to apply, courts uniformly require that the technique or procedure at issue ordinarily must not be well known to the public.[12]

(D.C. Cir. 2014) (finding that agency did not provide sufficient detail to determine if records fell into Ex. 7(E)); Skinner v. DOJ, 806 F. Supp. 2d 105, 116 (D.D.C. 2011) [hereinafter Skinner II] (declaring that "[l]aw enforcement procedures and techniques are afforded categorical protection under Exemption 7(E)").

[10] 5 U.S.C. § 552(a)(8)(A) (2018).

[11] Blackwell, 646 F.3d at 42 (noting that "'[r]ather than requiring a highly specific burden of showing how the law will be circumvented, [E]xemption 7(E) only requires that the [agency] demonstrate logically how the release of the requested information might create a risk of circumvention of the law'") (quoting Mayer Brown LLP v. IRS, 562 F.3d 1190, 1194 (D.C. Cir. 2009)); accord Skinner v. DOJ, 893 F. Supp. 2d 109, 114 (D.D.C. 2012) [hereinafter Skinner III] (noting that D.C. Circuit precedent sets a "'low bar'" for withholding under Exemption 7(E)) (quoting Blackwell, 646 F.3d at 42), aff'd sub nom. per curiam, Skinner v. ATF, No. 12-5319, 2013 WL 3367431 (D.C. Cir. May 31, 2013); see also Mayer Brown, 562 F.3d at 1194 (observing that while FOIA requires exemptions to be construed narrowly, Exemption 7(E) constitutes "broad language").

[12] See ACLU of N. Cal. v. DOJ, 880 F.3d 473, 492 (9th Cir. 2018) (finding that agency cannot withhold portions of manual on surveillance techniques for federal prosecutors because they describe investigative techniques known to public generally); Schwartz v. DEA, 692 F. App'x. 73, 74 (2d Cir. 2017) (affirming district court decision that techniques and procedures possibly revealed by video of a drug interdiction operation are known to public and cannot be withheld); Rugiero v. DOJ, 257 F.3d 534, 551 (6th Cir. 2001) (stating that first clause of Exemption 7(E) "protects [only] techniques and procedures not already well-known to the public"); Davin, 60 F.3d at 1064 (holding that "[t]his exemption . . . may not be asserted to withhold 'routine techniques and procedures already well known to the public'") (quoting Ferri v. Bell, 645 F.2d 1213, 1224 (3d Cir. 1981)); Rosenfeld v. DOJ, 57 F.3d 803, 815 (9th Cir. 1995) (establishing rule within that circuit that law enforcement techniques must not be well known to public); Founding Church of Scientology of D.C. v. NSA, 610 F.2d 824, 832 n.67 (D.C. Cir. 1979) (finding that Exemption 7(E) does not ordinarily protect "routine techniques and procedures already well known to the public"); ACLU Found. v. DOJ, 418 F. Supp. 3d 466, 480 (N.D. Cal. 2019) (declining to support the FBI's 7(E) Glomar response because "disclosure of social media surveillance – a well-known general technique –would not reveal the *specific means* of surveillance"); Elec. Frontier Found. v. DOJ, No. 17-1039, 2019 WL 1714433, at * 3 (D.D.C. Apr. 17, 2019) (same) (quoting Founding Church of Scientology of D.C., 610 F.2d at 832); Dutton v. DOJ, 302 F. Supp. 3d 109, 125 (D.D.C. 2018) (finding agency properly invoked 7(E) to protect information revealing the "specific use of an investigative step" that is not publicly known and could hinder law enforcement investigations if made public); ACLU of Mich., 2012 WL 4513626,

Accordingly, techniques such as "wiretaps,"[13] the "use of post office boxes,"[14] pretext telephone calls,[15] and "planting transponders on aircraft suspected of smuggling"[16] have been denied protection under Exemption 7(E) when courts have found them to be generally known to the public. Courts have also found Exemption 7(E) inapplicable when the information could not fairly be characterized as describing "techniques or procedures."[17]

---

at *9 (noting that categorical withholding is only permissible for unknown techniques and procedures); Kubik v. BOP, No. 10-6078, 2011 WL 2619538, at *11 (D. Or. July 1, 2011) (finding that tactics used by BOP personnel during prison riot cannot be withheld because they are known to inmates who were present during riot); Unidad Latina En Accion, 253 F.R.D. at 51-52 (finding that "the details, scope and timing" of surveillance techniques such as target apprehension charts are "not necessarily well-known to the public" and thus are properly withheld).

[13] Billington v. DOJ, 69 F. Supp. 2d 128, 140 (D.D.C. 1999) (noting that "commonly known law enforcement practices, such as wiretaps . . . are generally not shielded"), vacated on other grounds, 233 F.3d 581 (D.C. Cir. 2000); Pub. Emps. for Env't Resp. v. EPA, 978 F. Supp. 955, 963 (D. Colo. 1997) (noting that "[i]nterception of wire, oral, and electronic communications are commonly known methods of law enforcement"), appeal dismissed voluntarily, No. 97-1384 (10th Cir. Nov. 25, 1997).

[14] See Billington, 69 F. Supp. 2d at 140 (observing as general matter that "use of post office boxes" is "commonly known" for purposes of Exemption 7(E)).

[15] See Rosenfeld, 57 F.3d at 815 (rejecting agency's attempt to protect existence of pretext telephone calls because this technique is generally known to public); see also Campbell v. DOJ, No. 89-3016, 1996 WL 554511, at *10 (D.D.C. Sept. 19, 1996) (ordering disclosure of information pertaining to various "pretexts" because information is known to public, requested records do not describe details of techniques, and disclosure would not undermine techniques' effectiveness), rev'd on other grounds, 164 F.3d 20 (D.C. Cir. 1998); Struth v. FBI, 673 F. Supp. 949, 970 (E.D. Wis. 1987) (dismissing pretext as merely "garden variety ruse or misrepresentation").

[16] Hamilton v. Weise, No. 95-1161, 1997 U.S. Dist. LEXIS 18900, at *30-31 (M.D. Fla. Oct. 1, 1997).

[17] See Ibrahim v. U.S. Dep't of State, 311 F. Supp. 3d 134, 144 (D.D.C. 2018) (ordering release of agency's assessment of request for reconsideration of refugee resettlement application because it does not disclose law enforcement techniques); ACLU of Ariz. v. DHS Sec. Off. for C.R. & C.L., No. 15-00247, 2017 WL 3478658, at *14 (D. Ariz. Aug. 14, 2017) (unpublished disposition) (ordering release of "case numbers assigned to allegations of mistreatment of minors" because they do not reveal law enforcement techniques or procedures); ACLU v. DHS, 243 F. Supp. 3d 393, 403-05 (S.D.N.Y. 2017) (finding that questions asked of alien juveniles suspected of smuggling did not constitute "a specialized, calculated technique"); ACLU of Wash. v. DOJ, No. 09-0642, 2012 U.S. Dist. LEXIS 137204, at *17-19 (W.D. Wash. Sept. 21, 2012) (ordering release of characteristics of individuals suspected of illegal activity as well as internal agency telephone number associated with Terrorist Watch List because such information does not constitute law enforcement

However, even records pertaining to commonly known procedures have been protected from disclosure when the circumstances of their usefulness are not widely

techniques or procedures, regardless of harm associated with releasing such information). Compare Shapiro v. DOJ, 153 F. Supp. 3d 253, 272-73 (D.D.C. 2016) (holding that agency cannot categorically withhold search slips associated with all FOIA requests within past twenty-five years because they do not reveal law enforcement techniques, procedures, or guidelines), with Shapiro v. DOJ, 239 F. Supp. 3d 100, 111-16 (D.D.C. 2017) [hereinafter Shapiro I] (holding that FOIA request search slips created within past twenty-five years for which agency had issued "no records" responses to underlying FOIA request are protectable under 7(E) as "part of a complex mosaic related to ongoing FBI operations, involving one of the FBI's domestic terrorism priorities").

known,[18] or their use in combination with other factors would compromise the underlying techniques or procedures."[19]

---

[18] See, e.g., Broward Bulldog, Inc. v. DOJ, 939 F.3d 1164, 1191 (11th Cir. 2019) (noting that "even for well-known techniques or procedures, Exemption 7(E) protects information that would reveal facts about such techniques or their usefulness that are not generally known to the public, as well as other information when disclosure could reduce the effectiveness of such techniques"); Shapiro v. DOJ, 893 F.3d 796, 800-01 (D.C. Cir. 2018) [hereinafter Shapiro II] (affirming application of Exemption 7(E) to records generated from commercially-available database because details of agency's methods of searching and managing database "are not generally known"); Hamdan v. DOJ, 797 F.3d 759, 777-78 (9th Cir. 2015) (concluding that agency properly withheld records that would reveal "a specific *means* of conducting surveillance and credit searches rather than an application" of these publicly known techniques); Schwartz v. DEA, No. 13-5004, 2016 WL 154089, at *35 (E.D.N.Y Jan. 8, 2016) (unpublished disposition) (clarifying that "circumstances concerning the application of a technique are protectable where they reveal previously unknown techniques or previously unknown aspects of known techniques"); ACLU of Mich. v. FBI, No. 11-13154, 2012 WL 4513626, at *11 (E.D. Mich. Sept. 30, 2012) (finding that public's knowledge of some aspects of technique or procedure "not dispositive" where manner and circumstances of use not publicly known); Elec. Frontier Found. v. DOD, No. 09-05640, 2012 WL 4364532, at *5 (N.D. Cal. Sept. 24, 2012) (rejecting plaintiff's argument that agency could not withhold details of agency's known use of social networking websites to conduct investigations because withheld details were not known to public); Vazquez v. DOJ, 887 F. Supp. 2d 114, 117-18 (D.D.C. 2012) (noting that while public is generally aware of FBI's National Crime Information Center databases, details of their use and whether individuals are mentioned in them is not known to public), aff'd per curiam, No. 13-5197, 2013 WL 6818207 (D.C. Cir. Dec. 18, 2013); Muslim Advocs. v. DOJ, 833 F. Supp. 2d 92, 104-05 (D.D.C. 2011) [hereinafter Muslim Advocs. I] (finding that while certain aspects of law enforcement techniques at issue are publicly known, because circumstances under which such techniques may be used are non-public, withholding of such information is permissible); Kubik v. BOP, No. 10-6078, 2011 U.S. Dist. LEXIS 71300, at *33 (D. Or. July 1, 2011) (agreeing that withholding is justified where identity of technique is known but circumstances of use of technique is unknown); Skinner I, 744 F. Supp. 2d 185, 215 (D.D.C. 2010) (protecting portion of document specifying which of several publicly-known law enforcement techniques were used in particular investigation and FBI's numerical rating of effectiveness of such techniques because future targets could modify their illicit activities to circumvent such techniques); Jordan v. DOJ, No. 07-2303, 2009 WL 2913223, at *15-16 (D. Colo. Sept. 8, 2009) (protecting photocopied inmate correspondence to protect details of BOP's well-known inmate mail-monitoring technique, endorsing protection of specific application of known technique where release could diminish effectiveness of such technique); Barnard v. DHS, 598 F. Supp. 2d 1, 23 (D.D.C. 2009) (recognizing that "[t]here is no principle . . . that requires an agency to release all details [of] techniques simply because some aspects are known to the public"); Buffalo Evening News, Inc. v. U.S. Border Patrol, 791 F. Supp. 386, 392 n.5, 393 n.6 (W.D.N.Y. 1992) (finding that Exemption 7(E) protects fact of whether alien's name is listed in INS Lookout Book and method of apprehension of alien).

[19] See, e.g., Citizens for Resp. & Ethics in Wash. v. DHS, No. 20-1400, 2021 WL 950415, at *5-6 (D.D.C. Mar. 12, 2021) (approving use of "the mosaic theory" to withhold number of

Moreover, courts have endorsed the withholding of the details of a wide variety of commonly known procedures – for example, polygraph examinations,[20] undercover

---

Secret Service personnel on protective trip because disclosure would provide "'one piece of information that could be combined with others to better understand [the Secret Service's] protective methods and their strengths and weaknesses'") (quoting agency declaration); Whittaker v. DOJ, No. 18-01434, 2020 WL 6075681, at *5-6 (D.D.C. Oct. 15, 2020) (protecting name check search results from a background investigation because disclosure of an individual name check result, though it may seem innocuous, could be pieced together with other name check results enabling inferences to be drawn from those results to the point where a "picture can start to form about how the FBI uses its resources"); Reporters Comm. for Freedom of the Press v. FBI, No. 15-1392, 2020 WL 1324397 , at *11 (D.D.C. Mar. 20, 2020) ("While any one piece of information might not compromise the FBI's techniques or procedures, 'pieces of information can be assembled – in mosaic fashion – to provide a framework to determine how, when, under which circumstances, certain te[ch]niques are employed.'") (quoting agency declaration); Shapiro v. DOJ, 393 F. Supp. 3d 111, 121 (D.D.C. 2019) (approving protection of database name because disclosure would "forever associate the database name to the information" contained in a specific serial that the FBI has not withheld, including the "type of information stored in the database and the type of investigation in which the database is referenced" thereby increasing the risk that a terrorist armed with this information could "predict FBI investigative strategies and enhance [their] ability to avoid detection by the FBI); Asian L. Caucus v. DHS, No. 08-00842, 2008 WL 5047839, at *4 (N.D. Cal. Nov. 24, 2008) (approving protection of database names that relate to watch lists, noting that watch lists may be common knowledge but disclosure of related database names "could . . . facilitate improper access to the database"); Gordon v. FBI, 388 F. Supp. 2d 1028, 1035-36 (N.D. Cal. 2005) (protecting details of agency's aviation "watch list" program, including records detailing "selection criteria" for watch lists and handling and dissemination of lists, and "addressing perceived problems in security measures"); cf. Elec. Priv. Info. Ctr. v. DOJ, 490 F. Supp. 3d 246, 268 (D.D.C. 2020) (protecting non-public information regarding Special Counsel's investigation including investigative focus and strategies and gathering and/or analysis of information, which directly implicate investigative targets, dates, and scope of investigatory operations, and noting that "although the redacted information itself may not constitute a technique, procedure, or guideline, with the disclosure of such information 'comes the knowledge of how the agency employs its procedures or techniques' . . . .") (quoting Elec. Priv. Info. Ctr. v. DEA, 401 F. Supp. 3d 37, 46-47 (D.D.C. 2019)).

[20] See, e.g., Sack v. DOD, 823 F.3d 687, 694-95 (D.C. Cir. 2016) (concluding that release of reports concerning polygraphs could undermine effectiveness of such examinations); Frankenberry v. FBI, 567 F. App'x 120, 124-25 (3d Cir. 2014) (affirming withholding of polygraph procedures that are unknown to public because disclosure could encourage circumvention of law); Hale v. DOJ, 973 F.2d 894, 902-03 (10th Cir. 1992) (concluding that disclosure of "polygraph matters" could hamper their effectiveness), cert. granted, vacated & remanded on other grounds, 509 U.S. 918 (1993); Schneider v. DOJ, 498 F. Supp. 3d 121, 129-30 (D.D.C. 2020) (affirming withholding of information concerning polygraph programs and techniques used to assess the suitability of job applicants and current employees because public disclosure could enable "future applicants and those with intent to harm the government [to] tailor their responses during polygraph sessions and screening

interviews to circumvent security procedures"); Piper v. DOJ, 294 F. Supp. 2d 16, 30 (D.D.C. 2003) (declaring that polygraph materials were properly withheld because release would reveal sensitive "logistical considerations").

operations,[21] surveillance techniques,[22] and bank security measures[23] – because disclosure could reduce or even nullify the effectiveness of such procedures.[24] As one

---

[21] See, e.g., Djenasevic v. EOUSA, 319 F. Supp. 3d 474, 490 (D.D.C. 2018) (finding that portions of undercover operations manual are withholdable because release would allow criminals to restructure activities to circumvent law); Brown v. FBI, 873 F. Supp. 2d 388, 407-08 (D.D.C. 2012) (withholding Vehicle Identification Numbers of vehicles used in undercover operations because criminals could determine which vehicles were being used by law enforcement agents); Kortlander v. BLM, 816 F. Supp. 2d 1001, 1014 (D. Mont. 2011) (protecting means by which law enforcement "plans and executes undercover operations" because disclosure could allow wrongdoers to plan criminal activities to evade detection); Sinito v. DOJ, No. 87-0814, 2000 WL 36691372, at *14 (D.D.C. July 12, 2000) (holding that disclosure of information about "electronic recording device" (body microphone) "would impair the FBI's ability to conduct future investigations"), summary affirmance granted, 22 F. App'x 1 (D.C. Cir. 2001); Foster v. DOJ, 933 F. Supp. 687, 693 (E.D. Mich. 1996) (holding that release of techniques and guidelines used in undercover operations would diminish effectiveness).

[22] See, e.g., Buzzfeed, Inc. v. DOJ, 344 F. Supp. 3d 396, 407 (D.D.C. 2018) (holding that "public awareness that the FBI uses airplanes, or even, press speculation that certain planes are FBI planes, is not the same as, and does not give rise to the same risk as, the FBI's own confirmation of its use of specific aircraft"); Soghoian v. DOJ, 885 F. Supp. 2d 62, 75 (D.D.C. 2012) (protecting electronic surveillance techniques because release of information showing what information is collected during surveillance, how it is collected, and when it is not collected could allow criminals to evade detection); Lewis-Bey v. DOJ, 595 F. Supp. 2d 120, 138 (D.D.C. 2009) (protecting details of electronic surveillance techniques, including "'circumstances . . . timing of their use, and the specific location where they were employed'") (quoting agency's declaration); Shores v. FBI, 185 F. Supp. 2d 77, 85 (D.D.C. 2002) (protecting details of surveillance operations at federal prison, including information about telephone system).

[23] See, e.g., Ford v. DOJ, 208 F. Supp. 3d 237, 254 (D.D.C. 2016) (finding that "[e]ven if some cameras are 'visible' as a deterrent, other cameras may be placed at angles or in areas unknown to the public and disclosure of this information could, as the FBI points out, 'provide criminals the necessary information to circumvent the very purpose of a bank surveillance system, making banks more vulnerable to bank robberies and/or other criminal activity, and therefore circumvent the law'"); Maguire v. Mawn, No. 02-2164, 2004 WL 1124673, at *3 (S.D.N.Y. May 19, 2004) (protecting details of bank's use of "bait money" even though technique is publicly known because "disclosure . . . could reasonably make the [b]ank more susceptible to robberies in the future"); Dayton Newspapers, Inc. v. FBI, No. 3-85-815, 1993 WL 1367435, at *6 (S.D. Ohio Feb. 9, 1993) (concluding that agency properly withheld details of bank security devices and equipment used in bank robbery investigation).

[24] See, e.g., Hale, 973 F.2d at 902-03 (concluding that disclosure of use of security devices and their modus operandi could lessen their effectiveness); Bowen v. FDA, 925 F.2d 1225, 1229 (9th Cir. 1991) (deciding that release of specifics of cyanide-tracing techniques would present serious threat to future product-tampering investigations); Frank LLP v. Consumer Fin. Prot. Bureau, 327 F. Supp. 3d 179, 185 (D.D.C. 2018) (concluding that disclosure of

court observed, this is especially true "when the method employed is meant to operate clandestinely, unlike [other techniques] that serve their crime-prevention purpose by operating in the open."[25] In this regard, the use of a "Glomar response"[26] under Exemption 7(E), i.e., where the agency neither confirms nor denies the existence of the requested records, has been approved by the courts when disclosing the abstract fact that a particular law enforcement technique was employed would reveal the circumstances under which that technique was used.[27]

---

methods of questioning would allow entities "'to coach future witnesses in similar cases on how to avoid providing incriminating information'" which would thwart future use) (quoting agency's declaration); McGehee v. DOJ, 800 F. Supp. 2d 220, 236-37 (D.D.C. 2011) (finding that Exemption 7(E) does not require that techniques be unknown to public where release of non-public details of such techniques would allow circumvention of techniques); Cal-Trim, Inc. v. IRS, 484 F. Supp. 2d 1021, 1027 (D. Ariz. 2007) (protecting records related to agency investigation because release could allow individuals under investigation "to craft explanations or defenses based on the [IRS] agent's analysis or enable them the opportunity to disguise or conceal the transactions that are under investigation"); Leveto v. IRS, No. 98-285, 2001 U.S. Dist. LEXIS 5791, at *21 (W.D. Pa. Apr. 10, 2001) (protecting dollar amount budgeted for agency to investigate particular individual because release could allow others to learn agency's monetary limits and undermine such investigations in future).

[25] Maguire, 2004 WL 1124673, at *3.

[26] See Phillippi v. CIA, 546 F.2d 1009, 1013 (D.C. Cir. 1976) (approving agency's response where it would "neither confirm nor deny" the existence of responsive records) (origin of term "Glomar response").

[27] See Platsky v. NSA, 547 F. App'x 81, 82 (2d Cir. 2013) (affirming agency's Exemption 7(E) Glomar response in neither confirming nor denying requester's placement on government watchlist); Catledge v. Mueller, 323 F. App'x 464, 467 (7th Cir. 2009) (affirming agency's refusal to confirm or deny existence of National Security Letters pertaining to requester); Braun v. FBI, No. 18-2145, 2019 WL 3343948, at *5 (D.D.C. July 25, 2019) (affirming refusal to confirm or deny whether a requester is on any watch list because public disclosure would risk "giving away information that might tip off those on the watch list or aid those who seek to avoid being placed on it"); Buzzfeed, Inc., 344 F. Supp. 3d at 406-07 (holding that agency properly refused to confirm or deny use of a specific aircraft under its aerial surveillance program); Myrick v. Johnson, 199 F. Supp. 3d 120, 124-25 (D.D.C. 2016) (concluding that agency's response in neither confirming nor denying particular undercover operation is appropriate because acknowledging its existence would risk circumvention); Vazquez v. DOJ, 887 F. Supp. 2d 114, 117-18 (D.D.C. 2012) (affirming agency's use of Exemption 7(E) Glomar because public confirmation of whether or not individual is listed in one of FBI's National Crime Information Center databases would cause harm meant to be protected by Exemption 7(E)); El Badrawi v. DHS, 596 F. Supp. 2d 389, 396 (D. Conn. 2009) (concluding agency "properly asserted a Glomar response" where "confirming or denying that [an individual] is a subject of interest . . . would cause the very harm FOIA Exemption[] . . . 7(E) [is] designed to prevent"); cf. Amadis v. DOJ, 388 F. Supp. 3d 1, 7 (D.D.C. 2019) (holding agency properly applied Exemption 7(E) to protect records related to its search that produced a "No Records" / Glomar response because "requesters put the FBI in an untenable position when they seek search slips and [FOIPA Document Processing

Courts have construed Exemption 7(E) to encompass the withholding of a wide range of techniques and procedures, including immigration enforcement techniques,[28] information regarding certain databases used for law enforcement purposes,[29]

System (FDPS)] case notes about such responses . . ."); Shapiro I, 239 F. Supp. 3d 100, 111-16 (D.D.C. 2017) (finding that FOIA request search slips created within past twenty-five years for which agency had issued "no records" responses to underlying FOIA request are withholdable because they could serve to confirm "the existence or non-existence of an investigation" and that "might assist those seeking to evade detection").

[28] Lowenstein II, 626 F.3d 678, 680-82 (2d Cir. 2010) (finding that criteria used to rank priority of immigration enforcement cases constitutes techniques and procedures rather than guidelines; further finding that law does not require showing of circumvention of law for such techniques and procedures); Ibrahim v. U.S. Dep't of State, 311 F. Supp. 3d 134, 143 (D.D.C. 2018) (finding that Exemption 7(E) applies to lines of questioning in Refugee Application Assessment because disclosure could enable applicants to strategically plan inaccurate responses); Ahmed v. U.S. Citizenship & Immigr. Serv., No. 11-6230, 2013 WL 27697, at *4-5 (E.D.N.Y. Jan. 2, 2013) (protecting techniques for vetting of naturalization applicants who might pose national security concerns); Fams. for Freedom II, 837 F. Supp. 2d 287, 296-97 (S.D.N.Y. 2011) (withholding operational details of train inspections made by Border Patrol agents); Tran v. DOJ, No. 01-0238, 2001 WL 1692570, at *3 (D.D.C. Nov. 20, 2001) (concluding that agency form – used when agencies share information from immigration records – was properly withheld because it would reveal law enforcement techniques).

[29] See, e.g., Shapiro II, 893 F.3d 796, 800-01 (D.C. Cir. 2018) (protecting records generated by commercially-available database because release would reveal how agency uses database and results it considers meaningful); Blackwell v. FBI, 646 F.3d 37, 42 (D.C. Cir. 2011) (affirming withholding of Choicepoint reports made to FBI because particular method by which data is "searched, organized, and reported" to FBI is not publicly known, and release of such reports could allow criminals to develop countermeasures to technique); Long v. ICE, 464 F. Supp. 3d 409, 422-23 (D.D.C. 2020) (protecting metadata and schemas of an ICE database because disclosure could enable a hacker "to move faster through the databases to view, modify, or delete data" and public disclosure could "incentivize future attacks and make those attacks more harmful"); Elec. Priv. Info. Ctr. v. DEA, 401 F. Supp. 3d 37, 46-47 (D.D.C. 2019) (protecting names of agencies that have access to the Hemisphere database because release of this information "necessarily discloses a technique or procedure used by that agency" as knowing the names of agencies using a particular database brings with it "the knowledge of how the agency employs its procedures or techniques"); Sharkey v. DOJ, No. 16-2672, 2018 WL 838678, at * 8 (N.D. Ohio Feb. 13, 2018) (protecting key indicators agency uses in deciding whether and how data is entered in non-public law enforcement databases because disclosure would reveal types and location of information agency "gathers, analyzes and utilizes within" database, "making it vulnerable to cyber attackers"); Gatson v. FBI, No. 15-5068, 2017 WL 3783696, at *13 (D.N.J. Aug. 31, 2017) (unpublished disposition) (protecting "non-public database search results and the printouts compiled therefrom"), summary affirmance granted, 779 F. App'x 112 (3d Cir. 2019); Hetznecker v. NSA, No. 16-945, 2017 WL 3617107, at *5 (E.D. Pa. Aug. 23, 2017) (protecting database identifiers under a mosaic analysis); Elec. Privacy Info. Ctr. v. Customs

& Border Prot., 248 F. Supp. 3d 12, 19 (D.D.C. 2017) (protecting "records detailing the function, access, navigation, and capabilities" of law enforcement database), aff'd per curiam, No. 17-5078, 2017 WL 4220339 (D.C. Cir. Aug. 1, 2017); Vazquez, 887 F. Supp. 2d at 117-18 (protecting FBI's National Crime Information Center transaction logs because release would alert wrongdoers as to whether and by whom their illegal activities are under investigation); Hasbrouck v. U.S. Customs & Border Prot., No. 10-3793, 2012 WL 177563, at *4 (N.D. Cal. Jan. 23, 2012) (protecting certain identifiers used to access personal information in law enforcement databases to prevent disclosure of whether "CBP also tracks one or more non-obvious identifier[s], or for it to admit that it cannot retrieve information except by obvious identifiers"); Adionser v. DOJ, 811 F. Supp. 2d 284, 300 (D.D.C. 2011) (protecting techniques and procedures concerning "the identification and contents of [certain] FBI databases"), aff'd in pertinent part per curiam, No. 11-5093, 2012 WL 5897172 (D.C. Cir. Nov. 5, 2012). But cf. Am. Immigr. Council v. ICE, 464 F. Supp. 3d 228, 243-44 (D.D.C. 2020) (rejecting agency's withholding of unique identifier that agency claimed could be used to obtain sensitive law enforcement information if individual "were to hack illegally into [agency's databases] because "the harm the exemption is designed to avert – the circumvention of the law – would not be caused or advanced by the disclosure of the data in question, and it depends upon the hypothetical commission of a crime that is independent of the disclosure of the data the defendant seeks to withhold").

surveillance tactics and methods,[30] portions of a law enforcement agency's investigations and operations manual,[31] funds expended in furtherance of an investigation,[32] identities

---

[30] See, e.g., Gatson, 2017 WL 3783696, at *13 (protecting "information concerning the installation, locations, monitoring, and types of devices utilized in surveillance"); Citizens for Resp. & Ethics in Wash. v. DOJ, 160 F. Supp. 3d 226, 242-43 (D.D.C. 2016) (protecting information concerning development, capability, and limitation of drones and unmanned aerial vehicles because disclosure would risk circumvention of law); ACLU of Mich. v. FBI, No. 11-13154, 2012 WL 4513626, at *10-11 (E.D. Mich. Sept. 30, 2012) (protecting devices, methods, and tools used for surveillance and monitoring of illegal activity because disclosure of such techniques would allow criminals to develop countermeasures to nullify effectiveness of law enforcement investigations); Soghoian v. DOJ, 885 F. Supp. 2d 62, 75 (D.D.C. 2012) (protecting electronic surveillance techniques and guidance provided to investigators on use of such techniques because release could allow criminals to circumvent law enforcement efforts); Frankenberry v. FBI, No. 08-1565, 2012 U.S. Dist. LEXIS 39027, at *71 (M.D. Pa. Mar. 22, 2012) (accepting FBI's explanation that disclosure of precise placement of recording devices used by FBI to monitor conversations would allow circumvention of technique), aff'd on other grounds, 567 F. App'x 120 (3d Cir. 2014); ACLU v. DOJ, 698 F. Supp. 2d 163, 167 (D.D.C. Mar. 16, 2010) (protecting templates used by assistant U.S. attorneys to draft "applications, orders, and declarations to obtain authorization for cell phone monitoring" because release of such information would reveal details about types of information that such cell phone records can capture, limitations of such techniques, and uses of records that are not well known to public); Kurdykov v. U.S. Coast Guard, 657 F. Supp. 2d 248, 257 (D.D.C. 2009) (upholding protection of maritime counter-narcotics surveillance techniques and procedures); Carbe v. ATF, No. 03-1658, 2004 WL 2051359, at *11 (D.D.C. Aug. 12, 2004) (finding that "electronic surveillance request forms and asset forfeiture reimbursement forms . . . [are] [c]ertainly . . . protected from release by Exemption 7(E)," as disclosure "might reveal the nature of electronic equipment and the sequence of its uses").

[31] See, e.g., Djenasevic v. EOUSA, No. 18-5262, 2019 WL 5390964, at *1 (D.C. Cir. Oct. 3, 2019) (per curiam) (withholding non-public portions of DEA Agents' Manual because release of information "might increase the risk that a law will be violated or that past violators will escape legal consequences"); ACLU of N.J. v. DOJ, No. 11-2553, 2012 WL 4660515, at *9-10 (D.N.J. Oct. 2, 2012) (unpublished disposition) (withholding portions of FBI's Domestic Investigations and Operations Guide (DIOG) that list certain techniques, procedures and events that trigger FBI's use of such techniques and procedures, because disclosure of such records could allow bad actors to circumvent FBI's efforts), aff'd sub nom. ACLU of N.J. v. FBI, 733 F.3d 526 (3d Cir. 2013); ACLU of Mich. v. FBI, No. 11-13154, 2012 WL 4513626, at *10 (E.D. Mich. Sept. 30, 2012) (withholding sections of FBI's DIOG that would, if released, allow wrongdoers to undermine FBI's law enforcement activities); Elec. Frontier Found. v. DOD, No. 09-05640, 2012 WL 4364532, at *4-5 (N.D. Cal. Sept. 24, 2012) (protecting portions of law enforcement handbook containing details of agency's use of internet and social networking websites for investigations); Muslim Advocs. II, 833 F. Supp. 2d 92, 109 (D.D.C. 2011) (protecting portions of FBI's DIOG that would reveal circumstances under which investigations are or are not approved, and which particular investigative activities are or are not allowed in context of particular investigations, because such information could allow wrongdoers to alter behavior to avoid detection by law

of vendors supplying equipment and services to law enforcement agencies,[33] law enforcement codes,[34] and techniques used to uncover tax fraud.[35] Courts have also

---

enforcement officers); Muslim Advocs. I, 833 F. Supp. 2d 92, 104-05 (D.D.C. 2011) (endorsing withholding of chapters five and ten of FBI's DIOG).

[32] See, e.g., Citizens for Resp. & Ethics in Wash. v. DHS, No. 20-1400, 2021 WL 950415, at *7-8 (D.D.C. Mar. 12, 2021) (protecting information concerning room rates, meal expenditures and incidental expenses because "releasing these figures could help wrongdoers estimate the number of Secret Service personnel on the trip, which in turn could help them predict the size of future Secret Service details"); Associated Press v. FBI, 265 F. Supp. 3d 82, 100 (D.D.C. 2017) (protecting purchase price of tool to unlock smartphone of suspected terrorist because release would allow adversaries to "assess the nature of the tool and determine its likely capabilities"); Frankenberry, 2012 U.S. Dist. LEXIS 39027, at *71 (protecting expenditures made by law enforcement authorities during investigation), aff'd, 567 F. App'x 120 (3d Cir. 2014); Concepcion v. FBI, 606 F. Supp. 2d 14, 43-44 (D.D.C. 2009) (withholding amount of money used to purchase evidence). But see Kan. ex rel. Schmidt v. DOD, 320 F. Supp. 3d 1227, 1246 (D. Kan. 2018) (holding that law enforcement costs "without copious amounts of detail" do not reveal law enforcement techniques, procedures, or guidelines in a way that could increase the risk of circumvention); Hidalgo v. FBI, 541 F. Supp. 2d 250, 253-54 (D.D.C. 2008) (ordering disclosure of information regarding payments to confidential informants because agency failed to show risk of circumvention from disclosure).

[33] See, e.g., Associated Press, 265 F. Supp. 3d at 99 (protecting identity of technology vendor who assisted FBI in unlocking smartphone of suspected terrorist because disclosure would enable hostile entities "to circumvent the technology"); Citizens for Resp. & Ethics in Wash., 160 F. Supp. 3d at 243 (protecting identities of vendors and suppliers because disclosure would "reveal the equipment and services provided" to the law enforcement agency).

[34] See, e.g., Patino-Restrepo v. DOJ, No. 17-5143, 2019 WL 1250497, at *2 (D.C. Cir. Mar. 14, 2019) (per curiam) (holding that "DEA's redaction of internal codes and identification numbers was proper under FOIA Exemption 7(E)"); Lapp v. FBI, No. 14-160, 2016 WL 737933, at *5 (N.D. W. Va. Feb. 23, 2016) (protecting CJIS access codes because disclosure could allow unauthorized access to law enforcement databases); Skinner III, 893 F. Supp. 2d 109, 114 (D.D.C. 2012) (protecting DHS TECS codes because release could allow individual to access database or otherwise circumvent law); Miller v. DOJ, 872 F. Supp. 2d 12, 28-29 (D.D.C. 2012) (protecting TECS and NADDIS numbers maintained by DEA because release could reveal law enforcement techniques or otherwise lead to legal circumvention); McRae v. DOJ, 869 F. Supp. 2d 151, 168-69 (D.D.C. 2012) (withholding computer codes from TECS, National Criminal Information Center, and local law enforcement databases); Bloomer v. DHS, 870 F. Supp. 2d 358, 369 (D. Vt. 2012) (withholding law enforcement TECS database codes); Abdelfattah v. ICE, 851 F. Supp. 2d 141, 145 (D.D.C. 2012) (protecting FBI "program codes").

[35] See Palmarini v. IRS, No. 17-3430, 2019 WL 1429547, at *5 (E.D. Pa. Mar. 29, 2019) (holding that agency properly protected checklist form used to assess compliance with tax laws because release of this information would reveal enforcement processes and priorities of the IRS that "may enable tax dodgers to avoid detection"); Carp v. IRS, No. 00-5992,

upheld protection for techniques and procedures pertaining to the forensic analysis of firearms[36] and computers,[37] details concerning information technology security,[38] details about the status of investigatory efforts,[39] search and arrest warrant execution

---

2002 WL 373448, at *6 (D.N.J. Jan. 28, 2002) (concluding that disclosure would "expose[] specific, non-routine investigative techniques used by the IRS to uncover tax fraud"); Tax Analysts v. IRS, 152 F. Supp. 2d 1, 17 (D.D.C. 2001) (protecting agency summary of tax-avoidance scheme, "including identification of vulnerabilities" in IRS operations), rev'd & remanded on other grounds, 294 F.3d 71 (D.C. Cir. 2002); Peyton v. Reno, No. 98-1457, 2000 WL 141282, at *1 (D.D.C. Jan. 6, 2000) (protecting Discriminant Function scores used to select tax returns for evaluation); Wishart v. Comm'r, No. 97-20614, 1998 WL 667638, at *6 (N.D. Cal. Aug. 6, 1998) (protecting Discriminant Function scores to avoid possibility that "taxpayers could manipulate" return information to avoid IRS audits), aff'd, 199 F.3d 1334 (9th Cir. 1999) (unpublished table decision).

[36] See Nat'l Pub. Radio, Inc. v. FBI, No. 18-03066, 2021 WL 1668086, at *9 (D.D.C. Apr. 28, 2021) (protecting video footage featuring ammunition ballistics tests because disclosure would "arm adversaries with the foundational information about the offensive and defensive capabilities of law enforcement" while also enabling those adversaries to use this information "to circumvent the law by modifying the types of ammunition they use when dealing with law enforcement"); Skinner I, 744 F. Supp. 2d 185, 214-15 (D.D.C. 2010)(protecting details of firearms toolmark forensic techniques to avoid disclosure of means by which law enforcement officers identify such toolmarks).

[37] See Blackwell v. FBI, 646 F.3d 37, 42 (D.C. Cir. 2011) (protecting techniques of forensic examinations of computers conducted by law enforcement personnel because release would expose "computer forensic vulnerabilities" to wrongdoers); see also Gatson v. FBI, No. 15-5068, 2017 WL 3783696, at *14 (D.N.J. Aug. 31, 2017) (protecting "computer analysis response team reports and data").

[38] See, e.g., Prechtel v. FCC, 330 F. Supp. 3d 320, 335 (D.D.C. 2018) (protecting agency's electronic server logs because disclosure "would reveal sensitive information regarding [its] IT architecture, including security measures [it] takes to protect its systems from malicious activity" and would provide a """roadmap""" to circumvent agency's defensive efforts) (quoting agency declaration); Poitras v. DHS, 303 F. Supp. 3d 136, 159 (D.D.C. 2018) (withholding "'protected internal e-mail addresses, non-public intranet web addresses, and a secure internal e-mail tool'" because disclosure would increase risk of unauthorized access to agency's IT system) (quoting agency declaration); Levinthal v. FEC, 219 F. Supp. 3d 1, 8-9 (D.D.C. 2016) (protecting study that assesses vulnerabilities in information technology system because possible security risk exists and disclosure could permit unlawful access to agency system).

[39] See, e.g., Gatson, 2017 WL 3783696, at *13 (protecting "records containing information about the types and dates of investigations conducted" by agency because release would reveal activities that "trigger a full investigation"); Skinner II, 806 F. Supp. 2d 105, 115-16 (D.D.C. 2011) (withholding "all-points bulletin" regarding ongoing criminal law enforcement operation); Council on Am.-Islamic Rels., Cal. v. FBI, 749 F. Supp. 2d 1104, 1123 (S.D. Cal. 2010) (finding that disclosure of bases for investigations, dates of initiation of investigations, and whether investigations are "preliminary" or "full field" would allow

techniques,[40] suspect threat detection techniques,[41] techniques and procedures concerning detainees and inmates,[42] law enforcement checkpoints,[43] selection criteria

---

targets to avoid detection and circumvent law, and would impede FBI's investigative effectiveness); cf. Shapiro I, 239 F. Supp. 3d 100, 111-16 (D.D.C. 2017) (protecting FOIA request search slips created within past twenty-five years for which agency had issued "no records" responses to underlying FOIA request because disclosure "would likely reflect important information about the 'scope of the FBI's [domestic terrorism] program in the United States, the scope and focus of its investigative efforts, and strategies it plans to pursue in preventing and disrupting domestic terrorist activity'" which could "create a risk of circumvention of the law") (quoting agency declaration).

[40] See Skinner I, 744 F. Supp. 2d at 214-15 (protecting details of search and arrest warrant techniques where disclosure would allow investigatory subjects to identify circumstances under which search warrants are executed).

[41] See Heartland All. Nat'l Immigrant Just. Ctr. v. DHS, 840 F.3d 419, 421 (7th Cir. 2016) (holding that "withholding of the name of a terrorist organization from an alien who is being questioned" is a law enforcement technique protectable under Exemption 7(E)); Elec. Privacy Info. Ctr. v. Customs & Border Prot., 248 F. Supp. 3d 12, 19 (D.D.C. 2017) (protecting details of internal agency system that allows agency to identify and apprehend individuals posing a security or law enforcement risk); ACLU of N.J. v. DOJ, No. 11-2553, 2012 WL 4660515, at *10 (D.N.J. Oct. 2, 2012) (protecting criteria for identification and evaluation of suspected terrorist groups because release of such information would allow targets to alter behavior to "avoid detection and to exploit gaps in FBI intelligence"); Elec. Frontier Found. v. DOD, No. 09-05640, 2012 WL 4364532, at *10 (N.D. Cal. Sept. 24, 2012) (withholding search terms used to detect online threats to Secret Service protectees); ACLU of Wash. v. DOJ, No. 09-0642, 2012 U.S. Dist. LEXIS 137204, at *5-6 (W.D. Wash. Sept. 21, 2012) (protecting "events, behaviors, and objects" to be considered in detection of terrorist activity because even if some indicators are publicly known, disclosure of all such factors would allow wrongdoers to adjust behavior to avoid detection); Skinner II, 806 F. Supp. 2d at 115-16 (agreeing with agency's withholding of criminal profile describing habits and threat level of subject of investigation).

[42] See, e.g., Rosenberg v. DOD, 342 F. Supp. 3d 62, 94-95 (D.D.C. 2018) (protecting protocols addressing handling of detainees on hunger strikes because disclosure would render techniques and procedures ineffective); Pinson v. DOJ, 313 F. Supp. 3d 88, 117-18 (D.D.C. 2018) (protecting use of force techniques and procedures in federal prison because disclosure would allow circumvention and could reduce usefulness); cf. Evans v. BOP, 951 F.3d 578, 587 (D.C. Cir. Mar. 10, 2020) (rejecting withholding of prison surveillance video in full because agency had not explained why it could not use techniques commonly used by average citizens to segregate video to remove 7(E) concerns).

[43] Skinner II, 806 F. Supp. 2d at 115-16 (protecting information regarding actions to be taken by law enforcement personnel stationed at checkpoints if subjects of investigation are encountered); cf. Fams. for Freedom v. U.S. Customs & Border Prot., 797 F. Supp. 2d 375, 391 (S.D.N.Y. 2011) [hereinafter Fams. for Freedom I] (allowing withholding of station-level, but not regional arrest data, for Customs border entry checkpoints despite

and fraud indicators associated with applications for employment or government benefits,[44] certain interview techniques,[45] and a list showing which select techniques and procedures were used by the FBI in a given case, along with the FBI's internal rating of the effectiveness of each of those techniques.[46]

---

simultaneously holding that such data does not constitute "techniques or procedures" or "guidelines").

[44] See Morley v. CIA, 508 F.3d 1108, 1129 (D.C. Cir. 2007) (affirming CIA's invocation of Exemption 7(E) to prevent release of techniques and procedures pertaining to background investigations conducted to determine suitability for security clearances); Cath Legal Immigr. Network, Inc. v. USCIS, No. 19-1511, 2020 WL 5747183, at *13 (approving withholding of document evaluating fraud in Special Immigration Juvenile cases "because release . . . would disclose how the Agency considers fraud indicators, creating a risk of circumvention of the law"); Sheridan v. OPM, 278 F. Supp. 3d 11, 23 (D.D.C. 2017) (finding that "'[i]t is self-evident that information revealing security clearance procedures could render those procedures vulnerable and weaken their effectiveness at uncovering background information on potential candidates'") (quoting Mayer Brown LLP v. IRS, 562 F.3d 1190, 1192 (D.C. Cir. 2009)); Techserve All. v. Napolitano, 803 F. Supp. 2d 16, 29 (D.D.C. 2011) (allowing withholding of "selection criteria, fraud indicators, and investigative process" . . . "use[d] in fraud investigations during the H-1B visa process").

[45] Frank LLP v. Consumer Fin. Prot. Bureau, 480 F. Supp. 3d 87, 103-04 (D.D.C. 2020) (finding application of Exemption 7(E) to withhold interview techniques to be proper because "the *specific* interview methods used to investigate Consumer Financial Protection Act and Fair Debt Collection Practices Act violations are confidential" and not generally known by the public).

[46] See, e.g., Frankenberry v. FBI, 567 F. App'x 120, 124-25 (3d Cir. 2014) (affirming protection of portions of FBI FD-515 form used to rate effectiveness of investigative techniques); Skinner I, 744 F. Supp. 2d 185, 214-15 (D.D.C. 2010) (noting that release of such information could allow criminal targets to change their modus operandi to avoid detection); Tunchez v. DOJ, 715 F. Supp. 2d 49, 55-56 (D.D.C. 2010) (same), aff'd per curiam, No. 10-5228, 2011 WL 1113423 (D.C. Cir. Mar. 14, 2011); Sellers v. DOJ, 684 F. Supp. 2d 149, 164-65 (D.D.C. 2010) (noting that multiple cases have upheld withholding of such records).

Although courts have rejected agency declarations that are too conclusory,[47] which merely recite the statutory standard,[48] or which otherwise fail to demonstrate that the

---

[47] See, e.g., Stahl v. DOJ, No. 19-4142, 2021 WL 1163154, at *9 (E.D.N.Y. Mar. 26, 2021) (rejecting agency's argument that portions of a surveillance video are protected under Exemption 7(E) due to the agency's failure to explain how release of the video footage "would compromise the agency's ability to perform investigations or prosecutions"); Ecological Rts. Found. v. EPA, No. 19-980, 2021 WL 535725, at *30 (D.D.C. Feb. 13, 2021) (criticizing agency's declaration for failing to include any "specification of the law enforcement ends to which the records relate or indeed, any evidence that the records were even used by, or made available to, law enforcement"); Elec. Frontier Found. v. DOJ, No. 17-03263, 2019 WL 2098084, at *2 (N.D. Cal. May 14, 2019) (finding government's argument that aggregate disclosure of termination letters issued to private companies would reveal a law enforcement trend to be "dubious" and not protected under Exemption 7(E)); ACLU v. DHS, 243 F. Supp. 3d 393, 403- (S.D.N.Y. 2017) (finding that agency did not meet its burden to provide more than "'generic assertions'" and "'boilerplate'" justifications) (quoting ACLU v. Off. of the Dir. of Nat'l Intelligence, No. 10-4419, 2011 WL 5563520, at *11 (S.D.N.Y. Nov. 15, 2011)); Strunk v. U.S. Dep't of State, 845 F. Supp. 2d 38, 47 (D.D.C. 2012) (holding that even under "low standard" for withholding under Exemption 7(E) established by D.C. Circuit, agency's declaration offered "too little detail" to demonstrate withholdability of records at issue); Raher v. BOP, No. 09-526, 2011 WL 2014875, at *9 (D. Or. May 24, 2011) (granting summary judgment to requester because agency's declarant failed to explain why responsive records met standard for withholding under Exemption 7(E)); Clemente v. FBI, 741 F. Supp. 2d 64, 88 (D.D.C. 2010) (noting that declarant cannot merely rely upon "vaguely worded categorical description" of withheld law enforcement techniques, but "must provide evidence . . . of the nature of the techniques in question"); Allard K. Lowenstein Int'l Hum. Rts. Project v. DHS, 603 F. Supp. 2d 354, 360 (D. Conn. 2009) [hereinafter Lowenstein I] (criticizing portions of agency's declaration describing "ongoing law enforcement techniques" as "vague" and "of little, or no, use"; agency "must understand that affidavits and indices must be 'relatively detailed' and nonconclusory to serve their intended purpose") (citation omitted), aff'd on other grounds, 626 F.3d 678 (2d Cir. 2010); Feshbach v. SEC, 5 F. Supp. 2d 774, 786-87, 786 n.11 (N.D. Cal. 1997) (finding agency's reasons for withholding computer printouts from internal database to be conclusory and insufficient); see also Jett v. FBI, 139 F. Supp. 3d 352, 363-64 (D.D.C. 2015) (concluding after in camera review that agency properly withheld investigative strategies despite inadequacy of agency's declaration); El Badrawi, 583 F. Supp. 2d at 313-16, 319-20 (ordering in camera review for all Exemption 7(E) claims made by defendants due to deficiencies in declarations), subsequent opinion, 596 F. Supp. 2d 389, 397-99 (D. Conn. 2009) (following in camera review, ordering partial releases of portions of records previously withheld under Exemption 7(E), approving withholdings of other portions, but simultaneously ordering supplemental Vaughn Indices for those portions properly withheld to correct deficiencies noted in previous opinion).

[48] See, e.g., Citizens for Resp. & Ethics in Wash. v. DOJ, 746 F.3d 1082, 1102 (D.C. Cir. 2014) (finding agency's "near-verbatim recitation of the statutory standard" inadequate); Island Film, S.A. v. Dep't of the Treasury, 869 F. Supp. 2d 123, 138 (D.D.C. 2012) (rejecting agency's attempt to withhold database printouts because agency "merely recite[d] the language of the exemption"); El Badrawi v. DHS, 583 F. Supp. 2d 285, 313 (D. Conn. 2008)

release of records would cause the claimed harms,[49] courts have permitted agencies to describe secret law enforcement techniques in only general terms, where necessary, while

---

(finding agencies' "Vaughn indices merely restate statutory language and case law, and lack the specificity necessary" for de novo review).

[49] See, e.g., Evans v. BOP, 951 F.3d 578, 586-87 (D.C. Cir. Mar. 10, 2020) (finding agency's affidavit in support of withholding portions of surveillance footage to be "vague" and failing to provide sufficient specificity to trigger 7(E) protection); Prop. of the People, Inc. v. DOJ, No. 17-1193, 2021 WL 1700069, at *7 (D.D.C. Apr. 29, 2021) (noting that "'[agency's] explanation here fails to demonstrate "that release of [these] document[s] might increase the risk 'that a law will be violated or that past violators will escape legal consequences'"" and finding nothing in surveillance logs from over twenty years ago that "bad actors could make use of"); Ecological Rts. Found., 2021 WL 535725, at *30-31 (noting agency failed to identify a law enforcement technique, procedure, or guideline connected to the redacted information or "any way in which disclosure of this information would create or enhance a risk of violation of the law"), vacating opinion in part on reconsideration, 2021 WL 2209380 (D.D.C. June 1, 2021)); Pinson v. DOJ, 313 F. Supp. 3d 88, 118-19 (D.D.C. 2018) (rejecting agency's withholding of records related to statute-based programming assignment used to manage inmates because agency did not demonstrate that information was not publicly known or show how risk of circumvention of law would occur); Higgs v. U.S. Park Police, No. 16-96, 2018 WL 3109600, at *14-15 (S.D. Ind. June 25, 2018) (rejecting application of Exemption 7(E) to twenty-year old National Crime Information Center reports because agency declaration "fails to acknowledge the passage of time . . . and . . . the possibility that such techniques are sufficiently out of date so as to negate the possible risk of criminals gaining access thereto"), aff'd in part & remanded in part on other grounds, 933 F.3d 897 (7th Cir. 2019); ACLU of Ariz. v. DHS Sec. Off. for C.R. & C.L., No. 15-00247, 2017 WL 3478658, at *14 (D. Ariz. Aug. 14, 2017) (unpublished disposition) (rejecting withholding of codes, web addresses, and case numbers because it is implausible that disclosure "could allow easy navigation of internal law enforcement computer systems" and "case numbers are not connected to law enforcement databases"); Long v. ICE, 149 F. Supp. 3d 39, 53 (D.D.C. 2015) (holding that agency did not demonstrate that disclosure of law enforcement metadata and database schema would increase risk of claimed harm of cyber-attack or data breach because no external entry point to databases exists); Fams. for Freedom I, 797 F. Supp. 2d 375, 391-94 (S.D.N.Y. 2011) (rejecting agency's withholding of border arrest statistics; finding they were not sufficiently detailed to enable wrongdoers to circumvent border security measures; also rejecting withholding of "charge codes" keyed to legal reason that individual was arrested for violation of immigration laws because such codes were already publicly available and could not cause harm); Lowenstein I, 603 F. Supp. 2d at 363 (ordering release of "general outline of the operational steps" because it "would not reveal specific operational techniques"); Jud. Watch, Inc. v. U.S. Secret Serv., 579 F. Supp. 2d 182, 187-88 (D.D.C. 2008) (stating that records pertaining to visitor names, dates of visits, and persons visited would not reveal investigation procedures); Hidalgo v. FBI, 541 F. Supp. 2d 250, 253-54 (D.D.C. 2008) (ordering disclosure of payment information to confidential informants because "the FBI has not shown that there is a 'significant risk' that its future investigations will be circumvented by disclos[ure]") (internal citations omitted).

withholding the full details.[50] Courts have also recognized that sometimes it is not possible to describe secret law enforcement techniques even in general terms without disclosing the very information sought to be withheld.[51] A court's in camera review of the documents at issue may be required to demonstrate the propriety of nondisclosure in such cases.[52]

Guidelines for Law Enforcement Investigations and Prosecutions

The second clause of Exemption 7(E) protects "guidelines for law enforcement investigations or prosecutions if [their] disclosure could reasonably be expected to risk circumvention of the law."[53]

The Court of Appeals for the Second Circuit has distinguished between "guidelines" in the second clause of Exemption 7(E) and "techniques and procedures" in the first clause, by noting that "guidelines" refer to the means by which agencies allocate resources for law enforcement investigations (whether to investigate) while "techniques and

---

[50] See, e.g., Truthout v. DOJ, 667 F. App'x 637, 637-38 (9th Cir. 2016) (concluding that further description in agency declaration would force agency to reveal withheld information); Hamdan v. DOJ, 797 F.3d 759, 778 (9th Cir. 2015) (concluding that "further detail would compromise the very techniques the government is trying to keep secret"); Bowen v. FDA, 925 F.2d 1225, 1229 (9th Cir. 1991) (ruling that release of specifics of cyanide-tracing techniques would present serious threat to future product-tampering investigations); Brown v. FBI, 873 F. Supp. 2d 388, 407 (D.D.C. 2012) (endorsing practice of submitting documents for in camera review where even general description of records would reveal secret law enforcement techniques or procedures); Jud. Watch, Inc. v. Dep't of State, 650 F. Supp. 2d 28, 34 n.6 (D.D.C. 2009) (allowing agency to describe techniques and procedures in general terms where greater specificity would allow investigatory targets to thwart investigation).

[51] See Boyd v. ATF, No. 05-1096, 2006 WL 2844912, at *9 (D.D.C. Sept. 29, 2006) (stating that "[i]n some cases, it is not possible to describe secret law enforcement techniques without disclosing the very information withheld"); McQueen v. United States, 264 F. Supp. 2d 502, 521 (S.D. Tex. 2003) (finding that requested documents detail how agent detected tax evaders and that "these details, by themselves, would reveal law enforcement techniques and procedures" and thus were properly withheld), summary affirmance granted on other grounds, 100 F. App'x 964 (5th Cir. 2004).

[52] See, e.g., Jones v. FBI, 41 F.3d 238, 249 (6th Cir. 1994) (concluding upon in camera review that investigative techniques were properly withheld); Sussman v. DOJ, No. 03-3618, 2008 WL 2946006, at *10 (E.D.N.Y. July 29, 2008) (ordering in camera review where agency asserted that revealing name of investigative technique would allow circumvention of investigative efforts).

[53] 5 U.S.C. § 552(b)(7)(E) (2018); see Mayer Brown LLP v. IRS, 562 F.3d 1190, 1192-93 (D.C. Cir. 2009) (discussing meaning of phrase "could reasonably be expected to risk circumvention of the law" found in second clause of Exemption 7(E)).

procedures" refer to the means by which agencies conduct investigations (how to investigate).[54]

The Court of Appeals for the District of Columbia Circuit has held that the government need not prove that circumvention of the law is a necessary result of disclosure, but instead found that Exemption 7(E)'s circumvention clause is satisfied if disclosure could "risk" a circumvention harm.[55] The D.C. Circuit found that the agency need not show that there is a certainty that a risk is present; it is enough if there is an "expectation" of a risk of circumvention.[56] Even the expectation of risk need not be certain, the court held, as the statute merely requires that the risk "could reasonably" be expected.[57] The D.C. Circuit opined that this standard "is written in broad and general terms" to ensure the necessary deterrence of those who would otherwise attempt to evade the law.[58]

Courts have found protection for various types of law enforcement guidelines "that pertain[] to the prosecution or investigative stage of a law enforcement matter,"[59]

---

[54] See Allard K. Lowenstein Int'l Hum. Rts. Project v. DHS, 626 F.3d 678, 682 (2d Cir. 2010) (noting as example that if tax investigators are told only to bring charges against those who evade more than a certain enumerated dollar amount in taxes, such guidance constitutes guidelines, while if investigators are given instructions on manner in which to investigate those suspected of tax evasion, such details constitute techniques and procedures); see also Fams. for Freedom v. U.S. Customs & Border Prot., 837 F. Supp. 2d 287, 296-97 (S.D.N.Y. 2011) (relying on definition set forth in Allard to state that techniques and procedures constitute how, where, and when law enforcement methods are carried out, while policy and budgetary decisions about law enforcement staffing patterns arguably constitute "guidelines" under Exemption 7(E)).

[55] Mayer Brown, 562 F.3d at 1192-93.

[56] Id.

[57] Id.; see also Blackwell v. FBI, 646 F.3d 37, 42 (D.C. Cir. 2011) (same) (quoting Mayer Brown); McRae v. DOJ, 869 F. Supp. 2d 151, 169 (D.D.C. 2012) (same).

[58] Mayer Brown, 562 F.3d at 1192-93; see also Strunk v. Dep't of State, 845 F. Supp. 2d 38, 47 (D.D.C. 2012) (observing that Mayer Brown set forth a "low standard" for withholding records pursuant to Exemption 7(E)).

[59] See Jud. Watch, Inc. v. FBI, No. 00-745, 2001 WL 35612541, at *9 (D.D.C. Apr. 20, 2001).

including law enforcement manuals,[60] policy guidance documents,[61] settlement guidelines,[62] monographs,[63] and emergency plans,[64] as well as other types of law enforcement guidelines.[65] One court has upheld protection for computer codes, not

---

[60] See, e.g., PHE, Inc. v. DOJ, 983 F.2d 248, 251 (D.C. Cir. 1993) (approving withholding of portion of FBI manual containing investigation guidance); Gatson v. FBI, No. 15-5068, 2017 WL 3783696, at *14 (D.N.J. Aug. 31, 2017) (protecting "operational directives concerning sensitive investigative techniques and strategies"), summary affirmance granted, 779 F. App'x 112 (3d Cir. 2019); Peter S. Herrick's Customs & Int'l Trade Newsl. v. U.S. Customs & Border Prot., No. 04-00377, 2006 WL 1826185, at *7 (D.D.C. June 30, 2006) (protecting many portions of manual pertaining to seized property, including details of "the transport, seizure, storage, testing, physical security, evaluation, maintenance, and cataloguing of, as well as access to, seized property"); Guerrero v. DEA, No. 93-2006, slip op. at 14-15 (D. Ariz. Feb. 22, 1996) (approving nondisclosure of portions of Special Agents Manual); Church of Scientology Int'l v. IRS, 845 F. Supp. 714, 723 (C.D. Cal. 1993) (concluding that parts of agency Law Enforcement Manual concerning "procedures for handling applications for tax exemption and examinations of Scientology entities" and memorandum regarding application of such procedures were properly withheld); cf. ACLU of Mich. v. FBI, No. 11-13154, 2012 WL 4513626, at *11 (E.D. Mich. Sept. 30, 2012) (protecting hypotheticals used to train investigators to recognize circumstances that would trigger an investigation, circumstances under and extent to which informants are allowed to participate in activities of third parties, and approval limitations on use of certain technique or procedure by law enforcement personnel), aff'd, 734 F.3d 460 (6th Cir. 2013).

[61] See Vento v. IRS, No. 08-159, 2010 WL 1375279, at *8 (D.V.I. Mar. 31, 2010) (endorsing protection of DOJ policy memorandum to IRS employees regarding when and how they should process certain law enforcement summons); Asian L. Caucus v. DHS, No. 08-00842, 2008 WL 5047839, at *5 (N.D. Cal. Nov. 24, 2008) (protecting interim policy guidance for border searches and examinations even where guidance was superseded by later version because "the newer version does not render the [earlier] policy valueless").

[62] See Mayer Brown, 562 F.3d at 1196 (finding that settlement guidelines in case that involved fraudulent tax schemes "fall squarely within" language of Exemption 7(E)'s second clause).

[63] See Silber v. DOJ, No. 91-876, transcript at 25 (D.D.C. Aug. 13, 1992) (bench order) (ruling that disclosure of DOJ monograph on fraud litigation "would present the specter of circumvention of the law").

[64] See Pub. Emps. for Env't Resp. v. U.S. Sec. Int'l Boundary & Water Comm'n, 740 F.3d 195, 205 (D.C. Cir. 2014) (upholding invocation of Exemption 7(E) as to emergency action plans for two dams); Ctr. for Nat'l Sec. Studies v. INS, No. 87-2068, 1990 WL 236133, at *5-6 (D.D.C. Dec. 19, 1990) (recognizing that release of INS plans to be deployed in event of attack on U.S. could assist terrorists in circumventing border).

[65] See, e.g., Jordan v. DOJ, 668 F.3d 1188, 1201 (10th Cir. 2011) (protecting guidelines to staff for handling dangerous inmate because public release of guidelines could allow inmate to circumvent such guidelines); Rosenberg v. DOD, 342 F. Supp. 3d 62, 94-95 (D.D.C. 2018) (protecting protocols addressing handling of detainees on hunger strikes because disclosure

because the codes themselves constituted law enforcement guidelines, but because wrongdoers could use such codes to illegally gain access to sensitive law enforcement databases that contain protectable law enforcement guidelines.[66] Courts have denied protection, however, when the agency has failed to demonstrate that circumvention of the

would render guidelines ineffective); Iraqi Refugee Assistance Project v. DHS, No. 12-3461, 2017 WL 1155898, at *7 (S.D.N.Y. Mar. 27, 2017) (approving use of Exemption 7(E) to withhold enforcement guidelines related to refugee applications because public disclosure "could help applicants evade investigator techniques and thus circumvent the law"); Sussman v. U.S. Marshall Serv., No. 03-610, 2005 WL 3213912, at *9 (D.D.C. Oct. 13, 2005) (protecting "guidelines and procedures utilized in investigation [of] threats against federal court employees," because release "could create a risk of circumvention of the law"), aff'd in pertinent part, vacated in part & remanded in part on other grounds, 494 F.3d 1106 (D.C. Cir. 2007); Tax Analysts v. IRS, 152 F. Supp. 2d 1, 17 (D.D.C. 2001) (agreeing with agency that Technical Assistance documents are law enforcement guidelines and determining that disclosure of agency summary of tax-avoidance scheme, "including identification of vulnerabilities" in IRS operations, could risk circumvention of law), rev'd & remanded on other grounds, 294 F.3d 71 (D.C. Cir. 2002).

[66] See Strunk v. U.S. Dep't of State, 905 F. Supp. 2d 142, 147-49 (D.D.C. 2012) (agreeing that TECS database codes should be withheld to prevent unauthorized access to databases used by U.S. Customs and Border Protection, which contain information such as guidelines followed by Customs officials to target and inspect suspicious international travelers).

law would occur[67] or where the information at issue was not related to law enforcement investigations or prosecutions. [68]

Similarly, courts have disapproved agency declarations under Exemption 7(E)'s second clause when they provide conclusory or otherwise insufficient justifications for the withholdings.[69] Additionally, courts have found it necessary at times to conduct in

---

[67] See, e.g., ACLU of N. Cal. v. DOJ, 880 F.3d 473, 492 (9th Cir. 2018) (holding that portions of law enforcement manual containing instructions on use of electronic surveillance in criminal investigations and prosecutions "provides no relevant information that would assist criminals in" circumventing the law); Tushnet v. ICE, 246 F. Supp. 3d 422, 437 (D.D.C. 2017) (ordering review of withholdings of guides for identifying counterfeit trademarked goods because application of Exemption 7(E) is "inappropriate if there is no risk that a law could be violated . . . and successful parodies do not violate trademark laws"); Long v. ICE, 149 F. Supp. 3d 39, 53 (D.D.C. 2015) (holding that agency did not demonstrate disclosure of law enforcement metadata and database schema would increase risk of claimed harm of cyber-attack or data breach because no external entry point to databases exists); Fams. for Freedom v. U.S. Customs & Border Prot., 837 F. Supp. 2d 287, 296-97 (S.D.N.Y. 2011) (ordering release of portions of Amtrak meeting minutes, past Border Patrol staffing patterns, and transit node definitions because such records are not "techniques and procedures," and to extent such records constitute "guidelines" their release would not risk legal circumvention); ACLU of Wash. v. DOJ, No. 09-0642, 2011 WL 887731, at *7-9 (W.D. Wash. Mar. 10, 2011) (denying protection for variety of watch list related material including watch listing procedures, criteria for watch list inclusion, location of database information, procedures to prevent individuals from discovery of watch list status, watch list field codes, and guidelines for handling individuals determined to be on watch list, noting that much of this information was already public and agency failed to adequately explain harm from releasing remainder of withheld information), reconsideration granted in part on other grounds, 2011 WL 1900140, (W.D. Wash. May 19, 2011); Unidad Latina En Accion v. DHS, 253 F.R.D. 44, 59 (D. Conn. 2008) (ordering disclosure of queries contained in agency emails, finding that disclosure would not risk circumvention of law); Gordon v. FBI, 388 F. Supp. 2d 1028, 1036-37 (N.D. Cal. 2005) (holding that agency did not adequately explain how release of "the legal basis for detaining someone whose name appears on a watch list . . . could be used to circumvent agency regulations").

[68] See Peter S. Herrick's Customs & Int'l Trade Newsl. v. U.S. Customs & Border Prot., No. 04-00377, 2006 WL 1826185, at *8 (D.D.C. June 30, 2006) (holding that portion of agency manual pertaining to destruction of seized property is not related to law enforcement investigation and instead "relate[s] only to the conservation of the agency's physical and monetary resources"); Cowsen-El v. DOJ, 826 F. Supp. 532, 533-34 (D.D.C. 1992) (finding agency's program statement to be internal policy document wholly unrelated to investigations or prosecutions).

[69] See, e.g., PHE, Inc. v. DOJ, 983 F.2d 248, 252 (D.C. Cir. 1993) (describing agency's affidavit as "too vague and conclusory to support summary judgment"; agency's submission should have included "more precise descriptions of the nature of the redacted material" from agency's enforcement manual); Hussain v. DHS, 674 F. Supp. 2d 260, 271 (D.D.C. 2009) (explaining that withholdings cannot be upheld under Exemption 7(E) where agency's Vaughn index merely recites statutory language and fails to explain harm from

camera review of the withheld documents to establish the appropriateness of the agency's withholding under the second clause of Exemption 7(E).[70]

Homeland Security Records and Exemption 7(E)

Courts have regularly applied Exemption 7(E) to protect information relating to homeland security under both prongs of Exemption 7(E), including:

(1) guidelines for response to terrorist attacks;[71]

(2) records pertaining to terrorism "watch lists";[72]

---

release); Feshbach v. SEC, 5 F. Supp. 2d 774, 786-87, 786 n.11 (N.D. Cal. 1997) (finding agency's reasons for withholding checklists and selection criteria used "to determine what type of review to be given . . . documents filed with the [agency]" conclusory and insufficient).

[70] See, e.g., PHE, 983 F.2d at 252 (stating that "in camera review is appropriate when agency affidavits are not sufficiently detailed to permit meaningful assessment of the exemption claims"); Iraqi Refugee Assistance Project, 2017 WL 1155898, at *3 (finding that while agency's Vaughn index provides accurate and good-faith descriptions of the redacted material, "it describes them in broad terms, as is warranted given the potentially sensitive nature of some underlying subject matter," and that "absent in camera review, the Court would be unable to make adequate findings as to . . . the claimed FOIA exemptions and whether the discussion contain segregable factual content"); Mayer, Brown, Rowe & Maw LLP v. IRS, No. 04-2187, 2006 WL 2425523, at *8 (D.D.C. Aug. 21, 2006) (directing agency to submit "a representative sample of the [withheld] records for in camera review" because agency's declaration did not have sufficient detail to permit ruling on applicability of Exemption 7(E)), subsequent opinion, No. 04-2187, slip op. at 2-3 (D.D.C. Oct. 24, 2006) (concluding after in camera review that Exemption 7(E) was properly applied).

[71] See Bigwood v. DOD, 132 F. Supp. 3d 124, 153 (D.D.C. 2015) (adopting magistrate's recommendation) (finding Exemption 7(E) applies to records containing measures "to be taken in response to terrorist threats to military facilities"); Ctr. for Nat'l Sec. Studies v. INS, No. 87-2068, 1990 WL 236133, at *5-6 (D.D.C. Dec. 19, 1990) (according Exemption 7(E) protection to final contingency plan in event of attack on United States, to guidelines for response to terrorist attacks, and to contingency plans for immigration emergencies).

[72] See, e.g., Kalu v. IRS, 159 F. Supp. 3d 16, 23 (D.D.C. 2016) (finding agency may refuse to confirm or deny an individual's placement on its watch lists because doing so would "'circumvent the purpose of the watch lists'") (quoting Gordon v. FBI, 388 F. Supp. 2d 1028, 1037 (N.D. Cal. 2005)); El Badrawi v. DHS, 596 F. Supp. 2d 389, 396 (D. Conn. 2009) (agreeing that confirming or denying individual's presence in FBI's Violent Gang and Terrorist Organization file database "would cause the very harm FOIA . . . [Exemption] 7(E) [is] designed to protect"); Asian L. Caucus v. DHS, No. 08-00842, 2008 WL 5047839, at *4 (N.D. Cal. Nov. 24, 2008) (withholding detailed information regarding watch lists, and noting that "knowing about the general existence of government watchlists does not make further detailed information about the watchlists routine and generally known"); Gordon, 388 F. Supp. 2d at 1035-36 (protecting details of agency's aviation "watch list" program –

(3) terrorist "trend" information that would reveal travel plans by regional area;[73]

(4) records confirming whether an individual is the subject of a national security letter;[74]

(5) inspection and arrest statistics of border entry points;[75]

(6) analyses of security procedures;[76]

(7) records pertaining to domestic terrorism investigations;[77]

---

including records detailing "selection criteria" for lists and handling and dissemination of lists, and "addressing perceived problems in security measures").

[73] ACLU of Wash. v. DOJ, No. 09-0642, 2011 WL 887731, at *9 (W.D. Wash. Mar. 10, 2011) (crediting agency's explanation that disclosure of terrorist travel plans by geographic area could tip off terrorists about government's knowledge of their travel plans, allowing terrorists to take countermeasures against investigators).

[74] See Catledge v. Mueller, 323 F. App'x 464, 467 (7th Cir. 2009) (affirming agency's refusal to confirm or deny whether plaintiff was "a subject of the [national security] letters" because it "would reveal the circumstances under which the FBI has used this technique").

[75] See Am. Immigr. Council v. ICE, 464 F. Supp. 3d 228, 245 (D.D.C. 2020) (approving withholding of specific data concerning locations of border arrests and encounters because disclosure would "provide the public with information on staffing strengths and weaknesses of individual ports of entry"); Fams. for Freedom v. U.S. Customs & Border Prot., 797 F. Supp. 2d 375, 391 (S.D.N.Y. 2011) (allowing withholding of station-level, but not regional arrest data, for Customs border entry checkpoints because station-level data could tell wrongdoers about relative activity levels and arrest success rates between stations); Coastal Delivery Corp. v. U.S. Customs Serv., 272 F. Supp. 2d 958, 963-65 (C.D. Cal. 2003) (protecting number of examinations at particular seaport because information could be used in conjunction with other publicly available information to discern rates of inspection at that port, thereby allowing for identification of "vulnerable ports" and target selection).

[76] See, e.g., Voinche v. FBI, 940 F. Supp. 323, 329, 332 (D.D.C. 1996) (approving nondisclosure of information "relating to the security of the Supreme Court building and the security procedures for Supreme Court Justices" on basis of both former version of Exemption 2 and Exemption 7(E)), aff'd per curiam, No. 95-01944, 1997 WL 411685 (D.C. Cir. June 19, 1997); cf. U.S. News & World Rep. v. Dep't of the Treasury, No. 84-2303, 1986 U.S. Dist. LEXIS 27634, at *8 (D.D.C. Mar. 26, 1986) (upholding protection of Secret Service's contract specifications for President's armored limousine).

[77] See Allard K. Lowenstein Int'l Hum. Rts. Project v. DHS, 603 F. Supp. 2d 354, 364 (D. Conn. 2009) (finding "specific reference to the database [associated with effort to disrupt potential terrorist activities] used as a lookout was properly withheld under Exemption 7(E) since this information was compiled for law enforcement purposes, and if disclosed, could reasonably be expected to risk circumvention of the law"), aff'd on other grounds, 626 F.3d

(8) financial crimes research analysis;[78] and

(9) U.S. Customs Service traveler examination criteria and techniques.[79]

678 (2d Cir. 2010); ACLU v. FBI, 429 F. Supp. 2d 179, 194 (D.D.C. 2006) (holding that agency properly withheld certain records, release of which "could allow individuals 'to develop countermeasures' that could defeat the effectiveness of the agency's domestic terrorism investigations") (quoting agency declaration).

[78] See Boyd v. DEA, No. 01-0524, 2002 U.S. Dist. LEXIS 27853, at *11-13 (D.D.C. Mar. 8, 2002) (upholding protection under both clauses of Exemption 7(E) for highly sensitive research analysis contained in intelligence report).

[79] See Fams. for Freedom v. U.S. Customs & Border Prot., 837 F. Supp. 2d 287, 296-97 (S.D.N.Y. 2011) (protecting operational details of train passenger inspections by Customs agents); Barnard v. DHS, 598 F. Supp. 2d 1, 22 (D.D.C. 2009) (protecting "examination and inspection procedures," including instructions for processing international travelers); Asian L. Caucus v. DHS, No. 08-00842, 2008 WL 5047839, at *5 (N.D. Cal. Nov. 24, 2008) (withholding specific topics for questioning travelers attempting to enter United States); Hammes v. U.S. Customs Serv., No. 94-4868, 1994 WL 693717, at *1 (S.D.N.Y. Dec. 9, 1994) (protecting Customs Service criteria used to determine which passengers to stop and examine).