HUGH HANDEYSIDE (*pro hac vice*)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: 212-549-2500
Fax: 212-549-2583
hhandeyside@aclu.org

MATTHEW CAGLE (CA Bar No. 286101)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: 415-621-2493
Fax: 415-255-1478
mcagle@aclunc.org

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO-OAKLAND DIVISION

AMERICAN CIVIL LIBERTIES UNION FOUNDATION, *et al.*,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 19-CV-00290-EMC

PLAINTIFFS' OPPOSITION TO DEFENDANT'S MOTION FOR PARTIAL SUMMARY JUDGMENT

Hearing date: October 17, 2019
Time: 1:30 p.m.
Courtroom: 5
Judge: Hon. Edward M. Chen

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

This case concerns the federal government's use of powerful tools to monitor the speech of U.S. citizens and noncitizens on various social media platforms. Surveillance of social media is a major priority for numerous federal agencies, which have expended millions of dollars on technology that searches and scrapes the social media web for purposes that include criminal investigation, intelligence gathering, visa processing, immigration benefits and enforcement, and border screening. The reach of this kind of surveillance is global—it can affect anyone domestically or abroad who uses social media—its consequences can be severe, and it risks chilling people's expression of dissent or disfavored views.

Because the public has a vital interest in understanding the policies that govern social media surveillance and the tools that the federal government uses to conduct it, Plaintiffs American Civil Liberties Union Foundation and American Civil Liberties Union Foundation of Northern California (together, the "ACLU") submitted requests for records under the Freedom of Information Act ("FOIA") to seven federal agencies, including the Federal Bureau of Investigation ("FBI"). Plaintiffs filed this lawsuit after the agencies failed to respond as FOIA requires.

In moving for partial summary judgment, the FBI acknowledges, as it must, that it engages in surveillance of social media. Yet it argues that it cannot disclose whether it conducts such surveillance for certain purposes: immigration benefits determinations, immigration enforcement, and border and transportation screening. According to the FBI, confirming the existence or nonexistence of records relevant to those purposes would reveal the extent of the FBI's capabilities, which it claims are exempt from disclosure under FOIA, and enable people to evade investigation.

This "Glomar" assertion is fundamentally illogical and improper. Processing the disputed parts of the FOIA request and producing responsive documents would not reveal any law enforcement technique or procedure that is exempt from disclosure under FOIA, because social media surveillance is a publicly known technique. The FBI and other federal agencies have openly and repeatedly disclosed their use of social media surveillance for an array of purposes.

Having made public its wide-ranging interest in, and use of, social media surveillance, the FBI cannot now use a Glomar assertion to attempt an end-run around FOIA and the transparency obligations it imposes.

Ultimately, the FBI's motion amounts to an acknowledgment that if people knew the extent to which the government is monitoring what they say on social media, they would be less likely to say things of interest to the FBI. But the scope of government monitoring is no great mystery. Given the FBI's own public disclosures and those of other federal agencies, anyone actually seeking to violate the law already knows that law enforcement agencies monitor social media. At the same time, the unfortunate consequence of that surveillance for the broader public is self-censorship and a chilling effect on constitutionally protected expression and association.

FOIA is a bulwark against excessive government secrecy, not a means of perpetuating an implausible fiction of deniability. The FBI's motion is meritless and should be denied.

STATEMENT OF FACTS

I. The FBI's "Enterprise Wide" Use Of Social Media Surveillance

The FBI has long monitored and analyzed social media content for wide-ranging purposes. In 2012, the FBI issued a public Request for Information from contractors on a "social media application" that would enable the FBI to "instantly search and monitor" information on social media platforms.[1] The agency required that the application be "infinitely flexible" such that it could "support a myriad of functional FBI missions" and "provide an automated search and scrape capability of both social networking sites and open source news sites."[2] The FBI later notified the public of its "intent to procure the Geofeedia social media monitoring platform," which it stated "is also a location, analysis and engagement based platform."[3]

The FBI revealed in November 2016 that it would acquire software designed by

---

[1] FBI, Strategic Info. & Operations Ctr., *Request for Information – Social Media Application* 3 (Jan. 19, 2012), attached as Ex. A to the Declaration of Hugh Handeyside ("Handeyside Decl.").

[2] *Id.* at 1, 3.

[3] FBI, *Social Media Monitoring Platform*, Solicitation No. DJF-15-3150-PR-0028925 (Sept. 15, 2015), https://goo.gl/zEuG4W.

Dataminr, a firm that, according to the FBI, was "able to provide the mission critical social media monitoring needed by the FBI."[4] In justifying the acquisition, the FBI stated that it "needs near real time access to the full universe of tweets on a daily basis in order to obtain the most current information available in furtherance of its law enforcement and intelligence missions."[5] The FBI stated that the Dataminr software would enable it to "search the complete Twitter firehose, in near real time, using customizable filters" that are "specifically tailored to operational needs" and that "track FBI investigative priorities."[6]

Similarly, in a July 2019 public contract solicitation, the FBI stated that "[t]he mission-critical exploitation of social media enables the Bureau to proactively detect, disrupt, and investigate an ever growing diverse range of threats."[7] It again stated that it "needs near real time access to a full range of social media exchanges in order to obtain the most current information available in furtherance of its law enforcement and intelligence missions,"[8] and it sought proposals for a "social media early alerting tool in order to mitigate multifaceted threats."[9] "The need for social media," the FBI stated, is "Enterprise wide"—*i.e.*, across the agency—as employees in "each division and field office . . . are set on a Social Media Exploitation mission to address a broad range of threats."[10] The FBI indicated that the tool it sought through the solicitation must provide Bureau users with notifications "derived from constant monitoring of

---

[4] FBI, *Limited Source Justification*, Solicitation No. DJF-17-1300-PR00000555, at 4 (Nov. 8, 2016), attached as Ex. B to Handeyside Decl.

[5] FBI, Counterterrorism Div. – Exploitation Threat Section, *Request for Quote – Social Media Awareness and Monitoring Licenses*, Solicitation No. DJF-17-1300-PR-0000555, at 3 (Nov. 8, 2016), attached as Ex. C to Handeyside Decl.

[6] Ex. B, *supra* note 4, at 1.

[7] FBI, *Social Media Alerting Statement of Objectives*, Solicitation No. DJF-194750PR0000369, at 2 (July 8, 2019), attached as Ex. D to Handeyside Decl.

[8] FBI, *Request for Proposal – Social Media Alerting*, Solicitation No. DJF-194750PR0000369, at 5 (July 8, 2019), attached as Ex. E to Handeyside Decl.

[9] FBI, *Social Media Alerting Subscription*, Solicitation No. DJF-194750PR0000369 (July 8, 2019), https://t.ly/knyNq.

[10] Ex. D, *supra* note 7, at 2.

social media platforms based on keywords relevant to national security and location," and must be capable of filtering information according to "specific subjects, identifiers, geographic location, keywords, [and] photographic tagging."[11] It also required that the software enable FBI users to "[o]btain the full social media profile of persons-of-interest and their affiliation to any organization or groups through the corroboration of multiple social media sources."[12]

Federal spending records also reflect the FBI's acquisition of various software tools for social media monitoring and analysis.[13]

II. Other Federal Agencies' Use Of Social Media Surveillance For Screening And Vetting

The State Department, the Department of Homeland Security ("DHS"), and DHS components have repeatedly notified the public that they collect, analyze, and often retain social media content for various purposes, including immigration benefits determinations, immigration enforcement, and border and transportation screening ("enumerated purposes").

A. State Department

The State Department has vastly expanded its collection of social media information in recent years for the express purpose of immigration admissions vetting. As of early 2016, it was operating a social media screening pilot program at seventeen diplomatic posts for certain immigrant visas.[14] In May 2017, it submitted a notice that it would collect, *inter alia*, social media identifiers—*i.e.*, names, handles, or other identifiers used to create an account or screen

---

[11] *Id.* at 4.

[12] *Id.* at 5.

[13] *See, e.g.*, USASpending, https://www.usaspending.gov/#/award/13087064 (award to The Mitre Corporation for "social media image fingerprinting project"); USASpending, https://www.usaspending.gov/#/award/13094285 (award to Pen-Link, Ltd. for software that "parses and analyzes social media data"); USASpending, https://www.usaspending.gov/#/award/81987472 (award to Magnet Forensics USA, Inc. for tool used "to extract social media footprint and related activities from digital evidence").

[14] *Crisis of Confidence: Preventing Terrorist Infiltration Through U.S. Refugee and Visa Programs: Hearing Before the H.R. Comm. On Homeland Sec.*, 114th Cong. 7 (2016) (written statement of Michelle Bond, Assistant Secretary for Consular Affairs), attached as Ex. F to Handeyside Decl.

name—from approximately 65,000 visa applicants each year.[15] Less than a year later, in March 2018, the department published two notices of new rules requiring nearly all of the approximately 14.7 million people who annually apply for work or tourist visas to submit social media identifiers they have used in the past five years on up to 20 online platforms in order to travel or immigrate to the United States.[16] The State Department's collected social media information is stored in the Consular Consolidated Database, which feeds into the Automated Targeting System, a database that DHS uses for a variety of immigration-and border-related purposes.[17]

B. Department of Homeland Security

DHS and its components, including Defendants in this case charged with immigration admissions, immigration enforcement, and transportation screening, routinely collect and monitor social media content. In documents produced in this lawsuit, DHS states that it "has been at the forefront among Federal agencies in developing the capability to incorporate social media data in its screening and vetting processes," and that the DHS Office of Science and Technology "has been developing tools and processes towards realizing DHS's long term objective of deploying screening capabilities related to social media."[18] In 2015, DHS convened a "Social Media Vetting Task Force" to examine the department's "current and future use of social media in the DHS vetting process for operational and intelligence purposes."[19] A February

---

[15] Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 20,956 (May 4, 2017); *see also* 60-Day Notice of Proposed Information Collection: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 36,180 (Aug. 3, 2017).

[16] 60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration, 83 Fed. Reg. 13,806 (Mar. 30, 2018); *see also* 60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa, 83 Fed. Reg. 13,807 (Mar. 30, 2018).

[17] DHS, Privacy Impact Assessment for the Automated Targeting System 35-37 (Jan. 13, 2017), attached as Ex. P to Handeyside Decl.

[18] Email from [redacted] to [redacted], Jan. 2, 2018, attached as Ex. G to Handeyside Decl.

[19] Email from David J. Palmer, DHS Associate General Counsel, to multiple recipients, Dec. 17, 2015, attached as Ex. H to Handeyside Decl.

2017 report by the DHS Inspector General also noted the establishment within DHS of a "Shared Social Media Screening Service" and the planned "department-wide use of social media screening."[20] The same report confirmed DHS's use of manual and automated social media screening of immigration and visa applications.[21]

Each major DHS component—including the Defendants in this case—has incorporated social media monitoring and analysis into its operations.[22] In September 2016, U.S. Customs and Border Protection ("CBP") began asking citizens and nationals of countries participating in the Visa Waiver Program to provide social media identifiers before traveling to the United States.[23] CBP has made clear that any such information "may be used for national security and law enforcement purposes," and that if an applicant chooses not to provide social media information as part of an application, 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."[24] Separately, CBP uses "publicly available search engines and content aggregators" to "monitor[] content on social media sites for information that informs Agency situational awareness."[25] In recent years, CBP has awarded contracts to procure licenses

---

[20] DHS, Office of Inspector General, OIG-17-40, DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success 1 n.2, 4 (2017) ("DHS OIG Report"), attached as Ex. I to Handeyside Decl.

[21] *Id.* at 1; *see also* DHS, Agency Information Collection Activities: Generic Clearance for the Collection of Social Media Information on Immigration and Foreign Travel Forms, 84 Fed. Reg. 46,557, 46,558 (Sept. 4, 2019) ("DHS currently uses publicly available social media information to support its vetting and adjudication programs, and to supplement other information and tools that DHS trained personnel regularly use in the performance of their duties.").

[22] *See* Ex. G, *supra* note 18 ("CBP, ICE, TSA and USCIS have been developing, testing, and operationalizing the use of social media in various pilots and programs.").

[23] DHS, Privacy Compliance Review of the U.S. Customs and Border Protection Electronic System for Travel Authorization 1 (2017), attached as Ex. J to Handeyside Decl.

[24] *Id.*

[25] DHS, Privacy Impact Assessment for the Publicly Available Social Media Monitoring and Situational Awareness Initiative 1 (Mar. 25, 2019), attached as Ex. K to Handeyside Decl.

for software that performs social media monitoring and analytics.[26]

U.S. Immigration and Customs Enforcement ("ICE") uses social media surveillance extensively for the enforcement of immigration laws in coordination with the FBI and other Defendants. According to documents ICE produced in this lawsuit, ICE established an "Open Source Team" in September 2014.[27] ICE describes the unit as "the first Program within ICE to leverage open source/social media exploitation 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."[28] Under a separate "Social Media pilot program" initiated in August 2016, ICE conducts constant monitoring of visitors' social media:

> The premise of this initiative is to track non-immigrants from the time they file a visa application with the Department of State, to the time they enter the United States, and through the time when they either depart the United States, or until such time as they become an overstay or otherwise fail to comply with the terms of admission.[29]

If, during this surveillance, ICE "uncovers derogatory information about a visa applicant," it coordinates with CBP and the State Department for follow-up action.[30] If the applicant has already entered the United States, ICE analysts request an investigation that is "coordinated through the Joint Terrorism Task Force ('JTTF')."[31] JTTFs are administered by the FBI.[32]

---

[26] *See, e.g.*, USASpending, https://www.usaspending.gov/#/award/23784019 (award to Thundercat Technology, LLC for social media monitoring software licenses); *see also* USASpending, https://www.usaspending.gov/#/award/68617237 (award to Panamerica Computers, Inc. for similar licenses).

[27] DHS, Homeland Security Investigations, Shared Services for Vetting Board Recommendation 2 (undated), attached as Ex. L to Handeyside Decl.

[28] *Id.*

[29] *Id.*

[30] DHS, Homeland Security Investigations, Extreme Vetting – Visa Security Program – PATRIOT 3 (undated), attached as Ex. M to Handeyside Decl.

[31] *Id.*

[32] *See* FBI, Joint Terrorism Task Forces, https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces. Federal records also show that ICE has spent millions of dollars on contracts with social media analytics and data mining firm Giant Oak. *See, e.g.*, USASpending, https://www.usaspending.gov/#/award/67807277 (award for open source/social media data

U.S. Citizenship and Immigration Services ("USCIS") collects and evaluates social media for various immigration screening-related purposes. The Fraud Detection and National Security ("FDNS") Directorate within USCIS has maintained a Social Media Division since 2014 that conducts "enhanced FDNS review" for certain asylum and refugee applicants.[33] USCIS also established five separate pilot programs for expanded social media screening of immigration applicants.[34] During the course of immigration benefits determinations, FDNS searches and can collect information on applicants from social media platforms or commercial data brokers.[35] Content collected through these initiatives—including "social media handles, aliases, associated identifiable information, and search results"—can be retained in the Alien Files system, which USCIS maintains and CBP and ICE can access.[36]

The Transportation Security Administration ("TSA") also participates in DHS's "department-wide use of social media screening."[37] TSA is a member of the DHS Social Media Working Group, "an inter-agency initiative aimed at the coordination of social media screening efforts," and as of early 2018 TSA, along with other DHS components, was "developing, testing, and operationalizing the use of social media in various pilots and programs."[38] According to public FBI contract documents, TSA also obtained Dataminr licenses for social media monitoring, based on "the unique relationship between Twitter and Dataminr as well as

---

analytics); USASpending, https://www.usaspending.gov/#/award/66685141 (similar award).

[33] *Refugee Admissions FY 2018: Hearing Before the Subcomm. on Immigration and Border Sec. H. Comm. on the Judiciary*, 115th Cong. (2017) (written testimony of L. Francis Cissna, Director, USCIS), https://t.ly/xyAn9.

[34] Ex. I, *supra* note 20, at 2, 7-8. The DHS Inspector General concluded that the pilot programs lacked "measurement criteria" and were "of limited use in planning and implementing an effective, department-wide future social media screening program." *Id.* at 2.

[35] DHS, Privacy Impact Assessment for the Fraud Detection and National Security Data System (FDNS-DS) 4, 14-16 (May 18, 2016), attached as Ex. N to Handeyside Decl.

[36] DHS, Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,557 (Sept. 18, 2017).

[37] *See* Ex. I, *supra* note 20, at 1.

[38] Ex. G, *supra* note 18.

Dataminr's ability to provide near real-time access to the full Twitter firehose."[39]

III. Procedural Background

To provide the public with information about the policies and guidance governing social media surveillance, the tools agencies use to conduct it, and its consequences for citizens and non-citizens, the ACLU submitted a FOIA request ("Request") on May 24, 2018 to seven federal agencies, including the FBI. *See* Decl. of Michael G. Seidel (Sept. 9, 2019), ECF No. 31-1 ("Seidel Decl.") at 15. Among other records, the Request sought:

> 2) All records created since January 1, 2015 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;
>
> c. Records concerning any product or service capable of using social media content for border or transportation screening purposes;
>
> d. Records concerning any product or service capable of using social media content in the investigation of potential criminal conduct;

Id. at 20-21.

In correspondence dated June 8, 2018, the FBI acknowledged receipt of the Request and stated that "upon reviewing the substantive nature of your request, we can neither confirm nor deny the existence of records responsive to your request pursuant to FOIA exemption (b)(7)(E) [5 U.S.C. §522 (b)(7)(E)]." *Id.* at 31. On July 18, 2018, the ACLU administratively appealed this "Glomar" response to all requested records. *Id.* at 36-41. The Department of Justice (DOJ) Office of Information Policy (OIP) acknowledged receipt of the appeal on July 23, 2018 and denied the ACLU's request for expedited processing of the appeal. *Id.* at 63.

Having received no further response to the administrative appeal, or any records from the

---

[39] Ex. B, *supra* note 4, at 4 (footnote omitted).

other agencies, the ACLU filed this lawsuit on January 17, 2019. *See* Complaint, ECF No. 1.

In correspondence dated January 31, 2019, OIP stated that it had granted the appeal and remanded the Request "back to the FBI for a search for responsive records." ECF No. 31-1 at 66. The FBI notified the ACLU in a letter dated May 31, 2019 that it would process portions of the Request. *Id.* at 69. It nonetheless stated it would assert a Glomar response for certain records:

> In regards to items 2) – a., b., and c. of your request, the FBI can neither confirm nor deny the existence of any responsive records. To do so would disclose the existence or non-existence of non-public law enforcement techniques, procedures, and/or guidelines. The acknowledgment that any such records exist or do not exist could reasonably be expected to risk circumvention of the law. Thus, pursuant to FOIA Exemption (b)(7)(E) [5 U.S.C.§552 (b)(7)(E)], the FBI neither confirms nor denies the existence of records responsive to these particular portions of your request.

Id. The Court subsequently directed the parties to submit partial summary judgment briefing to determine whether the FBI should process parts 2(a), 2(b), and 2(c) of the Request. ECF No. 26.

LEGAL FRAMEWORK

I. The Freedom of Information Act

Congress enacted FOIA to "pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny." *Muchnick v. Dep't of Homeland Sec.*, 225 F. Supp. 3d 1069, 1072 (N.D. Cal. 2016) (quoting *Dep't of State v. Ray*, 502 U.S. 164, 173 (1991). "The basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 152 (1989) (citation omitted). The Supreme Court has observed that "[w]ithout question, [FOIA] is broadly conceived" and is animated by a "philosophy of full agency disclosure." *Id.* (quoting *Envtl. Prot. Agency v. Mink*, 410 U.S. 73, 80 (1973) and *Dep't of Air Force v. Rose*, 425 U.S. 352, 360-61 (1976)). It therefore sets a "strong presumption in favor of disclosure." *Ray*, 502 U.S. at 173.

Consistent with that presumption, FOIA exemptions are "explicitly made exclusive and must be narrowly construed." *Milner v. Dep't of Navy*, 562 U.S. 562, 565 (2011) (citations and internal quotation marks omitted). The government always bears the burden to show that records are subject to an exemption and can be withheld. 5 U.S.C. § 552(a)(4)(B); *Rosenfeld v. Dep't of*

Justice, 57 F.3d 803, 808 (9th Cir. 1995).

II. The Glomar Response

"Glomar responses are an exception to the general rule that agencies must acknowledge the existence of information responsive to a FOIA request and provide specific, non-conclusory justifications for withholding that information." *Roth v. Dep't of Justice*, 642 F.3d 1161, 1178 (D.C. Cir. 2011) (citation omitted). Courts therefore only uphold an agency's Glomar response when confirming or denying the existence of records "would cause harm cognizable under a FOIA exception." *Pickard v. Dep't of Justice*, 653 F.3d 782, 786 (9th Cir. 2011) (quoting *Wolf v. Cent. Intelligence Agency*, 473 F.3d 370, 374 (D.C. Cir. 2007)). In determining whether information revealing the existence or non-existence of records falls into a FOIA exemption, "courts apply the general exemption review standards established in non-*Glomar* cases." *Wolf*, 473 F.3d at 374 (citation omitted). Thus, "an agency's justification for invoking a FOIA exemption, whether directly or in the form of a *Glomar* response, is sufficient if it appears logical or plausible." *Am. Civil Liberties Union v. Cent. Intelligence Agency*, 710 F.3d 422, 427 (D.C. Cir. 2013) (citing *Wolf*, 473 F.3d at 374-75) (internal quotation marks omitted).

As with a conventional FOIA response, an agency asserting a Glomar response bears the burden of proving that an exemption applies. *Am. Civil Liberties Union v. Dep't of Defense*, 322 F. Supp. 3d 464 (S.D.N.Y. 2018). A Glomar response will be justified only in "unusual circumstances and only by a particularly persuasive affidavit." *Florez v. Cent. Intelligence Agency*, 829 F.3d 178, 182 (2d Cir. 2016).

III. FOIA Exemption (b)(7)(E)

FOIA Exemption 7(E) protects from disclosure:

> [R]ecords 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.

5 U.S.C. § 552(b)(7)(E). It is well-settled that exemption 7(E) "only exempts investigative techniques not generally known to the public." *Am. Civil Liberties Union of N. Cal. v. Dep't of*

Justice, 880 F.3d 473, 491 (9th Cir. 2018) (citing *Rosenfeld v. Dep't of Justice*, 57 F.3d 803, 815 (9th Cir. 1995). Similarly, "[i]f an agency record discusses 'the application of [a publicly known technique] to ... particular facts,' the document is not exempt under 7(E)." *Id.* (quoting *Rosenfeld*, 57 F.3d at 815).

Thus, the FBI bears the burden of demonstrating that it is logical or plausible that confirming the existence or nonexistence of social media surveillance records would (1) "disclose techniques and procedures for law enforcement investigations or prosecutions" that are not generally known to the public, or (2) "disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." *See* 5 U.S.C. § 552(b)(7)(E).[40] The FBI has not met its burden here.

ARGUMENT

I. The FBI's Glomar Assertion Is Improper Because It Is Neither Logical Nor Plausible.

The federal government's monitoring and surveillance of social media in a variety of contexts—including for the enumerated purposes—is widely known. Because the FBI and other federal agencies have repeatedly disclosed their use of social media surveillance, it is wholly illogical for the FBI to assert that confirming the existence or non-existence of records in response to the Request would disclose a law enforcement technique or procedure.

A. Social media surveillance is a publicly known law enforcement technique.

The starting point for any analysis of FOIA exemptions is the language of the statute. *See Pickard*, 653 F.3d at 787 ("A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning.") (quoting *Perrin v. United States*, 444 U.S. 37, 42 (1979)). The language of exemption 7(E) is unambiguous: it applies only where the production of records "would disclose techniques and procedures for law enforcement investigations or prosecutions." 5 U.S.C. §

[40] The Ninth Circuit has held that the "circumvention of the law" component of exemption 7(E) applies only to "guidelines for law enforcement investigations or prosecutions." *See Hamdan v. Dep't of Justice*, 797 F.3d 759, 778 (9th Cir. 2015).

552(b)(7)(E).

No such disclosure of techniques or procedures would occur merely if the FBI processes the Request, because the FBI and the other Defendants have already disclosed, openly and repeatedly, their use of social media surveillance as a multi-faceted technique. *See Rosenfeld*, 57 F.3d at 815 ("It would not serve the purposes of FOIA to allow the government to withhold information to keep secret an investigative technique that is routine and generally known."). As set forth above, the FBI has acknowledged on numerous occasions that it engages in wide-ranging surveillance of social media content and that it considers such surveillance a critical part of its operations. As early as 2012, the FBI was broadcasting its need for a "social media application" to "instantly search and monitor" social media content.[41] It later notified the public that it would obtain Dataminr software that would provide "the mission critical social media monitoring needed by the FBI."[42] It again labeled the "constant monitoring of social media platforms" and "exploitation of social media" as "mission-critical" in July 2019—one year after its full Glomar response to the Request and just over a month after the partial Glomar response it continues to assert.[43]

Notably, 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. The social media application it contracted for in 2012 had to be "infinitely flexible" and "support a myriad of functional FBI missions."[44] The Dataminr software the FBI acquired in 2016 was "in furtherance of its law enforcement and intelligence missions"[45]—the full gamut of FBI activities. The FBI required that the software enable it to use "customizable filters . . . specifically tailored to operational needs" and be able to "track FBI investigative

---

[41] Ex. A, *supra* note 1, at 3.

[42] Ex. B, *supra* note 4, at 4.

[43] Ex. D, *supra* note 7, at 2, 4.

[44] Ex. A, *supra* note 1, at 1.

[45] Ex. C, *supra* note 5, at 3.

priorities."[46] The FBI went even further in its July 2019 contract documentation, stating that "[t]he need for social media . . . [is] Enterprise wide" and that employees in "*each division and field office* . . . are set on a Social Media Exploitation mission to address a broad range of threats."[47]

These all-encompassing disclosures regarding the FBI's "exploitation of social media" render implausible its basis for the Glomar response. Nevertheless, Defendant's declarant states that revealing whether the FBI has responsive records

> would itself reveal the fact that the FBI has the capability, or lacks the capability, to employ tools to analyze data located on social media platforms, in conjunction with immigration enforcement data, in furtherance of criminal or national security investigations; and the fact that the FBI has the capability, or lacks the capability, to employ tools to analyze data located on social media platforms in transportation screening.

Seidel Decl. ¶ 18, ECF No. 31-1 at 9. The FBI's contract specifications, however, make clear that the FBI has that capability.[48] Moreover, as Defendant's declarant acknowledges, "if the FBI were to deploy tools in the specific setting of analyzing social media data in conjunction with immigration enforcement data, it would be doing so in furtherance of its law enforcement, national security, or intelligence gathering missions." *Id.* ¶ 16, ECF No. 31-1 at 8. Those are precisely the "missions" for which the FBI has repeatedly stated that it conducts social media surveillance.[49]

The federal government's use of social media surveillance for the enumerated purposes is also well-known—a fact that underscores the illogic of the FBI's position. An array of public sources confirm that DHS, its components, and the State Department conduct social media screening for visa processing, immigration benefits determinations, immigration enforcement,

---

[46] Ex. B, *supra* note 4, at 1.

[47] Ex. D, *supra* note 7, at 2 (emphasis added).

[48] *See, e.g.*, Ex. B, *supra* note 4, at 1 (requiring "customizable filters . . . specifically tailored to operational needs"); Ex. D, *supra* note 7, at 4 (requiring filtering according to "specific subjects, identifiers, geographic location, keywords, [and] photographic tagging").

[49] *See* Ex. A, *supra* note 1, at 1; Ex. C, *supra* note 5, at 3; Ex. E, *supra* note 8, at 5.

and border and transportation screening.[50] It is telling that none of the other Defendants in this lawsuit—including Defendants directly responsible for immigration benefits determinations (USCIS), immigration enforcement (ICE), and border and transportation screening (CBP)—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. It is clear, moreover, that the FBI cooperates extensively with these agencies on issues involving the enumerated purposes.[51] The pervasive use of social media monitoring for these purposes leaves no doubt that that it is a "routine and generally known" technique. *See Rosenfeld*, 57 F.3d at 815.

Notably, exemption 7(E) does not 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. In other words, the FBI may not evade FOIA's mandate by arguing that the application of a particular technique *by the FBI* has not been disclosed, where the use of that technique by other federal agencies is plainly a matter of public record. *Cf. Am. Civil Liberties Union v. Cent. Intelligence Agency*, 710 F.3d 422, 430 (D.C. Cir. 2013) ("*ACLU*") (concluding, in case involving exemptions (b)(1) and (b)(3), that "[g]iven these official acknowledgments that the United States has participated in drone strikes, it is neither logical nor plausible for the CIA to maintain that it would reveal anything not already in the public domain to say that the Agency 'at least has an intelligence interest' in drone strikes").

Abundant public information confirms that social media surveillance, including for the

---

[50] *See, e.g.*, *supra* notes 16 (visa and immigration processing), 19 (DHS vetting), 21 (immigration and visa applications), 23 (Visa Waiver Program vetting), 25 ("situational awareness" at the border), 29 (visa life cycle vetting), 37 (immigration benefits determinations), 40 (transportation security).

[51] *See, e.g.*, Dep't of Justice Inspector General & DHS Inspector General, A Joint Review of Law Enforcement Cooperation on the Southwest Border between the Federal Bureau of Investigation and Homeland Security Investigations (July 2019), attached as Ex. O to Handeyside Decl., at 12 (describing "joint casework," including "HSI assisting the FBI with immigration-related issues"), 26 (FBI cooperation with ICE's Enforcement and Removal Operations), 28 ("The FBI and HSI also have [memoranda of understanding] governing . . . information sharing from DHS alien information databases.").

enumerated purposes, is a generally known law enforcement technique. This is fatal to the FBI's motion.

B. The FBI may not use a Glomar response to conceal specific applications of its use of social media surveillance.

The crux of the FBI's argument in support of the Glomar response is that parts 2(a) – (c) of the Request "seek records about tools for analyzing social media data in conjunction with a specific type of enforcement action: *immigration enforcement*." Seidel Decl. ¶ 13, ECF No. 31-1 at 6; Def.'s Notice & Mot. for Partial Summary Judgment ("Def.'s Mot."), ECF No. 31 at 13. And "[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." Def.'s Mot., ECF No. 31 at 13.

Rosenfeld forecloses that argument. In that case, the Ninth Circuit affirmed the district court's ruling that the law enforcement technique at issue—a pretext phone call—is "an investigative technique generally known to the public" and therefore not subject to exemption (b)(7)(E). 57 F.3d at 815. In so holding, the court rejected the government's argument that the relevant technique was a more specific one: the use of the identity of a particular individual for the pretext phone call. *Id.* The court observed, "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.*

Here, the FBI is similarly seeking to withhold information about the application of what it acknowledges is a known technique (social media surveillance) to specific circumstances (the enumerated purposes). *See* Seidel Decl. ¶ 18, ECF No. 31-1 at 9 ("While the FBI has acknowledged it reviews social media information when generally pursuing its law enforcement duties, it has not confirmed use of the generally known technique in the specific setting sought by Plaintiffs herein."). That argument is as flawed as it was in *Rosenfeld*, and it cannot be

squared with exemption (b)(7)(E) or the narrow construction that must be applied to it.

Courts have rejected the FBI's attempts to invoke exemption (b)(7)(E) by obscuring a publicly known technique by referencing its specific application. For instance, the U.S. District Court for the District of Columbia recently held that the FBI could not validly issue a Glomar response under exemption (b)(7)(E) regarding the impersonation of documentary filmmakers, reasoning that it is "unclear how the impersonation of documentary filmmakers as a whole can be a secret technique when the impersonation of news media is not." *Reporters Comm. for Freedom of Press v. Fed. Bureau of Investigation*, 369 F. Supp. 3d 212, 223 (D.D.C. 2019). In another case, the court rejected the FBI's distinction between the use of a technique vis-à-vis fugitives as opposed to "criminals under investigation" because "[t]here is no reason to suppose that the use of a successful technique would be limited to a particular kind of case." *Ferguson v. Kelley*, 448 F. Supp. 919, 926 (N.D. Ill. 1977).

Hamdan v. Department of Justice, 797 F.3d 759 (9th Cir. 2015), is not to the contrary. In that case, the FBI claimed that exemption (b)(7)(E) applied to records that would reveal "techniques and procedures related to surveillance and credit searches." *Id.* at 777. The court recognized that "credit searches and surveillance are publicly known law enforcement techniques," but it nonetheless noted that the FBI's affidavits stated that "the records reveal techniques that, if known, could enable criminals to educate themselves about law enforcement methods used to locate and apprehend persons." *Id.* Distinguishing *Rosenfeld*, the court concluded that the affidavits implied "a specific *means* of conducting surveillance and credit searches" and held that the records fell under exemption (b)(7)(E). *Id.* at 777-78.

Hamdan is inapposite for two reasons. First, the court ruled exempt a technique itself—a "method[] used to locate and apprehend persons," *id.* at 777—not, as here, the application of a known technique for a purpose that other federal agencies have publicly acknowledged. Second, *Hamdan* did not involve a Glomar assertion; the FBI in that case had responded to the request but was seeking to withhold certain portions of the produced records. *Id.* The FBI here, by contrast, has taken the untenable position that even processing the Request would reveal a law enforcement technique, despite overwhelming public evidence already demonstrating its use of

that technique.

C. The FBI's predictions of the consequences of processing the Request misapprehend the nature of online speech.

The FBI's Glomar response suffers from another inherent defect: it relies on flawed assumptions about the consequences of processing the Request and producing any responsive records. Defendant's declarant states that "providing a non-Glomar response under these circumstances would provide criminals or terrorists with a key piece of investigative information to . . . predict the use of investigative tools/intelligence analysis to alter or plan their activity if such records exist." Seidel Decl. ¶ 19, ECF No. 31-1 at 9. He further states that "[i]nforming international terrorists the FBI monitors social media information in conjunction with immigration data, would inform them the FBI is closely monitoring their behavior on social media platforms in association with any efforts to immigrate into the United States," and conversely that "[c]onfirming the FBI has no responsive records would allow them 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." *Id.* ¶ 20, ECF No. 31-1 at 10.

These predictions strain credulity. As described above, the U.S. government has repeatedly and expansively disclosed its use of social media surveillance, including for the enumerated purposes. It is beyond implausible that "international terrorists" seeking to immigrate to the United States would not suspect that the U.S. government monitors their "behavior on social media platforms." *See id.*; *see also ACLU*, 710 F.3d at 431 ("[A]s it is now clear that the Agency does have an interest in drone strikes, it beggars belief that it does not also have documents relating to the subject."). Even more fanciful is the notion that, if the FBI were to confirm that it has no responsive records, terrorists could seek to enter the United States "without fear of investigative scrutiny," *see* Seidel Decl. ¶ 20, ECF No. 31-1 at 10, given the intense scrutiny of visitors' and immigrants' social media that DHS and the State Department have already disclosed.

The FBI's predictions also ignore that the consequences of any surveillance of social media accrue regardless of its purpose or the entity that conducts it. Unlike traditional, offline

speech, which typically occurs only in specific locations or physical contexts, online speech is hosted on platforms that are global in scope—it occurs at a unitary locus. Thus, to the extent surveillance of online speech causes consequences, they will ensue as a result of *any* publicly known surveillance by *any* government agency. Because the U.S. government's use of social media surveillance for the enumerated purposes is fully public, any purported effects of the disclosure of the technique for those purposes are a *fait accompli*, and the FBI cannot plausibly argue that its own involvement or non-involvement in such surveillance would impact its effectiveness. *See Reporters Comm.*, 369 F. Supp. 3d at 225 (rejecting FBI Glomar response and concluding that revealing the FBI has responsive records "would not reduce or nullify the effectiveness of the technique when it is actually used" because of "information already publicly available to criminals"). Put simply, the ship has sailed.

Additionally, in describing the purported harms of processing the Request, the FBI effectively concedes that knowledge of social media surveillance prompts people to limit their speech online. But asserting that a Glomar response is necessary in order to avoid "circumvention of the law," *see* Seidel Decl. ¶ 19, ECF No. 31-1 at 9, misunderstands what the First Amendment protects and mistakenly equates both actual and foregone speech with law-evading activity. Online speech of citizens and others in the United States is protected by the First Amendment and rarely constitutes a violation of the law. *See Signature Mgmt. Team, LLC v. Automattic, Inc.*, 941 F. Supp. 2d 1145, 1154 (N.D. Cal. 2013) ("[O]nline speech stands on the same footing as other speech—there is no basis for qualifying the level of First Amendment scrutiny that should be applied to online speech.") (quoting *In re Anonymous Online Speakers*, 661 F.3d 1168, 1173 (9th Cir. 2011)). Similarly, the decision *not* to speak is itself constitutionally protected. *Wooley v. Maynard*, 430 U.S. 705, 714 (1977) ("The right to speak and the right to refrain from speaking are complementary components of the broader concept of individual freedom of mind."). Any person's reluctance to make statements publicly on social media, therefore, cannot reasonably be equated with "circumvention of the law." *See* Seidel Decl. ¶ 19, ECF No. 31-1 at 9.

The FBI's claims regarding the purported harms of producing responsive records actually

serve as a recognition of the chilling effect that social media surveillance has on freedom of expression more broadly—making clear the public interest in records responsive to the Request. Indeed, even uncertainty about whether the FBI or any other government agency is monitoring online speech prompts self-censorship and the kinds of consequences of which the FBI warns. *See, e.g., United States v. Jones*, 565 U.S. 400, 416 (2012) ("Awareness that the Government *may be* watching chills associational and expressive freedoms.") (Sotomayor, J., concurring) (emphasis added); *MacPherson v. Internal Revenue Serv.*, 803 F.2d 479, 484 (9th Cir. 1986) ("The mere compilation by the government of records describing the exercise of First Amendment freedoms creates the *possibility* that those records will be used to the speaker's detriment, and hence has a chilling effect on such exercise.") (emphasis added). The FBI concedes that it engages in social media surveillance. Seidel Decl. ¶ 13, ECF No. 31-1 at 7. Its recognition that such surveillance chills freedom of expression underscores the impropriety of its Glomar response.

D. This case differs fundamentally from others in which courts have upheld the FBI's use of a Glomar response under exemption (b)(7)(E).

Cases in which courts have permitted Glomar responses under exemption (b)(7)(E) are limited and typically involve circumstances in which producing responsive records would reveal whether a specific individual is or was a subject of investigation. For instance, in *Vasquez v. Department of Justice*, 887 F. Supp. 2d 114 (D.D.C. 2012), the court upheld the FBI's Glomar assertion in response to a request for transactions and entries related specifically to the requester in the FBI's National Crime Information Center database. *Id.* at 117-18. *See also El Badrawi v. Dep't of Homeland Sec.*, 596 F. Supp. 2d 389, 396 (D. Conn. 2009) (concluding that "confirming or denying that [an individual] is a subject of interest . . . would cause the very harm FOIA Exemption[] . . . 7(E) [is] designed to prevent"). The cases that Defendant cites are in this vein; they all involved requests that would have revealed any investigative interest in a specific individual or entity. *See* Def.'s Mot., ECF No. 31 at 12; *Kalu v. Internal Revenue Serv.*, 159 F. Supp. 3d 16, 23 (D.D.C. 2016) (Glomar assertion as to whether requester's name was on a watchlist); *Gordon v. FBI*, 388 F. Supp. 2d 1028, 1037 (N.D. Cal. 2005) (same); *Cozen*

O'Connor v. Dep't of Treasury, 570 F. Supp. 2d 749, 788 (E.D. Pa. 2008) (Glomar responses to requests that sought records regarding terrorism-related designations of specific individuals and entities).

These cases are not instructive here. Merely acknowledging whether the FBI conducts surveillance of social media for the enumerated purposes would not identify or rule out any given individual as a subject of interest. *See Reporters Comm.*, 369 F. Supp. 3d at 224 ("Simply revealing that the FBI has any such records would not allow criminals to discern whether or not the FBI has used the technique to investigate their own, specific criminal activity, because all a criminal would know is the existence of an unquantified number of records."). For this additional reason, the FBI's motion fails.

II. The FBI's Explanation Of The Basis For Its Glomar Response Is Inadequate.

An agency may only satisfy its Glomar burden by submitting affidavits that "explain[] in as much detail as possible the basis for [the agency's] claim that it can be required neither to confirm nor to deny the existence of the requested records." *Wilner v. Nat'l Sec. Agency*, 592 F.3d 60, 68 (2d Cir. 209) (quoting *Phillippi v. Cent. Intelligence Agency*, 546 F.2d 1009, 1013 (D.C. Cir. 1976)). "[C]onclusory affidavits that merely recite statutory standards, or are overly vague or sweeping will not . . . carry the government's burden." *Larson v. Dep't of State*, 565 F.3d 857, 864 (D.C. Cir. 2009). Where affidavits submitted in support of Glomar responses are perfunctory or unsubstantiated, courts have rejected them and required the government to confirm or deny the existence of records. *See, e.g.*, *Roth*, 642 F.3d at 1181 (rejecting government's justifications for *Glomar* response under law-enforcement exemptions); *Jefferson v. Dep't of Justice*, 284 F.3d 172, 178-79 (D.C. Cir. 2002).

The Seidel Declaration fails to provide the requisite detail or logical support for the FBI's Glomar assertion, let alone the "particularly persuasive affidavit" required in the Glomar context. *See Florez*, 829 F.3d at 182. Mr. Seidel states in conclusory fashion that "confirming or denying the existence of records . . . would allow criminals, terrorists, or intelligence targets to modify their behavior to evade FBI investigative efforts." Seidel Decl. ¶ 13, ECF No. 31-1 at 7. But nowhere in his declaration does Mr. Seidel explain *how* or *why* that would be the case, and

for the reasons set forth above, this prediction is neither logical nor plausible.

CONCLUSION

The FBI's Glomar response is invalid. Plaintiffs respectfully request that the motion for partial summary judgment be denied, and that the FBI be directed to process the Request and promptly produce records responsive to parts 2(a), 2(b), and 2(c).

Respectfully submitted,

DATED: September 20, 2019

/s/ Hugh Handeyside
Hugh Handeyside
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: 212-549-2500
hhandeyside@aclu.org

Matthew Cagle
American Civil Liberties Union Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
Telephone: 415-621-2493
mcagle@aclunc.org

Attorneys for Plaintiffs