

1 JOSEPH HUNT
 Assistant Attorney General
 2 ELIZABETH SHAPIRO
 Deputy Director, Federal Programs Branch
 3 ELIZABETH TULIS
 Trial Attorney (NY Bar)
 4 AMY POWELL
 Trial Attorney (NY Bar)
 5 Department of Justice
 Civil Division, Federal Programs Branch
 6 1100 L Street, NW
 Washington, DC 20005
 7 T: 202-514-9237
 E: elizabeth.tulis@usdoj.gov
 8 *Attorneys for Defendants*

9
 10 UNITED STATES DISTRICT COURT
 11 NORTHERN DISTRICT OF CALIFORNIA
 12 SAN FRANCISCO DIVISION
 13

<p>14 AMERICAN CIVIL LIBERTIES UNION FOUNDATION, et al.,</p> <p>16 Plaintiffs,</p> <p>17</p> <p>18 v.</p> <p>19</p> <p>20 UNITED STATES DEPARTMENT OF JUSTICE, et al.,</p> <p>21</p> <p>22 Defendants.</p>	<p>Case No. 3:19-cv-00290-EMC</p> <p>DEFENDANT’S REPLY IN FURTHER SUPPORT OF MOTION FOR PARTIAL SUMMARY JUDGMENT WITH RESPECT TO FBI</p> <p>Hearing Date: Oct. 24, 2019 Time: 1:30 pm Place: Courtroom 5</p>
--	--

23
 24
 25
 26 **DEFENDANT DOJ’S REPLY IN FURTHER SUPPORT OF MOTION FOR
 PARTIAL SUMMARY JUDGMENT WITH RESPECT TO FBI**
 27
 28

TABLE OF CONTENTS

1 INTRODUCTION 1

2 ARGUMENT 1

3 I. The FBI Properly Invoked Exemption 7(E) to Protect Information

4 About a Law Enforcement Technique. 1

5 II. The Details Withheld Are Not Publicly Known 4

6 III. Although a Harm Showing is Not Required, FBI Has Shown a Risk of

7 Circumvention of the Law. 7

8 CONCLUSION..... 8

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

TABLE OF AUTHORITIES

Cases

ACLU v. CIA,
 710 F.3d 422 (D.C. Cir. 2013)..... 6

BuzzFeed, Inc. v. DOJ,
 344 F. Supp. 3d 396 (D.D.C. 2018)..... 4

Gardels v. CIA,
 689 F.2d 1100 (D.C. Cir. 1982)..... 7

Hamdan v. DOJ,
 797 F.3d 759 (9th Cir. 2017) 2, 3, 8

Hunt v. CIA,
 981 F.2d 1116 (9th Cir. 1992) 2

Janangelo v. Treasury Inspector Gen. for Tax Admin.,
 726 F. App’x 660 (9th Cir. 2018) 7

McCash v. CIA,
 No. 5:15-CV-02308-EJD, 2017 WL 1047022 (N.D. Cal. Mar. 20, 2017) 3

Pickard v. DOJ,
 653 F.3d 782 (9th Cir. 2011) 7

Reporters Comm. for Freedom of Press v. FBI,
 369 F. Supp. 3d 212 (D.D.C. 2019)..... 3, 4

Rosenfeld v. DOJ,
 57 F.3d 803 (9th Cir. 1995) 3

Wolf v. CIA,
 473 F.3d 370 (D.C. Cir. 2007)..... 7

INTRODUCTION

1
2 The Federal Bureau of Investigation (“FBI”) properly declined to confirm or deny the
3 existence of responsive documents to a subset of Plaintiffs’ request. FBI made this partial
4 Glomar response pursuant to Exemption 7(E) to protect information about a particular law
5 enforcement technique – namely, whether or not FBI has acquired software by which it analyzes
6 social media information related to immigration enforcement or transportation security.
7 Plaintiffs argue that this is just a “specific application” of social media analysis, but this is not a
8 known technique applied to a particular investigation, it is non-public information about the
9 technique in general. Plaintiffs primarily argue that this information is already public, but
10 Plaintiffs cannot establish that FBI has previously disclosed the details sought here. Plaintiffs
11 argue that FBI is already known to analyze social media in general, that FBI’s publicly-known
12 software may be capable of this already, and that other agencies are known to analyze social
13 media specifically for immigration purposes. None of these purported disclosures reveal the
14 precise information withheld here – whether FBI has acquired software unique to immigration
15 enforcement. Accordingly, Plaintiffs arguments fail, and the FBI is entitled to partial summary
16 judgment.

ARGUMENT

I. The FBI Properly Invoked Exemption 7(E) to Protect Information About a Law Enforcement Technique.

17
18
19
20 The FBI has established that the existence or nonexistence of responsive records related
21 to the acquisition of social media analytical tools for immigration enforcement or transportation
22 security is properly exempt from disclosure pursuant to Exemption 7(E). *See* FBI Mot. for
23 Partial Summ. J., at 6-10, ECF No. 31. Plaintiffs appear to concede, as they must, that this
24 would reveal information about a law enforcement technique.¹ Instead, they argue that the
25
26

27 ¹ Plaintiffs do not appear to contest the Glomar as specifically applied to the request for
28 “[r]ecords concerning any product or service capable of using social media content for border or

1 information revealed is a specific application of a known technique. Pls.' Opp'n at 16-18, ECF
2 No. 33. But this argument ignores both the explanation in the declaration and the plain language
3 of the request. The partial Glomar does not attempt to avoid disclosure of whether or FBI uses
4 its social media analysis capability in any particular case, and Plaintiffs fail to grapple with the
5 explanation provided by the FBI. The Seidel Declaration, which is entitled to substantial weight,
6 *see Hunt v. CIA*, 981 F.2d 1116, 1119 (9th Cir. 1992), takes into account that FBI has confirmed
7 its general use of social media for investigative purposes. Seidel Decl. ¶ 13, ECF No. 31-1 (“the
8 FBI has acknowledged generally it monitors social media as a law enforcement technique.”).
9 The Declaration explains that “[t]he use of such tools for immigration enforcement would imply
10 that the FBI is analyzing social media data in conjunction with immigration records or similar
11 data” and that confirming or denying the existence of records showing the FBI applies such
12 techniques specific to immigration enforcement or transportation would “reveal the fact that the
13 FBI has the capability, or lacks the capability, to employ tools to analyze data located on social
14 media platforms, in conjunction with immigration enforcement data, in furtherance of criminal or
15 national security investigations.” *Id.* ¶¶ 13, 18. This is not information about the use of social
16 media analysis in any particular case; rather, it shows a *specific means* of using social media.
17 The request, after all, is not for information about specific cases or categories of cases; it is a
18 request for records about acquisition of analytic tools that have specific *capabilities*. *See*
19 Request, Seidel Decl. Ex. A. Those capabilities, or lack thereof, are the techniques being
20 protected.

21 This is consistent with the case law in this Circuit. In *Hamdan*, the Ninth Circuit held
22 that an agency can withhold details about how it uses a tool, even if the existence of that tool is
23 publicly known. *Hamdan v. DOJ*, 797 F.3d 759, 777-78 (9th Cir. 2017). The Court held that
24 even though credit searches and surveillance are “publicly known law enforcement techniques,”

25
26
27 transportation screening purposes.” Accordingly, the Court should treat that portion of the
28 motion for summary judgment as conceded.

1 the FBI could properly withhold details of specific “techniques and procedures related to
2 surveillance and credit searches.” *Id.* at 777. Plaintiffs gloss over the facts of that case, but the
3 holding repudiates Plaintiffs’ central argument here—that FBI cannot withhold any information
4 about a generally known technique. Plaintiffs otherwise attempt to distinguish *Hamdan*, arguing
5 that it is not a Glomar case, *see* Pls.’ Opp’n at 17, but it is hard to see how that helps them. In
6 *Hamdan*, the request was for records about *particular individuals* and the FBI was nonetheless
7 able to withhold information about particular techniques as applied to those individuals because
8 it would reveal a “*specific means*” of using that technique rather than a specific application of
9 that technique. *Hamdan*, 797 F.3d at 777-78. Because the request was aimed at records about a
10 particular individual about whom FBI acknowledged having records, there was no need to
11 Glomar. Here, the request itself is aimed specifically at gathering more information about a law
12 enforcement technique in general, and a Glomar is necessary to avoid giving away the very
13 information to be protected. The information here is even more clearly protected by 7(E).

14 Plaintiffs instead rely heavily on *Rosenfeld*, where in 1995, the Ninth Circuit held that the
15 use of a “pretext phone call” in a particular case was a technique generally known to the public
16 and not subject to Exemption 7(E). *Rosenfeld v. DOJ*, 57 F.3d 803, 815 (9th Cir. 1995)
17 (citations omitted). The Circuit rejected the argument that the use of a pretext phone call in a
18 particular case was a fact which itself was entitled to protection under 7(E). *See id.* But here, as
19 in *Hamdan*, the specific application of a technique is not what is at issue; rather, the FBI is
20 protecting details about the specific means by which that technique is or is not used. *See*
21 *Hamdan*, 797 F.3d at 777-78); *McCash v. CIA*, No. 5:15-CV-02308-EJD, 2017 WL 1047022, at
22 *2 (N.D. Cal. Mar. 20, 2017).²

23
24 ² Plaintiffs also cite *Reporters Committee for Freedom of Press v. FBI*, 369 F. Supp. 3d 212
25 (D.D.C. 2019). In that case, the district court ultimately rejected the argument that the defendant
26 could refuse to confirm or deny the existence of records about FBI’s impersonation of
27 documentary filmmakers, because the court found that the technique was publicly known. *See*
28 *id.* at 223. The court also noted that it was “unclear how the impersonation of documentary
filmmakers as a whole can be a secret technique when the impersonation of news media is not,”
but did not decide this question and based its holding on the specific finding that the

1 Plaintiffs also argue that this case “differs fundamentally from others in which courts
2 have upheld” a Glomar based on 7(E) because such cases “typically involve circumstances in
3 which producing responsive records would reveal whether a specific individual is or was a
4 subject of [an] investigation.” Pls.’ Opp’n at 20. Certainly, FBI strongly protects records that
5 would identify subjects of investigations. Plaintiffs’ argument that courts have typically allowed
6 a Glomar under Exemption 7(E) where confirming the existence or non-existence of responsive
7 records would reveal whether or not a particular person is an investigative subject is in
8 considerable tension with Plaintiffs’ primary argument that 7(E) cannot protect specific
9 applications of law enforcement techniques. Indeed, the cases cited by Plaintiffs suggest that a
10 Glomar response is particularly appropriate when disclosure would reveal information about
11 specific individuals. But Plaintiffs’ argument that a Glomar under Exemption 7(E) is limited to
12 those circumstances is also wrong. While there is not a great deal of litigation regarding 7(E)
13 Glomar responses in any context, there is nothing in the statutory standard that would limit its
14 use as Plaintiffs suggest. *See, e.g., BuzzFeed, Inc. v. DOJ*, 344 F. Supp. 3d 396, 407 (D.D.C.
15 2018) (upholding 7(E) Glomar regarding FBI’s use of aerial surveillance).

16 **II. The Details Withheld Are Not Publicly Known.**

17 Plaintiffs argue that “[s]ocial media surveillance is a publicly known law enforcement
18 technique,” *see* Pls.’ Opp’n at 12-16, but the FBI has not maintained otherwise, and none of the
19 information put forward by Plaintiffs here discloses whether or not the FBI uses “social media
20 surveillance” in conjunction with immigration information, or in the context of transportation
21 security in furtherance of other investigations.

22 Most of the exhibits filed by Plaintiffs establish only that FBI sought and obtained the
23 capability to analyze social media content in the furtherance of its mission. *See* Pls.’ Exs. A, B,
24 C, D, E, ECF Nos. 34-1, 2, 3, 4, 5. FBI’s primary mission, however, does not include

25 _____
26 impersonation of filmmakers was specifically, publicly known. *Id.* Here, there is no plausible
27 allegation, let alone any factual showing, that use of social media analysis in conjunction with
28 immigration data is a publicly known FBI law enforcement technique.

1 immigration enforcement and certainly does not necessarily entail that FBI would be seeking to
2 monitor social media in conjunction with immigration information. Seidel Decl. ¶ 16. And
3 these documents do not reveal all details and capabilities with respect to these products. It bears
4 repeating that FBI is in fact searching for and processing documents like those cited by Plaintiffs
5 here – because their existence does not reveal whether or not FBI is using the application in
6 conjunction with immigration records.

7 Plaintiffs argue that these documents show “enterprise wide” capability to monitor or
8 analyze social media content and are not “limited to specific aspects of the FBI’s activities.”
9 Pls.’ Opp’n at 13-14. But the existence of general capability to analyze social media does not
10 reveal whether the specific capabilities at issue exist. Even if one could assume that FBI could
11 monitor social media related to every single investigation or category of investigations in its
12 jurisdiction, an assumption that is far from established, that would not reveal whether or not the
13 FBI did so specifically in conjunction with immigration information, or whether it possesses
14 records that concern a product or service with the specific capability of using social media
15 content for immigration enforcement purposes. The documents do not support a contrary
16 position. For example, Exhibit B is the Limited Source Justification for a requisition for a
17 “customizable detection and alerting functionality” related to “breaking news and events” on
18 Twitter, ECF No. 34-2 at 2, and it states that: “Dataminr’s Indicators and Warnings service . . .
19 provides access to . . . the full [Twitter] firehose and it will permit the FBI to design and apply
20 filters that are specifically tailored to operational needs” and “offers a reach back capability in
21 the event the FBI needs help creating a particular filter or has other technical issues.” *Id.* at 1-2.
22 This document shows that FBI sought the ability to filter and search the Twitter data stream, but
23 does not reveal what specific filters are used or whether they are cross-referenced with other
24 records or in what context. The subset of the request subject to the partial Glomar seeks
25 information specifically about whether FBI sought software with a specific capability. *See* Seidel
26
27
28

1 Decl., Exs. A, F. None of the documents on which Plaintiffs rely reveals whether or not that is
2 the case.³

3 Next, Plaintiffs argue that other agencies have acknowledged having the capability to
4 review social media in conjunction with immigration records. As Plaintiffs concede, however,
5 DHS components are responsible for securing the border and making immigration
6 determinations. And the State Department makes visa determinations. The FBI, in contrast, “is
7 the primary investigative agency of the federal government,” Seidel Decl. ¶ 15, and Plaintiffs
8 have pointed to no evidence that it is generally known to the public whether the FBI utilizes or
9 has sought to utilize products or services with the specific capabilities identified in items 2.a-c of
10 the Request. The fact that other agencies might review social media in conjunction with
11 immigration records for their own purposes does not reveal whether the FBI engages in such
12 activity as a law enforcement technique.

13 The *ACLU* case cited by Plaintiffs is inapposite. *See* Pls.’ Opp’n at 15 (citing *ACLU v.*
14 *CIA*, 710 F.3d 422, 430 (D.C. Cir. 2013)). That case involved the question of whether the CIA
15 had waived its ability to assert a Glomar response under Exemptions 1 and 3 through “official
16 acknowledgment.” *See ACLU*, 710 F.3d at 426. The D.C. Circuit concluded that the CIA could
17 not invoke a Glomar response to avoid confirming whether or not it had an “intelligence interest”
18 in drone strikes because that information had already been disclosed via statements by
19 government officials, including the CIA Director himself. *See id.* at 429-31. The case did not
20 concern the issue of whether a particular law enforcement technique was known to the general
21 public. Further, the case at no point suggested that, for purposes of the Exemption 7(E) analysis,
22 public knowledge of whether the FBI engages or does not engage in particular activities as a law
23

24
25 ³ Similarly, Exhibit D, a recent “Request for Proposal,” shows that FBI sought “social media
26 alerting” software that would permit “content filtering” that “supports prioritization; specific
27 subjects, identifiers, geographic location, keywords, photographic tagging.” ECF No. 34-4. It
28 makes no mention of the specific capabilities referenced in the relevant portions of Plaintiffs’
FOIA request.

1 enforcement technique could be established by showing that some other agency engages in the
2 activities in a different context.

3 Finally, it bears noting that Plaintiffs have not argued that FBI has waived Exemption
4 7(E) by officially acknowledging the information at issue, presumably because Plaintiffs cannot
5 meet the exacting standard for showing official acknowledgment. As the FBI explained in the
6 motion for partial summary judgment, an official acknowledgment requires that the information
7 requested be as specific as the information previously released, match the information previously
8 disclosed, and already have been made public through an official and documented disclosure.
9 *Pickard v. DOJ*, 653 F.3d 782, 785–86 (9th Cir. 2011); *Wolf v. CIA*, 473 F.3d 370, 374 (D.C.
10 Cir. 2007) (quoting *Gardels v. CIA*, 689 F.2d 1100, 1103 (D.C. Cir. 1982); *Janangelo v.*
11 *Treasury Inspector Gen. for Tax Admin.*, 726 F. App'x 660, 661 (9th Cir. 2018)). The FBI has
12 not confirmed or denied the use of social media analytical tools in conjunction with immigration
13 data, immigration enforcement, or transportation security, and none of the previously discussed
14 disclosures comes close to meeting the official acknowledgment standard.

15 **III. Although a Harm Showing Is Not Required, FBI Has Shown a Risk of**
16 **Circumvention of the Law.**

17 Plaintiffs concede that Exemption 7(E), as applied to law enforcement techniques, does
18 not require a showing of risk of circumvention of the law. Pls.' Opp'n at 12 n.40. Plaintiffs
19 nonetheless argue that "FBI's predictions of the consequences of processing the Request
20 misapprehend the nature of online speech." Pls.' Opp'n at 18-20. While Plaintiffs' discussion of
21 this issue is beside the point, it is also wrong.

22 First, Plaintiffs' suggestion that a First Amendment right to refrain from speech is
23 relevant to whether disclosure of a law enforcement technique or procedure might cause harm
24 equates First Amendment rights with a right to circumvent the law. *See* Pls.' Opp'n at 19-20. The
25 general right of individuals to speak or not does not preclude the FBI from taking steps to avoid
26 alerting criminals to ways to structure their criminal behavior to avoid detection by law
27 enforcement.

1 Second, though no showing of harm is necessary for Exemption 7(E) to apply, the FBI's
2 declarant explained in detail, confirming or denying the existence or non-existence of records
3 responsive to parts 2.a-c of the Request would alert criminals and foreign adversaries whether or
4 not the FBI uses a particular investigative means, and would thereby help such criminals and
5 foreign adversaries to structure their unlawful activities to avoid investigative scrutiny. Seidel
6 Decl. ¶¶ 20-22.

7 Contrary to Plaintiffs' bald assertion, Pls.' Opp'n at 21, the declarant's explanation of the
8 bases for the FBI's Glomar response is not "conclusory," and, as the matter before the Court
9 involves national security issues, the declaration is entitled to "substantial weight." *See Hamdan*,
10 797 F.3d at 769.

11 **CONCLUSION**

12 For the foregoing reasons, the Court should grant partial summary judgment for the FBI.

13
14 Dated: September 27, 2019

Respectfully Submitted,

15 JOSEPH HUNT
16 Assistant Attorney General

17 ELIZABETH SHAPIRO
18 Deputy Director, Federal Programs Branch

19 /s/ _____
20 ELIZABETH TULIS
21 AMY E. POWELL
22 U.S. Department of Justice, Civil Division
23 1100 L Street, NW
24 Washington, DC 20005
25 Phone: 202-514-9237
26 Email: elizabeth.tulis@usdoj.gov

27 *Attorneys for Defendants*
28