UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AMERICAN CIVIL LIBERTIES UNION FOUNDATION, et al.,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, et al.,

Defendants.

Case No. 19-cv-00290-EMC

ORDER DENYING DEFENDANT'S MOTION FOR PARTIAL SUMMARY JUDGMENT

Docket No. 31

I. INTRODUCTION

Plaintiffs American Civil Liberties Union Foundation and American Civil Liberties Union Foundation of Northern California seek information from a number of federal agencies regarding the government's monitoring of social media in various contexts. Plaintiffs sought that information through a Freedom of Information Act request, and the FBI responded with a partial Glomar response with respect to Plaintiffs' request for information related to immigration and transportation contexts. Plaintiffs filed this suit challenging the Glomar response. The FBI filed a Motion for Partial Summary Judgment as to the FBI's Glomar response.

II. BACKGROUND

A. Factual Background

Plaintiffs American Civil Liberties Union Foundation and American Civil Liberties Union Foundation of Northern California (collectively "Plaintiffs") bring this action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. *See* Complaint at 2, Docket No. 1. Defendants are the Department of Justice, the Federal Bureau of Investigation, the Department of Homeland Security, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, U.S.

Immigration and Customs Enforcement and the Department of State (collectively "Defendants"). *Id.* at 1. Plaintiffs seek information about "Defendant federal agencies' surveillance of social media users and speech." *Id.* at 2. Plaintiffs contend that Defendants "are taking steps to monitor social media users and their speech, activities, and associations" and that the agencies are pursuing the ability to engage in "programmatic and sustained tracking of U.S. citizens and noncitizens alike." *Id.* Plaintiffs further allege that Defendants have specifically "ramped up the monitoring and retention of immigrants' and visa applicants' social media information, including for the purpose of conducting what the Trump administration has called 'extreme vetting' or 'visa lifecycle vetting.'" *Id.*

In particular, the Complaint alleges that the FBI has "sought information from contractors on a planned automated tool that would enable the FBI to search and monitor information on social media platforms." *Id.* at 5. Plaintiffs' contend the FBI has also revealed "that it would acquire social media monitoring software that would give it full access to Twitter data, searchable using customizable filters 'tailored to operational needs.'" *Id.* "News reports further indicate that the FBI has established a social media surveillance task force," although the "purpose and scope of the task force remain unclear." *Id.* at 5–6. The Complaint argues that such surveillance "raises serious free speech and privacy concerns," "risks chilling expressive activity," and could "lead to the disproportionate targeting of racial and religious minority communities." *Id.* It also contends that "[b]asic due process and fairness are also undermined when significant decisions affecting peoples' lives . . . are influenced by secret algorithms that analyze information obtained from social media without necessary context or rules to prevent abuse." *Id.* at 6.

B. Procedural Background

On May 24, 2018, Plaintiffs submitted a FOIA request to Defendants "seeking the release of records pertaining to the federal government's social media surveillance." *Id.* at 2. Plaintiffs sought five categories of records:

(1) social media surveillance-related policies and guidance;

(2) records concerning the purchase or acquisition of social media surveillance technologies;

(3) communications to or from private businesses concerning social media surveillance products;

(4) communications to or from social media platforms concerning surveillance of social media content; and

(5) records concerning the use or incorporation of social media content within systems or programs that make use of algorithms, machine-learning processes, or predictive analytics applications.

Id. at 7.

The FBI acknowledged receipt of that FOIA request letter on June 8, 2018. *Id.* at 8. In its response, the FBI invoked Exemption 7(E) of FOIA, codified at 5 U.S.C. §552 (b)(7)(E). The exemption states:

> This section does not apply to matters that are . . . records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . 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.

In particular, the FBI stated: "we neither confirm nor deny the existence of records responsive to your request pursuant to FOIA exemption (b)(7)(E)," thereby issuing a so-called "Glomar" response to Plaintiff's entire request. *Id.* In July 2018, Plaintiffs administratively appealed the FBI's response. *Id.* The FBI denied Plaintiffs' request for expedited processing of the appeal, and on January 17, 2019, Plaintiffs filed suit in federal court (after receiving no further response to the administrative appeal in the intervening period). *Id.*

In May 2019, the FBI modified its initial Glomar response, limiting it to only part of Plaintiffs' request. *See* Joint Case Management Statement from June 5, 2019 ("JCMS") at 2, Docket No. 21. In particular, the FBI limited its Glomar response to the following portion of Plaintiffs' request:

2. All records created since January 1, 2015[1] concerning the purchase of, acquisition of, subscription to, payment for, or agreement to use any product or service that searches, analyzes, filters, monitors, or collects content available on any social media network, including but not limited to:

   a. Records concerning any product or service capable of using social media content in assessing applications for immigration benefits or admission to the United States;

   b. Records concerning any product or service capable of using social media content for immigration enforcement purposes; and

   c. Records concerning any product or service capable of using social media content for border or transportation screening purposes.

Defendant's Motion for Partial Summary Judgment ("Mot.") at 2, Docket No. 31. With respect to these parts of Plaintiffs' request, the FBI "refused to confirm or deny" the existence of responsive records, invoking the protections of FOIA Exemption (7)(E). *Id.* at 3. Plaintiffs challenge the FBI's refusal and argue that the agency has not "provided a legitimate basis for this assertion under 5 U.S.C. §552 (b)(7)(E)."[2] JCMS at 3. On September 6, 2019, Defendant DOJ filed a Motion for Partial Summary Judgment with Respect to the FBI. *See* Docket No. 31.

III. DISCUSSION

A. Legal Standard

Federal Rule of Civil Procedure 56 provides that a "court shall grant summary judgment [to a moving party] if the movant shows that there is no genuine dispute as to any material fact and

[1] "[T]he parties have [since] agreed to apply a starting date of January 1, 2016 for all parts of the Request to FBI except part 1 of the Request." JCMS at 2.

[2] At the Joint Case Management Conference on June 12, 2019, the Court directed the parties to submit "a joint letter addressing whether there is any administrative remedy Plaintiffs can pursue with respect to the FBI's modified response to their FOIA request." *See* Docket No. 23. On June 14, 2019, the parties responded with a letter, noting: "26 C.F.R. § 16.8(b)(2) provides that '[a]n appeal ordinarily will not be adjudicated if the request becomes a matter of FOIA litigation.' Because the request at issue is already in litigation, it appears that [the Department of Justice's Office of Information Policy] could not presently adjudicate an administrative appeal of the FBI's modified response." *See* Docket No. 24. The Court subsequently found it appropriate to resolve the issue "whether the FBI should process parts 2(a)–(c) of Plaintiffs' FOIA request." *See* Docket No. 26.

the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). An issue of fact is genuine only if there is sufficient evidence for a reasonable jury to find for the nonmoving party. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248-49 (1986). "The mere existence of a scintilla of evidence . . . will be insufficient; there must be evidence on which the jury could reasonably find for the [nonmoving party]." *Id.* at 252. At the summary judgment stage, evidence must be viewed in the light most favorable to the nonmoving party and all justifiable inferences are to be drawn in the nonmovant's favor. *See id.* at 255.[3]

Where a defendant moves for summary judgment based on an affirmative defense (*i.e.*, an issue on which it bears the burden of proof), the defendant must establish "all of the essential elements of the . . . defense to warrant judgment in [its] favor." *Martin v. Alamo Cmty. College Dist.*, 353 F.3d 409, 412 (5th Cir. 2003) (internal quotation marks omitted; emphasis omitted); *see also Clark v. Capital Credit & Collection Servs.*, 460 F.3d 1162, 1177 (9th Cir. 2006) (noting that a defendant bears the burden of proof at summary judgment with respect to an affirmative defense).

FOIA is animated by "the fundamental principle of public access to Government documents." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151 (1989). It is "broadly conceived," and "disclosure, not secrecy" is its dominant objective. *Id.* at 151–52. At the same time, Congress has exempted some information "under clearly delineated statutory language." *Id.* at 152 (citing *Department of Air Force v. Rose*, 425 U.S. 352, 360–61 (1976)). These exemptions are "limited" and "must be narrowly construed." *Rose*, 425 U.S. at 361. "Furthermore, 'the burden is on the agency to sustain its action.'" *John Doe Agency*, 493 U.S. at 152 (citing 5 U.S.C. § 552(a)(4)(B)). In other words, "[g]iven FOIA's overarching purpose, 'the strong presumption in favor of disclosure places the burden on the agency to justify the withholding of any requested

[3] Evidence may be presented in a form that is not admissible at trial so long as it could ultimately be capable of being put in admissible form. *See* Fed. R. Civ. P. 56(c)(2) (providing that "[a] party may object that the material cited to support or dispute a fact cannot be presented in a form that would be admissible in evidence"). *See, e.g., Fonseca v. Sysco Food Servs. of Ariz., Inc.*, 374 F.3d 840, 846 (9th Cir. 2004) (stating that "[e]ven the declarations that do contain hearsay are admissible for summary judgment purposes because they 'could be presented in an admissible form at trial'").

documents.'" *Civil Beat Law Ctr. for the Pub. Interest, Inc. v. Centers for Disease Control & Prevention*, 929 F.3d 1079, 1084 (9th Cir. 2019) (quoting *U.S. Dep't of State v. Ray*, 502 U.S. 164, 173 (1991)).

The Ninth Circuit has observed that "[g]enerally, FOIA cases should be handled on motions for summary judgment." *Lane v. Dep't of Interior*, 523 F.3d 1128, 1134 (9th Cir. 2008) (quoting *Miscavige v. IRS*, 2 F.3d 366, 369 (11th Cir.1993)); *see also Animal Legal Def. Fund v. U.S. Food & Drug Admin.*, 836 F.3d 987, 989 (9th Cir. 2016) ("Most FOIA cases are resolved by the district court on summary judgment . . . ."). Given the limited nature of discovery typically permitted in FOIA cases, district courts routinely "enter summary judgment on the basis of agency affidavits." *Lane*, 523 F.3d at 1134. Reliance on government affidavits is permissible "so long as the affiants are knowledgeable about the information sought and the affidavits are detailed enough to allow the court to make an independent assessment of the government's claim." *Id.* at 1135–36 (quoting *Lion Raisins, Inc. v. U.S. Dep't of Agric.*, 354 F.3d 1072, 1079 (9th Cir. 2004)). "Ultimately, an agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible.'" *Wolf v. C.I.A.*, 473 F.3d 370, 374–75 (D.C. Cir. 2007).

With respect to FOIA Exemption (7)(E), "[t]he legislative history of this exemption makes clear that it is to be applied only to techniques and procedures generally unknown to the public." *Dunaway v. Webster*, 519 F. Supp. 1059, 1082 (N.D. Cal. 1981); *see also Hamdan v. U.S. Dep't of Justice*, 797 F.3d 759, 777 (9th Cir. 2015) ("We have held that 'Exemption 7(E) only exempts investigative techniques not generally known to the public.'" (quoting *Rosenfeld v. U.S. Dep't of Justice*, 57 F.3d 803, 815 (9th Cir.1995))). Thus, Exemption (7)(E) covers "investigative techniques which are 'so unique as to warrant the exemption.'" *Id.* at 1083 (citing *Ferguson v. Kelley*, 448 F. Supp. 919, 926 (N.D. Ill. 1977)). Where "an agency record discusses the *application* of a publicly known technique to particular facts, the document is not exempt under 7(E). But if a record describes a specific *means* rather than an application of deploying a particular investigative technique, the record is exempt from disclosure under FOIA." *Am. Civil Liberties Union of N. California v. United States Dep't of Justice*, 880 F.3d 473, 491 (9th Cir. 2018) (internal quotations, brackets, and citations omitted).

In addition, the Ninth Circuit has clarified the scope of the exemption. Exemption (7)(E) protects 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." 5 U.S.C. § 552(b)(7)(E). The Ninth Circuit has clarified that the phrase "if such disclosure could reasonably be expected to risk circumvention of the law" applies only to the second clause, pertaining to the disclosure of *guidelines* for law enforcement investigations or prosecutions. *Hamdan*, 797 F.3d at 778 (citing *Allard K. Lowenstein Int'l Human Rights Project v. Dep't of Homeland Security*, 626 F.3d 678, 681 (2d Cir. 2010)). A risk of circumvention of the law is not required where the information would disclose *techniques and procedures* for such investigations or prosecutions. *Id.*

An agency may "provide a *Glomar* response, 'refus[ing] to confirm or deny the existence of records where to answer the FOIA inquiry would cause harm cognizable under a FOIA exception.'" *Pickard v. Dep't of Justice*, 653 F.3d 782, 785–86 (9th Cir. 2011) (quoting *Wolf*, 473 F.3d at 374). "In determining whether the existence of agency records *vel non* fits a FOIA exemption, courts apply the general exemption review standards established in non-*Glomar* cases." *Poulsen v. Dep't of Def.*, 373 F. Supp. 3d 1249, 1267 (N.D. Cal. 2019) (citing *Wolf*, 473 F.3d at 374). District courts "review *de novo* the agency's use of a FOIA exemption to withhold documents. Yet in conducting *de novo* review in the context of national security concerns, courts must accord *substantial weight* to an agency's affidavit concerning the details of the classified status of the disputed record." *Wolf v. C.I.A.*, 473 F.3d at 374 (internal quotations omitted) (quoting *Miller v. Casey*, 730 F.2d 773, 776 (D.C.Cir.1984)); *see also Hamdan*, 797 F.3d at 770 ("[W]hen dealing with properly classified information in the national security context, we are mindful of our limited institutional expertise on intelligence matters, as compared with the executive branch.").

B. Analysis

Exemption 7(E) applies only to investigative techniques that are not generally known to the public. *See Rosenfeld*, 57 F.3d at 815 (adopting the rule that "Exemption 7(E) only exempts

investigative techniques not generally known to the public"). Here, the FBI contends that while it "has acknowledged generally [that] it monitors social media as a law enforcement technique, it has not acknowledged whether it uses tools specifically to analyze social media data in conjunction with immigration records or enforcement procedures, or in the transportation security context." Mot. at 8 (quoting Declaration of Michael Seidel ("Seidel Decl.") ¶ 13, Docket No. 31-1). Thus, "[c]onfirming or denying the existence of records showing the FBI applies such techniques specific to immigration enforcement or transportation would . . . reveal FBI capabilities, or the lack thereof," such that the requested information is "properly withheld pursuant to Exemption 7(E)." Mot. at 1. The ACLU contends that the FBI has "already disclosed, openly and repeatedly, their use of social media surveillance as a multi-faceted technique," and that "the FBI's public disclosures of its reliance on social media surveillance are expansive; they are not substantively circumscribed or otherwise limited to specific aspects of the FBI's activities." Opp. at 13. Thus, it contends that a Glomar response based on Exemption 7(E) does not apply, regardless of whether it is publicly known that the FBI monitors social media specifically in the immigration or transportation security contexts. The tension between these positions raises several questions.

1. Disclosure by Other Agencies

First, does Exemption 7(E) require "the *responding agency*'s use of a technique" or does it merely focus on "whether a technique or procedure is publicly known"? *See* Opp. at 15 (emphasis added). In other words, if *other* federal agencies have disclosed use of social media monitoring in the immigration and transportation contexts, but the *FBI* has not, does that distinction matter for the purpose of assessing whether the technique is publicly known? Looking first to the text, Exemption 7(E) states: "This section does not apply to matters that are . . . records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . would disclose techniques and procedures for law enforcement investigations or prosecutions . . . ." 5 U.S.C. §552 (b)(7)(E). As the ACLU points out, the text does not explicitly "refer to the responding agency's use of a technique; instead, the focus of the analysis is on whether a technique or procedure is publicly known." Opp. at 15.

The parties focus on *American Civil Liberties Union v. C.I.A.*, 710 F.3d 422 (D.C. Cir.

2013). In *ACLU*, the plaintiff filed a FOIA request for CIA records pertaining to the use of drones. *Id.* at 425. The CIA issued a Glomar response, invoking FOIA Exemptions (b)(1) and (b)(3).[4] The ACLU challenged the response under the doctrine of "official acknowledgement." *Id.* at 425–26. Relying on the fact that the President, his counterterrorism advisor, and the CIA Director had all acknowledged that the United States uses drone strikes, the Court of Appeal concluded that it was not "logical or plausible" for the CIA to contend that it had not been officially acknowledged that the CIA "at least has an intelligence interest" in such strikes. *Id.* at 429. The Court stated: "Although the[] statements do not acknowledge that the CIA itself operates drones, they leave no doubt that some U.S. agency does." *Id.* And because the CIA "is, after all, the Central *Intelligence* Agency . . . it strains credulity to suggest that an agency charged with gathering intelligence affecting the national security does not have an 'intelligence interest' in drone strikes, even if that agency does not operate the drones itself." *Id.* at 430.

In *ACLU*, the court acknowledged that other courts had previously "permitted agencies to give a Glomar response despite the prior disclosure of another, unrelated agency." *ACLU*, 710 F.3d at 429 n.7 (citing *Frugone v. C.I.A.*, 169 F.3d 772, 774 (D.C. Cir. 1999) (courts "do not deem 'official' a disclosure made by someone other than the agency from which the information is being sought")). However, the court explained that agencies *may not* give a Glomar response "where the disclosures are made by an authorized representative of the agency's parent." *Id.* Consequently, it concluded that "[a] disclosure made by the President . . . falls on the 'parent agency' side of that line," and therefore that a Glomar response by the CIA was impermissible. *Id.*

Thus, *ACLU* does not suggest that the known use of a technique by one agency creates public knowledge of use by a different agency, unless it is publicly known that the agency's *parent agency* utilizes that technique. Here, the FBI's parent agency is the Department of Justice, and the ACLU presents no evidence that it is publicly known that the Department of Justice utilizes the social media monitoring techniques in question.

[4] Exemption 1 covers information "specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy." 5 U.S.C. § 552(b)(1). Exemption 3 covers information "specifically exempted from disclosure by statute." 5 U.S.C. § 552(b)(1).

Given the wide array of evidence indicating (1) that other agencies engage in social media monitoring in the immigration and transportation contexts, and (2) that those agencies cooperate, coordinate, and share information with the FBI, the Court also considers whether such evidence makes it possible to impute, for purposes of applying Exemption 7(E), social media monitoring in the immigration and transportation contexts to the FBI. The ACLU presents extensive evidence that the Department of Homeland Security ("DHS"), U.S. Customs and Border Patrol ("CBP"), U.S. Citizenship and Immigration Services ("USCIS"), Immigration and Customs Enforcement ("ICE"), and the Department of State ("DOS") engage in social media monitoring[5]:

- DHS
    - DHS operates a "Social Media Working Group," which is an inter-agency initiative aimed at the coordination of DHS social media screening efforts." Email Regarding Social Media Working Group ("SMWG Email"), Docket No. 34-7, Exh. G.
    - DHS "has convened a Social Media Vetting Task Force . . . to examine the Department's current and future us of social media in the DHS vetting process for operational and intelligence purposes." Email Regarding Social Media Vetting Task Force ("SMVT Email"), Docket No. 34-8, Exh. H.
    - "DHS has established a task force for using social media to screen applicants for immigration benefits." DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success ("Pilots Report") at PDF p. 3, Docket No. 34-9, Exh. I.
    - The Transportation Safety Administration (whose parent agency is DHS) was one of two agencies known to have a Dataminr[6] contract. FBI Justification for Other

[5] The ACLU also observes: "It is telling that none of the other Defendants in this lawsuit . . . have asserted that they can neither confirm nor deny whether they have responsive records. To the contrary, those Defendants have been producing records in response to the Request." *Id.* at 15.

[6] "Dataminr is the only company authorized by Twitter to provide customers direct access to the full, raw data stream of near real time Tweets." FBI Justification for Other Than Full and Open Competition at 4, Docket No. 34-2, Exh. B.

Than Full and Open Competition at 4, Docket No. 34-2, Exh. B. TSA "concluded that Dataminr was the only service that could satisfy their Indicator & Warning requirements because of the unique relationship between Twitter and Dataminr as well as Dataminr's ability to provide near real-time access to the full Twitter firehose." *Id.* This information helped the FBI to conclude "that Dataminr is the only company in the market that is able to provide the mission critical social media monitoring needed by the FBI." *Id.*

- CBP
  - Participates in DHS "Social Media Working Group." SMWG Email.
  - "While providing social media identifiers is optional [in the Electronic System for Travel Authorization process], should an applicant choose not to voluntarily provide social media information as part of his-her application, DHS/CBP may employ tools and search techniques in an attempt to locate and identify public social media accounts and profiles belonging to the applicant, for use in the screening and vetting process." Privacy Compliance Review of the US Customs and Border Protection Electronic System for Travel Authorization, Docket No. 34-10, Exh. J.
  - "[D]esignated CBP personnel monitor publicly available, open source social media to provide situation awareness and to monitor potential threats of dangers to CBP personnel and facility operators." Publicly Available Social Media Monitoring and Situational Awareness Initiative, Docket No. 34-11, Exh. K.
  - "Although CBP provides specific notice of social media information to [Electronic System for Travel Authorization[7]] applicants, and general notice through this [Privacy Impact Assessment Update], CBP cannot provide specific and timely notice to individuals who are subject to CBP review as a result of information

[7] ESTA is a "web-based application and vetting system used by CBP to determine the eligibility of foreign nationals seeking to travel to the United States under the Visa Waiver Program." Docket No. 34-10, Exh. J at 1.

obtained. Such notice would compromise the integrity of a law enforcement matter and assist that individual in evading detection." Privacy Impact Assessment Update for the Automated Targeting System, Docket No. 34-16, Exh. P at 35.

- USCIS
  - Participates in DHS "Social Media Working Group." SMWG Email.
  - "U.S. Citizenship and Immigration Services began pilots to expand social media screening of immigration applicants." Pilots Report at PDF p. 3.
  - The Fraud Detection and National Security Data System used by USCIS may conduct "[s]earches of publicly available information, including, but not limited to, social media sites." Privacy Impact Assessment for the Fraud Detention and National Security Data System, Docket 34-14, Exh. N.
- ICE
  - Participates in DHS "Social Media Working Group." SMWG Email.
  - "Immigration and Customs Enforcement independently began a pilot to use social media screening during the visa issuance process." Pilots Report at PDF p. 3.
  - "In September 2014 . . . through the Counterterrorism and Criminal Exploitation Unit, established the Open Source Team as the first Program within ICE to leverage open source/social media exploitation to expand upon the CTCEU's established abilities to utilize government and law enforcement databases in the investigation of national security and public safety concerns that exploit vulnerabilities in the U.S. immigration system." Shared Services for Vetting Board Recommendation, Docket No. 34-12, Exh. L.
- DOS
  - "[W]e began a pilot exploration of social media screen at 17 posts that adjudicate K-visa applications and immigrant visa applications for individuals from countries of concern." Statement of Michele Bond (Asst. Sect. for Consular Affairs, Dept. of State) before House Committee on Homeland Security, Docket No 34-6, Exh. F.

In addition, the ACLU presents evidence of a high degree of cooperation and information-sharing

between the FBI and these entities, which—as demonstrated above—are known to use social media monitoring:

- DOS
    - Screens fingerprints of visa applicants against FBI's criminal records (Docket No 34-6, Exh. F at PDF p. 4).
    - Screens visa applicant photos against FBI's suspected terrorist database (*Id.* at PDF p. 5).
    - Performs continued vetting of visa applicants and recipients in cooperation with the FBI. *Id.* at PDF p. 7.
    - "[H]a[s] visa information sharing agreements under which we widely disseminate our data to other agencies that may need to learn whether a subject of interest has, or has ever applied for, a U.S. visa," and this "continual vetting" is "performed in cooperation with the . . . FBI." *Id.* at PDF pp. 7–8.
    - "Pursuant to various information sharing documents, DHS, DOS, and several vetting agencies in the law enforcement and intelligence community have developed a process to share refugee application data in DOS's Worldwide Refugee Admissions Processing System (WRAPS) to enable vetting of DOS WRAPS data against each agency's respective holdings to identify possible derogatory information related to individuals seeking refugee status." Docket No. 34-16, Exh. P at 35.
- DHS
    - DHS acknowledges "joint casework" and "information sharing" between FBI and Homeland Security Investigations ("HIS"). Docket No. 34-15, Exh. O at 12.
    - "The FBI and HSI also have MOUs governing limited coordination on specific activities, such as investigations of terrorist financing, prosecutions of aliens of national security interest, and information sharing from DHS alien information databases." *Id.* at 28.

- CBP
  - "Although the provision of social media identifiers as part of the ESTA application may be optional for the [Visa Waiver Program] any information submitted may be used for national security and law enforcement purposes." Docket No. 34-10, Exh. J at 1.
  - "Social media identifiers provided by [ESTA] applicants are used to conduct screening, vetting, and law enforcement checks in order to make eligibility determinations . . . . Social media information, whether provided by an . . . applicant or located by officers and analysts during the adjudication process, is used to assist in determining the individual's eligibility . . . [and] to assist in determining if the applicant poses a law enforcement or security risk." *Id.* at 7.
- USCIS
  - US Citizenship and Immigration Services shares information from its Fraud Detection and National Security Data System (which may include information from social media websites) when it receives a request for information or when it "proactively discloses based on information in the record . . . [Requests for information] may be received from federal law enforcement agencies, e.g. . . . the FBI . . . ." Docket No. 34-14, Exh. N at 14, 24.

As to "public knowledge," few courts have addressed whether public knowledge of a technique by some agencies' can permit an inference of a partner agency's use of that same technique. There is more guidance from cases analyzing what constitutes "official disclosure." In that context, "[a] strict test applies" and "[c]lassified information that a party seeks to obtain or publish is deemed to have been officially disclosed only if it (1) is as specific as the information previously released, (2) matches the information previously disclosed, and (3) was made public through an official and documented disclosure." *Wilson v. C.I.A.*, 586 F.3d 171, 186 (2d Cir. 2009) (internal quotation marks omitted) (quoting *Wolf*, 473 F.3d at 378); *see also Pickard*, 653 F.3d at 787 (construing official disclosure or confirmation as "an intentional, public disclosure made by or at the request of a government officer acting in an authorized capacity by the agency in

control of the information at issue").

Within the more exacting context of official disclosure, courts have declined to "infer official disclosure of information . . . [from the] release of information by another agency, or even by Congress." *Wilson*, 586 F.3d at 186 (citing *Frugone*, 169 F.3d at 774); *see also Mobley v. C.I.A.*, 806 F.3d 568, 583 (D.C. Cir. 2015) ("Disclosure by one federal agency does not waive another agency's right to assert a FOIA exemption."); *Nat'l Sec. Counselors v. C.I.A.*, 898 F. Supp. 2d 233, 288–89 (D.D.C. 2012) ("Agency A says that Agency B has records responsive to a FOIA request, but Agency B says it can neither confirm nor deny that it has any such records. If this is what the plaintiff claims, however, that claim fails as a matter of well-established FOIA law. The D.C. Circuit has consistently held that, for purposes of a *Glomar* response, it 'do[es] not deem "official' a disclosure made by someone other than the agency from which the information is being sought.'" (citing *Frugone*, 169 F.3d at 774)). One case examining the issue within the context of Exemption 7(E) did extend the reasoning of "official disclosure" cases to the "public knowledge" context. *See Rosenberg v. U.S. Dep't of Def.*, 342 F. Supp. 3d 62, 95 (D.D.C. 2018) ("Plaintiffs cannot seek disclosure of [one agency's policies] based on another agency's public disclosure of its policies."). Thus, the Court finds that the weight of authority suggests that the ACLU cannot seek disclosure of the FBI's policies based on other agencies having disclosed their own policies, together with acknowledgement that they share information with the FBI.

2. Disclosure of Technique vs. Application of Known Technique

Even if the FBI's use of social media monitoring in the contexts at issue cannot be imputed from the conduct of other agencies, Exemption 7(E) does not protect disclosures of an *application* of a known technique to particular facts, as distinguished from disclosure of an unknown law enforcement technique.

In *Rosenfeld*, the plaintiff sought information from the FBI about its investigation of free speech protest movements on UC Berkeley's campus. *Rosenfeld*, 57 F.3d at 806. The court denied the FBI's request to withhold under Exemption 7(E) information about the use of pretext phone calls because such a tactic "would leap to the mind of the most simpleminded investigator."

Id. at 815.[8] Thus, the use of pretext phone calls was "generally known to the public." *Id.* It rejected the FBI's argument that the technique at issue was the application of the technique to a particular individual and not disclosable under Exemption 7(E). *Id.* The court explained: "If we were to follow such reasoning, the government could withhold information under Exemption 7(E) under any circumstances, no matter how obvious the investigative practice at issue, simply by saying that the 'investigative technique' at issue is not the practice but the application of the practice to the particular facts underlying that FOIA request." *Id.*

In *Hamdan*, by contrast, Plaintiff sought information from multiple federal agencies regarding the role the United States might have played in his detention and torture by the government of the United Arab Emirates. *See Hamdan*, 797 F.3d at 767–69. The court found that the FBI properly withheld records "related to surveillance and credit searches" under Exemption 7(E). It stated: "It is true that credit searches and surveillance are publicly known law enforcement techniques. But the affidavits say that the records reveal techniques that, if known, could enable criminals to educate themselves about law enforcement methods used to locate and apprehend persons. This implies a specific *means* of conducting surveillance and credit searches rather than an *application*." *Id.* at 777–78 (second emphasis added). The court further contrasted a "means of conducting surveillance" with the example of "satellite surveillance of a particular place," which would be an *application* of a known technique under *Rosenberg* [sic]." *Id.* at 778.

Under *Rosenfeld* and *Hamdan*, Exemption 7(E) cannot be used to withhold information about a technique that is generally known to the public when what is at issue is a specific application of that technique to a specific context. Conversely, Exemption 7(E) does protect specific means by which an agency uses a technique where the general technique is known, but the

[8] *Albuquerque Pub. Co. v. U.S. Dep't of Justice*, 726 F. Supp. 851 (D.D.C. 1989) contains similar language: "[W]e saw nothing exceptional or secret about the techniques . . . described—namely, the use of wired informants and 'bugs' secretly placed in rooms that are under surveillance. Anyone who is familiar with the media, both television and print, is aware that the police use these and similar techniques in the course of criminal investigations. . . . [T]he government should avoid burdening the Court with an *in camera* inspection of information pertaining to techniques that are commonly described or depicted in movies, popular novels, stories or magazines, or on television. These would include, it would seem to us, techniques such as eavesdropping, wiretapping, and surreptitious tape recording and photographing." *Albuquerque*, 726 F. Supp. at 857–58.

specific means of employing that technique are not. Disclosure of those means would permit people to "educate themselves about law enforcement methods" which could "preclude [the] use [of such techniques] in future cases." *Hamdan*, 797 F.3d at 777.

Thus, in *McCash v. Cent. Intelligence Agency*, No. 5:15-CV-02308-EJD, 2017 WL 1047022 (N.D. Cal. Mar. 20, 2017), the court found proper the FBI's withholding of information under Exemption 7(E) because, although the technique was publicly known, "the public does not know how [the technique] works or how it is used in investigations." *Id.* at *2. The documents sought included "screenshots of searches conducted within [the known law enforcement database] that show categories of information, specific information fields, crossed-out text, and technical details that 'would indicate the type of software being utilized and subject it to vulnerability.' One of the printouts also includes handwritten notes that 'describe the actions taken by the FBI in searching, the results of the search, and the FBI's analysis of the results.'" *Id.*

As noted above, in this case, the FBI has issued a Glomar response regarding "All records . . . concerning the purchase of, acquisition of, subscription to, payment for, or agreement to use any product or service that searches, analyzes, filters, monitors, or collects content available on any social media network, including but not limited to:

a. Records concerning any product or service capable of using social media content in assessing applications for immigration benefits or admission to the United States;

b. Records concerning any product or service capable of using social media content for immigration enforcement purposes; and

c. Records concerning any product or service capable of using social media content for border or transportation screening purposes."

Mot. at 2. As Mr. Seidel states in his declaration, while the FBI "acknowledged generally [that] it monitors social media as a law enforcement technique,"[9] it has not "acknowledged whether it uses

[9] The FBI "has acknowledged generally [that] it monitors social media as a law enforcement technique." Seidel Decl. ¶ 13; *see also* Seidel Decl. ¶ 18 ("the FBI has acknowledged it reviews social media information when generally pursuing its law enforcement duties"). The FBI has described the constant monitoring of social media platforms and exploitation of social media as "mission-critical." Docket No. 34-4, Exh. D at PDF pp. 3, 5.

tools specifically to analyze social media data in conjunction with immigration records or enforcement procedures, or in the transportation security context." Mot. at 8 (quoting Seidel Decl. ¶ 13); *see also* Seidel Decl. ¶ 18 (same assertion). He adds that "[c]onfirming or denying the existence of records showing the FBI applies such techniques specific to immigration enforcement or transportation would itself reveal FBI capabilities, or the lack thereof." Seidel Decl. ¶ 13, 18. In particular, the FBI asserts "[w]hile the FBI has acknowledged generally it monitors social media as a law enforcement technique, it has not acknowledged whether it uses tools specifically to analyze social media data in *conjunction with immigration records or enforcement procedures*, or *in the transportation security context*." Seidel Decl. ¶ 18 (emphasis added)).

The problem for Defendants is that disclosure of social media surveillance—a well known general technique—would not reveal the *specific means* of surveillance. Denying a Glomar response would only reveal in general the application of a known technique by the FBI to immigration- or transportation-related investigations. Merely requiring the FBI to answer whether there are documents of the kind requested would not, at this juncture, require the *disclosure* of those documents which might reveal specific tools and techniques utilized by the FBI. Hence, this case is more akin to *Rosenfeld* than *Hamdan* and *Albuquerque*.

3. Disclosing the FBI's *Incapacity*

Defendant argues with some logical force that denying the Glomar response could disclose the Agency's *lack* of capability. Mr. Seidel states in his declaration, "[c]onfirming or denying the existence of records showing the FBI applies such techniques specific to immigration enforcement or transportation would itself reveal FBI capabilities, *or the lack thereof*." Seidel Decl. ¶ 13 (emphasis added). Defendants argue that disclosing that the FBI does *not* have documents pertaining to the purchase or acquisition of social media surveillance products or services would reveal it does not have the capability to monitor social media, and that this would embolden people with criminal and/or terrorist intentions, enabling them to use (or continue using) social media to plan, execute, and publicize their plans. *See* Mot. at 8–9; *see also* Seidel Decl. ¶ 20 ("Confirming the FBI has no responsive records would allow [people] to continue their social media campaigns focused on spreading their violent messages, without fear of further

investigative scrutiny while attempting to enter the United States."). However, the language of Exemption 7(E) refers only to disclosure of techniques and procedures, and not to the lack of any such technique or procedure, and the Ninth Circuit has limited the application of "risk of circumvention" of the law under Exemption 7(E) to guidelines, not techniques and procedures. Hence, it is not clear whether Defendant's negative inference argument is cognizable under Exemption 7(E). For purposes of this motion, the Court assumes it is. *See, e.g.*, *Am. Civil Liberties Union v. Dep't of Def.*, No. CV 18-154-M-DWM, 2019 WL 3945845, at *12 (D. Mont. Aug. 21, 2019) (finding that FBI had not justified its Glomar response under Exemption 7(E) because FBI's contention that "admitting a lack of responsive records could indicate the FBI has failed to detect threats" did not "justify how disclosure of the records' *existence or nonexistence* would cause harm"); *cf. Am. Civil Liberties Union v. Office of the Dir. of Nat. Intelligence*, No. 10 CIV. 4419 RJS, 2011 WL 5563520, at *7 (S.D.N.Y. Nov. 15, 2011) (denying withholdings under Exemption 1 where Agency relied on "blanket assertion" that "would reveal information about [its] success or lack of success in its collection efforts and about the U.S. Intelligence Community's capabilities, priorities, and activities" (internal quotations omitted)).

Nonetheless, the risk of criminal activity escaping detection thru social media if the FBI were to reveal it has no records is substantially mitigated by two facts. First, it is well known that many related agencies do engage in social media surveillance in the immigration centers and share that information. This lessens the risk that people will be emboldened by the FBI's disclosure to spread criminal or terrorist messages through social media. Second, even if the FBI were to disclose it has no records of purchasing or acquiring products or services used to surveil social media, that does not mean that the FBI has no such tools at its disposal, as it could have developed such tools internally.

The exemptions to FOIA are to be narrowly construed, *Rose*, 425 U.S. at 361, and the burden of proving their applicability rests with the government. Defendant has not met its burden of justifying the FBI's Glomar response.

IV. CONCLUSION

For the foregoing reasons, the Court **DENIES** DOJ's Motion for Partial Summary Judgment with Respect to FBI.

This order disposes of Docket No. 31.

IT IS SO ORDERED.

Dated: November 18, 2019

EDWARD M. CHEN
United States District Judge