

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

United States District Court
Northern District of California

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.

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

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

22 B. Procedural Background

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

- 26 (1) social media surveillance-related policies and guidance;
- 27 (2) records concerning the purchase or acquisition of social media surveillance
28 technologies;

- 1 (3) communications to or from private businesses concerning social media surveillance
2 products;
- 3 (4) communications to or from social media platforms concerning surveillance of social
4 media content; and
- 5 (5) records concerning the use or incorporation of social media content within systems or
6 programs that make use of algorithms, machine-learning processes, or predictive
7 analytics applications.

8 *Id.* at 7.

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

12 This section does not apply to matters that are . . . records or
13 information compiled for law enforcement purposes, but only to the
14 extent that the production of such law enforcement records or
15 information . . . would disclose techniques and procedures for law
16 enforcement investigations or prosecutions, or would disclose
17 guidelines for law enforcement investigations or prosecutions if
18 such disclosure could reasonably be expected to risk circumvention
19 of the law.

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

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

- 1 2. All records created since January 1, 2015¹ concerning the purchase of, acquisition of,
2 subscription to, payment for, or agreement to use any product or service that searches,
3 analyzes, filters, monitors, or collects content available on any social media network,
4 including but not limited to:
- 5 a. Records concerning any product or service capable of using social media content in
6 assessing applications for immigration benefits or admission to the United States;
 - 7 b. Records concerning any product or service capable of using social media content
8 for immigration enforcement purposes; and
 - 9 c. Records concerning any product or service capable of using social media content
10 for border or transportation screening purposes.

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

17 **III. DISCUSSION**

18 **A. Legal Standard**

19 Federal Rule of Civil Procedure 56 provides that a “court shall grant summary judgment
20 [to a moving party] if the movant shows that there is no genuine dispute as to any material fact and
21

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

24 ² At the Joint Case Management Conference on June 12, 2019, the Court directed the parties to
25 submit “a joint letter addressing whether there is any administrative remedy Plaintiffs can pursue
26 with respect to the FBI’s modified response to their FOIA request.” *See* Docket No. 23. On June
27 14, 2019, the parties responded with a letter, noting: “26 C.F.R. § 16.8(b)(2) provides that ‘[a]n
28 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.

1 the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). An issue of fact is
 2 genuine only if there is sufficient evidence for a reasonable jury to find for the nonmoving party.
 3 *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248-49 (1986). “The mere existence of a
 4 scintilla of evidence . . . will be insufficient; there must be evidence on which the jury could
 5 reasonably find for the [nonmoving party].” *Id.* at 252. At the summary judgment stage, evidence
 6 must be viewed in the light most favorable to the nonmoving party and all justifiable inferences
 7 are to be drawn in the nonmovant’s favor. *See id.* at 255.³

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

15 FOIA is animated by “the fundamental principle of public access to Government
 16 documents.” *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151 (1989). It is “broadly
 17 conceived,” and “disclosure, not secrecy” is its dominant objective. *Id.* at 151–52. At the same
 18 time, Congress has exempted some information “under clearly delineated statutory language.” *Id.*
 19 at 152 (citing *Department of Air Force v. Rose*, 425 U.S. 352, 360–61 (1976)). These exemptions
 20 are “limited” and “must be narrowly construed.” *Rose*, 425 U.S. at 361. “Furthermore, ‘the
 21 burden is on the agency to sustain its action.’” *John Doe Agency*, 493 U.S. at 152 (citing 5 U.S.C.
 22 § 552(a)(4)(B)). In other words, “[g]iven FOIA’s overarching purpose, ‘the strong presumption in
 23 favor of disclosure places the burden on the agency to justify the withholding of any requested
 24

25 ³ Evidence may be presented in a form that is not admissible at trial so long as it could ultimately
 26 be capable of being put in admissible form. *See* Fed. R. Civ. P. 56(c)(2) (providing that “[a] party
 27 may object that the material cited to support or dispute a fact cannot be presented in a form that
 28 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’”).

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

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

16 With respect to FOIA Exemption (7)(E), “[t]he legislative history of this exemption makes
17 clear that it is to be applied only to techniques and procedures generally unknown to the public.”
18 *Dunaway v. Webster*, 519 F. Supp. 1059, 1082 (N.D. Cal. 1981); *see also Hamdan v. U.S. Dep’t of*
19 *Justice*, 797 F.3d 759, 777 (9th Cir. 2015) (“We have held that ‘Exemption 7(E) only exempts
20 investigative techniques not generally known to the public.’” (quoting *Rosenfeld v. U.S. Dep’t of*
21 *Justice*, 57 F.3d 803, 815 (9th Cir.1995))). Thus, Exemption (7)(E) covers “investigative
22 techniques which are ‘so unique as to warrant the exemption.’” *Id.* at 1083 (citing *Ferguson v.*
23 *Kelley*, 448 F. Supp. 919, 926 (N.D. Ill. 1977)). Where “an agency record discusses the
24 *application* of a publicly known technique to particular facts, the document is not exempt under
25 7(E). But if a record describes a specific *means* rather than an application of deploying a
26 particular investigative technique, the record is exempt from disclosure under FOIA.” *Am. Civil*
27 *Liberties Union of N. California v. United States Dep’t of Justice*, 880 F.3d 473, 491 (9th Cir.
28 2018) (internal quotations, brackets, and citations omitted).

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

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

26 B. Analysis

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

1 investigative techniques not generally known to the public”). Here, the FBI contends that while it
 2 “has acknowledged generally [that] it monitors social media as a law enforcement technique, it has
 3 not acknowledged whether it uses tools specifically to analyze social media data in conjunction
 4 with immigration records or enforcement procedures, or in the transportation security context.”
 5 Mot. at 8 (quoting Declaration of Michael Seidel (“Seidel Decl.”) ¶ 13, Docket No. 31-1). Thus,
 6 “[c]onfirming or denying the existence of records showing the FBI applies such techniques
 7 specific to immigration enforcement or transportation would . . . reveal FBI capabilities, or the
 8 lack thereof,” such that the requested information is “properly withheld pursuant to Exemption
 9 7(E).” Mot. at 1. The ACLU contends that the FBI has “already disclosed, openly and repeatedly,
 10 their use of social media surveillance as a multi-faceted technique,” and that “the FBI’s public
 11 disclosures of its reliance on social media surveillance are expansive; they are not substantively
 12 circumscribed or otherwise limited to specific aspects of the FBI’s activities.” Opp. at 13. Thus,
 13 it contends that a Glomar response based on Exemption 7(E) does not apply, regardless of whether
 14 it is publicly known that the FBI monitors social media specifically in the immigration or
 15 transportation security contexts. The tension between these positions raises several questions.

16 1. Disclosure by Other Agencies

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

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

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

13 In *ACLU*, the court acknowledged that other courts had previously “permitted agencies to
14 give a Glomar response despite the prior disclosure of another, unrelated agency.” *ACLU*, 710
15 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
16 ‘official’ a disclosure made by someone other than the agency from which the information is being
17 sought”). However, the court explained that agencies *may not* give a Glomar response “where the
18 disclosures are made by an authorized representative of the agency’s parent.” *Id.* Consequently, it
19 concluded that “[a] disclosure made by the President . . . falls on the ‘parent agency’ side of that
20 line,” and therefore that a Glomar response by the CIA was impermissible. *Id.*

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

26 _____
27 ⁴ Exemption 1 covers information “specifically authorized under criteria established by an
28 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).

1 Given the wide array of evidence indicating (1) that other agencies engage in social media
 2 monitoring in the immigration and transportation contexts, and (2) that those agencies cooperate,
 3 coordinate, and share information with the FBI, the Court also considers whether such evidence
 4 makes it possible to impute, for purposes of applying Exemption 7(E), social media monitoring in
 5 the immigration and transportation contexts to the FBI. The ACLU presents extensive evidence
 6 that the Department of Homeland Security (“DHS”), U.S. Customs and Border Patrol (“CBP”),
 7 U.S. Citizenship and Immigration Services (“USCIS”), Immigration and Customs Enforcement
 8 (“ICE”), and the Department of State (“DOS”) engage in social media monitoring⁵:

9 • DHS

- 10 ○ DHS operates a “Social Media Working Group,” which is an inter-agency initiative
 11 aimed at the coordination of DHS social media screening efforts.” Email
 12 Regarding Social Media Working Group (“SMWG Email”), Docket No. 34-7, Exh.
 13 G.
- 14 ○ DHS “has convened a Social Media Vetting Task Force . . . to examine the
 15 Department’s current and future use of social media in the DHS vetting process for
 16 operational and intelligence purposes.” Email Regarding Social Media Vetting
 17 Task Force (“SMVT Email”), Docket No. 34-8, Exh. H.
- 18 ○ “DHS has established a task force for using social media to screen applicants for
 19 immigration benefits.” DHS’ Pilots for Social Media Screening Need Increased
 20 Rigor to Ensure Scalability and Long-term Success (“Pilots Report”) at PDF p. 3,
 21 Docket No. 34-9, Exh. I.
- 22 ○ The Transportation Safety Administration (whose parent agency is DHS) was one
 23 of two agencies known to have a Dataminr⁶ contract. FBI Justification for Other
 24

25 _____
 26 ⁵ The ACLU also observes: “It is telling that none of the other Defendants in this lawsuit . . . have
 27 asserted that they can neither confirm nor deny whether they have responsive records. To the
 28 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.

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

8 • CBP

- 9 ○ Participates in DHS “Social Media Working Group.” SMWG Email.
- 10 ○ “While providing social media identifiers is optional [in the Electronic System for
11 Travel Authorization process], should an applicant choose not to voluntarily
12 provide social media information as part of his-her application, DHS/CBP may
13 employ tools and search techniques in an attempt to locate and identify public
14 social media accounts and profiles belonging to the applicant, for use in the
15 screening and vetting process.” Privacy Compliance Review of the US Customs
16 and Border Protection Electronic System for Travel Authorization, Docket No. 34-
17 10, Exh. J.
- 18 ○ “[D]esignated CBP personnel monitor publicly available, open source social media
19 to provide situation awareness and to monitor potential threats of dangers to CBP
20 personnel and facility operators.” Publicly Available Social Media Monitoring and
21 Situational Awareness Initiative, Docket No. 34-11, Exh. K.
- 22 ○ “Although CBP provides specific notice of social media information to [Electronic
23 System for Travel Authorization⁷] applicants, and general notice through this
24 [Privacy Impact Assessment Update], CBP cannot provide specific and timely
25 notice to individuals who are subject to CBP review as a result of information
26

27 _____
28 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.

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

4 • USCIS

- 5 ○ Participates in DHS “Social Media Working Group.” SMWG Email.
- 6 ○ “U.S. Citizenship and Immigration Services began pilots to expand social media
7 screening of immigration applicants.” Pilots Report at PDF p. 3.
- 8 ○ The Fraud Detection and National Security Data System used by USCIS may
9 conduct “[s]earches of publicly available information, including, but not limited to,
10 social media sites.” Privacy Impact Assessment for the Fraud Detention and
11 National Security Data System, Docket 34-14, Exh. N.

12 • ICE

- 13 ○ Participates in DHS “Social Media Working Group.” SMWG Email.
- 14 ○ “Immigration and Customs Enforcement independently began a pilot to use social
15 media screening during the visa issuance process.” Pilots Report at PDF p. 3.
- 16 ○ “In September 2014 . . . through the Counterterrorism and Criminal Exploitation
17 Unit, established the Open Source Team as the first Program within ICE to
18 leverage open source/social media exploitation to expand upon the CTCEU's
19 established abilities to utilize government and law enforcement databases in the
20 investigation of national security and public safety concerns that exploit
21 vulnerabilities in the U.S. immigration system.” Shared Services for Vetting Board
22 Recommendation, Docket No. 34-12, Exh. L.

23 • DOS

- 24 ○ “[W]e began a pilot exploration of social media screen at 17 posts that adjudicate
25 K-visa applications and immigrant visa applications for individuals from countries
26 of concern.” Statement of Michele Bond (Asst. Sect. for Consular Affairs, Dept. of
27 State) before House Committee on Homeland Security, Docket No 34-6, Exh. F.

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

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

3 • DOS

- 4 ○ Screens fingerprints of visa applicants against FBI’s criminal records (Docket No
5 34-6, Exh. F at PDF p. 4).
- 6 ○ Screens visa applicant photos against FBI’s suspected terrorist database (*Id.* at PDF
7 p. 5).
- 8 ○ Performs continued vetting of visa applicants and recipients in cooperation with the
9 FBI. *Id.* at PDF p. 7.
- 10 ○ “[H]a[s] visa information sharing agreements under which we widely disseminate
11 our data to other agencies that may need to learn whether a subject of interest has,
12 or has ever applied for, a U.S. visa,” and this “continual vetting” is “performed in
13 cooperation with the . . . FBI.” *Id.* at PDF pp. 7–8.
- 14 ○ “Pursuant to various information sharing documents, DHS, DOS, and several
15 vetting agencies in the law enforcement and intelligence community have
16 developed a process to share refugee application data in DOS’s Worldwide
17 Refugee Admissions Processing System (WRAPS) to enable vetting of DOS
18 WRAPS data against each agency’s respective holdings to identify possible
19 derogatory information related to individuals seeking refugee status.” Docket No.
20 34-16, Exh. P at 35.

21 • DHS

- 22 ○ DHS acknowledges “joint casework” and “information sharing” between FBI and
23 Homeland Security Investigations (“HSI”). Docket No. 34-15, Exh. O at 12.
- 24 ○ “The FBI and HSI also have MOUs governing limited coordination on specific
25 activities, such as investigations of terrorist financing, prosecutions of aliens of
26 national security interest, and information sharing from DHS alien information
27 databases.” *Id.* at 28.
- 28

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

19 As to “public knowledge,” few courts have addressed whether public knowledge of a

20 technique by some agencies’ can permit an inference of a partner agency’s use of that same

21 technique. There is more guidance from cases analyzing what constitutes “official disclosure.” In

22 that context, “[a] strict test applies” and “[c]lassified information that a party seeks to obtain or

23 publish is deemed to have been officially disclosed only if it (1) is as specific as the information

24 previously released, (2) matches the information previously disclosed, and (3) was made public

25 through an official and documented disclosure.” *Wilson v. C.I.A.*, 586 F.3d 171, 186 (2d Cir.

26 2009) (internal quotation marks omitted) (quoting *Wolf*, 473 F.3d at 378); *see also Pickard*, 653

27 F.3d at 787 (construing official disclosure or confirmation as “an intentional, public disclosure

28 made by or at the request of a government officer acting in an authorized capacity by the agency in

1 control of the information at issue”).

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

19 2. Disclosure of Technique vs. Application of Known Technique

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

24 In *Rosenfeld*, the plaintiff sought information from the FBI about its investigation of free
25 speech protest movements on UC Berkeley’s campus. *Rosenfeld*, 57 F.3d at 806. The court
26 denied the FBI’s request to withhold under Exemption 7(E) information about the use of pretext
27 phone calls because such a tactic “would leap to the mind of the most simpleminded investigator.”
28

1 *Id.* at 815.⁸ Thus, the use of pretext phone calls was “generally known to the public.” *Id.* It
 2 rejected the FBI’s argument that the technique at issue was the application of the technique to a
 3 particular individual and not disclosable under Exemption 7(E). *Id.* The court explained: “If we
 4 were to follow such reasoning, the government could withhold information under Exemption 7(E)
 5 under any circumstances, no matter how obvious the investigative practice at issue, simply by
 6 saying that the ‘investigative technique’ at issue is not the practice but the application of the
 7 practice to the particular facts underlying that FOIA request.” *Id.*

8 In *Hamdan*, by contrast, Plaintiff sought information from multiple federal agencies
 9 regarding the role the United States might have played in his detention and torture by the
 10 government of the United Arab Emirates. *See Hamdan*, 797 F.3d at 767–69. The court found that
 11 the FBI properly withheld records “related to surveillance and credit searches” under Exemption
 12 7(E). It stated: “It is true that credit searches and surveillance are publicly known law
 13 enforcement techniques. But the affidavits say that the records reveal techniques that, if known,
 14 could enable criminals to educate themselves about law enforcement methods used to locate and
 15 apprehend persons. This implies a specific *means* of conducting surveillance and credit searches
 16 rather than an *application*.” *Id.* at 777–78 (second emphasis added). The court further contrasted
 17 a “means of conducting surveillance” with the example of “satellite surveillance of a particular
 18 place,” which would be an *application* of a known technique under *Rosenberg* [sic].” *Id.* at 778.

19 Under *Rosenfeld* and *Hamdan*, Exemption 7(E) cannot be used to withhold information
 20 about a technique that is generally known to the public when what is at issue is a specific
 21 application of that technique to a specific context. Conversely, Exemption 7(E) does protect
 22 specific means by which an agency uses a technique where the general technique is known, but the
 23

24 ⁸ *Albuquerque Pub. Co. v. U.S. Dep’t of Justice*, 726 F. Supp. 851 (D.D.C. 1989) contains similar
 25 language: “[W]e saw nothing exceptional or secret about the techniques . . . described—namely,
 26 the use of wired informants and ‘bugs’ secretly placed in rooms that are under surveillance.
 27 Anyone who is familiar with the media, both television and print, is aware that the police use these
 28 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.

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

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

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

- 17 a. Records concerning any product or service capable of using social media content in
- 18 assessing applications for immigration benefits or admission to the United States;
- 19 b. Records concerning any product or service capable of using social media content
- 20 for immigration enforcement purposes; and
- 21 c. Records concerning any product or service capable of using social media content
- 22 for border or transportation screening purposes.”

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

25
 26 _____
 27 ⁹ The FBI “has acknowledged generally [that] it monitors social media as a law enforcement
 28 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.

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

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

17 3. Disclosing the FBI’s Incapacity

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

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

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

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

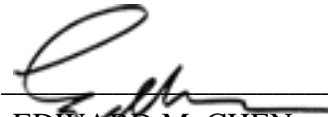
1 **IV. CONCLUSION**

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

4 This order disposes of Docket No. 31.

5
6 **IT IS SO ORDERED.**

7
8 Dated: November 18, 2019

9
10 
11 EDWARD M. CHEN
12 United States District Judge

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
United States District Court
Northern District of California