UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH SIX ACCOUNTS STORED AT PREMISES CONTROLLED BY ONE PROVIDER PURSUANT TO 18 U.S.C. § 2703 FOR INVESTIGATION OF VIOLATIONS OF 18 U.S.C. § 951	SC NO: 24-sc-2315 Case: 1:26-mc-00098 Assigned To : Boasberg, James E. Assign. Date : 6/22/2026 Description: Misc.

MICHAEL CAPUTO'S AND JUDICIAL WATCH, INC.'S COMBINED MOTION TO INTERVENE AND UNSEAL SEARCH WARRANT MATERIALS

Michael Caputo and Judicial Watch, Inc., by counsel, move to intervene in this matter for the limited purpose of unsealing the search warrant materials related to the November 18, 2024 warrant directed at Caputo's Google account. Caputo and Judicial Watch also move to unseal those materials. The reasons for this combined motion are stated in the accompanying memorandum of points and authorities.

Dated: June 22, 2026

Respectfully submitted,

Michael Bekesha (D.C. Bar No. 995749)
Sean O'Donnell (D.C. Bar No. 90040392)
JUDICIAL WATCH, INC.
425 Third Street S.W., Suite 800
Washington, DC 20024
Tel: (202) 646-5172
Email: mbekesha@JudicialWatch.org

Counsel for Michael Caputo and Judicial Watch, Inc.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH SIX ACCOUNTS STORED AT PREMISES CONTROLLED BY ONE PROVIDER PURSUANT TO 18 U.S.C. § 2703 FOR INVESTIGATION OF VIOLATIONS OF 18 U.S.C. § 951	)	SC NO: 24-sc-2315

MICHAEL CAPUTO'S AND JUDICIAL WATCH, INC.'S MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF THEIR COMBINED MOTION TO INTERVENE AND UNSEAL SEARCH WARRANT MATERIALS

I. Introduction.

Michael Caputo and Judicial Watch, Inc. respectfully request this Court allow them to intervene in this matter for the limited purpose of unsealing the search warrant materials related to the November 18, 2024 warrant directed at Caputo's Google account and unseal those materials. *See* Exhibit A. This Court has both the authority and the duty to consider the public's qualified First Amendment and common law right of access to judicial records. The warrant materials sought here are judicial records subject to the presumption of public access. Because no compelling governmental interest justifies continued sealing, and because both Caputo, whose entire online private life was seized, and Judicial Watch, which seeks to inform the public about the weaponization of the federal government against political opponents and their allies, have powerful interests in disclosure, the Court should unseal these materials.

II. Factual Background.

On November 18, 2024, this Court issued a search warrant that authorized the United States to seize the private content of Michael Caputo's Google account, as well as all data and transactional information related to that account, for the period from January 1, 2019, to April 1,

2021, from Google. The search warrant was sweeping in scope. It included all communications and attachments across every Google platform Caputo used, including email, messaging, voice, and chat services; all files stored or shared through Google Drive, Photos, and related storage services; all search history, web browsing history, and location data; calendar entries, contacts, and productivity documents; advertising and analytics data; and all associated metadata, including IP addresses, routing information, device identifiers, timestamps, and file sizes.

The same day, this Court ordered Google not to disclose the existence or content of the search warrant for a period of one year. The order prohibited Google from even informing Caputo that it received and was complying with the search warrant. The Court also sealed the warrant as well as the application, affidavit, supporting documents, and all other related materials until otherwise ordered by the Court. According to PACER, the seal remains in place.

III. Movants.

Movant Michael Caputo, a longtime ally of and policy advisor to President Donald J. Trump, is a political consultant and former Assistant Secretary for Public Affairs at the U.S. Department of Health and Human Services. He has never been charged with any crime. Yet, in the days after the November 2024 election, the United States seized his entire online private life, as reflected in his Google account. It did so without his knowledge. Caputo therefore seeks to unseal the search warrant materials to know the reasons for the United States' sweeping seizure and the evidence relied on to substantiate the search warrant. As the subject of the search warrant, whose most private communications, files, digital and banking records were seized without his knowledge, Caputo's interest in these records is obvious.

Judicial Watch is a not-for-profit, educational organization that seeks to promote transparency, accountability, and integrity in government and fidelity to the rule of law. An

integral part of Judicial Watch's mission is educating the public about the operations and activities of the government and government officials. To this end, Judicial Watch undertakes investigations of the federal government and federal officials by making extensive use of the Freedom of Information Act, among other investigative tools. Judicial Watch subsequently analyzes all records it receives and disseminates its findings to the public.

Here, Judicial Watch is investigating the potential politicization of numerous federal law enforcement agencies and whether they abused their powers to attack an ally of a political opponent. Judicial Watch's investigation has previously included obtaining judicial records related to the FBI's and the U.S. Department of Justice's investigations of President Donald J. Trump and his associates. *U.S. v. Sealed Search Warrant*, Case No. 22-mj-08332-BER-1 (S.D. Fla., Mot. filed Aug. 9, 2022) (motion to unseal the search warrant materials relating to the August 8, 2022 search of President Donald J. Trump's Florida residence); *In re Transcripts of this Court related to the Surveillance of Carter Page*, Case No. 18-misc-03 (F.I.S.C., filed Jul. 24, 2018) (motion for publication of transcripts of hearings relating to Foreign Intelligence Surveillance Act warrants of Carter Page); *Judicial Watch, Inc. v. U.S. Department of Justice*, Case No. 18-00245-CRC (D.D.C., filed Feb. 2, 2018) (FOIA lawsuit for judicial records relating to Foreign Intelligence Surveillance Act warrants of Carter Page). This investigation forms the broader context within which the warrant targeting Caputo must be understood.

With respect to investigations of Caputo, Judicial Watch is currently seeking records from the Federal Bureau of Investigation, the Office of the Director of National Intelligence, the Executive Office of the United States Attorney, and the U.S. Department of Justice's National Security Division, Office of Information Policy, and Criminal Division. Those records are being sought pursuant to the Freedom of Information Act in *Judicial Watch, Inc. v. U.S. Department of*

Justice, Case No. 25-cv-01903-RBW (D.D.C., filed June 17, 2025); *Judicial Watch, Inc. v. Office of the Director of National Intelligence*, Case No. 25-cv-02469-CKK (D.D.C., filed Jul. 30, 2025); and *Judicial Watch, Inc. v. U.S. Department of Justice*, Case No. 25-cv-02631-TJK (D.D.C., filed Aug. 12, 2025). Judicial Watch also has similar FOIA lawsuits related to the investigations of other individuals, including Rudy Giuliani and Mike Lindell. *See, e.g., Judicial Watch, Inc. v. U.S. Department of Justice*, Case No. 26-cv-01158-CRC (D.D.C., filed Apr. 6, 2026) (FOIA lawsuit for records of the FBI and the Justice Department's Criminal Division, Executive Office of the U.S. Attorneys and Office of Information Policy about investigations of Rudy Giuliani); *Judicial Watch, Inc. v. U.S. Department of Justice*, 25-cv-03850-SLS (D.D.C., filed Nov. 3, 2025) (FOIA lawsuit for records of the FBI and the Justice Department's Criminal Division and Office of Information Policy about investigations of Mike Lindell); *Judicial Watch, Inc. v. U.S. Department of Justice*, 25-cv-00588-JMC (D.D.C., filed Feb. 28, 2025) (FOIA lawsuit for records of the FBI about Christina Bobb).

The unsealing of these materials is just one piece of Judicial Watch's broader investigation. If the Court were to unseal the materials, Judicial Watch would obtain, analyze, and make them available to the public, furthering its mission of educating the public about the workings of the federal government.

IV. Argument.[1]

"The public's right of access to judicial records derives from two independent sources: the common law and the First Amendment." *In re L.A. Times Commns., LLC to Unseal Ct. Record*, 628 F. Supp. 3d 55, 62 (D.D.C. 2022) (citations omitted). The target of a criminal investigation also derives a right to the judicial records under the Warrant Clause of the Fourth Amendment. U.S. Const. amend. IV.

A. Caputo and Judicial Watch have a common law right to the warrant materials.

Search warrant materials, including the warrant application, supporting affidavit, and any related nondisclosure orders, qualify as judicial records. *In re L.A. Times Commns., LLC*, 28 F.4th 292, 297 (D.C. Cir. 2022). "The public's right of access to judicial records is a fundamental element of the rule of law." *Leopold v. United States*, 964 F.3d 1121, 1123 (D.C. Cir. 2020). "At bottom, it reflects the antipathy of a democratic country to the notion of 'secret law,' inaccessible to those who are governed by that law." *Id.* at 1127. A "strong presumption in favor of public access to judicial proceedings, including judicial records" therefore exists. *Id.* at 1127 (citation and internal quotations omitted).

When the government seeks to overcome this presumption and maintain a seal, courts in this Circuit apply the six-factor balancing test established in *United States v. Hubbard*, 650 F.2d 293 (D.C. Cir. 1980). "The *Hubbard* test has consistently served as our lodestar for evaluating motions to seal or unseal judicial records because it ensures that [courts] fully account for the

---

[1] Because the D.C. Circuit has held that "nonparties may permissively intervene for the purpose of challenging confidentiality orders," *EEOC v. Nat'l Children's Ctr., Inc.*, 146 F.3d 1042, 1045 (D.C. Cir. 1998), and that principle extends to orders sealing judicial records, Caputo and Judicial Watch focus this memorandum on the merits of their request to unseal the search warrant materials.

various public and private interests at stake." *Leopold*, 964 F.3d at 1127 (citation and internal quotations omitted); *see also MetLife, Inc. v. Financial Stability Oversight Council*, 865 F.3d 661, 666 (D.C. Cir. 2017). "Under the *Hubbard* test, a seal may be maintained only if the district court, after considering the relevant facts and circumstances of the particular case, and after weighing the interests advanced by the parties in light of the public interest and the duty of the courts, concludes that justice so requires." *Leopold*, 964 F.3d at 1131 (citation and internal quotations omitted). The six *Hubbard* factors are: (1) the need for public access to the documents at issue; (2) the extent of previous public access to the documents; (3) the fact that someone has objected to disclosure, and the identity of that person; (4) the strength of any property and privacy interests asserted; (5) the possibility of prejudice to those opposing disclosure; and (6) the purposes for which the documents were introduced during the judicial proceedings. *In re Press Application for Access to Judicial Recs. in Case No. 23-SC-31*, 704 F. Supp. 3d 161, 169 (D.D.C. 2023) (citation omitted).

All six *Hubbard* factors support unsealing.

First, the need for public access is substantial. The search warrant here was sweeping in scope as it sought Caputo's entire online private life as reflected in his Google account. The public has a real interest in knowing the evidence underlying the search warrant application for such an extraordinary seizure and whether the warrant was sought for legitimate law enforcement purposes rather than to target a political opponent's ally. These questions cannot be examined while the materials remain sealed.

Second, the public does not have access to these materials. They remain sealed entirely.

Third, Movants are unaware of any objection to this motion. No party has appeared to oppose unsealing. The government has offered no public justification for continued sealing. The absence of any identified opposing interest weighs in favor of disclosure.

Fourth, the privacy and property interests at stake favor Caputo, not the government. Caputo is the subject of the search warrant and affirmatively seeks disclosure of his own records. He has no interest in maintaining their confidentiality.

Fifth, no prejudice will result from disclosure. Caputo was never charged. The investigation appears to have concluded. There is no ongoing prosecution that disclosure could jeopardize, no witness whose safety is at risk, and no trial whose fairness could be compromised. The purported rationale for sealing that existed at the time the warrant issued no longer exists.

Sixth, the search warrant materials were introduced to obtain judicial authorization for a search. They had no other purpose but to assist the Court in deciding whether to issue the search warrant.

Taken together, all six factors weigh heavily in favor of unsealing. The historical presumption of access to warrant materials vastly outweighs any interest the government may have in maintaining the seal.

B. Michael Caputo and Judicial Watch have a First Amendment right to the warrant materials.

The First Amendment independently requires that certain judicial proceedings be open to the public. To determine when this right applies, courts apply the "experience and logic" test, asking: (1) whether "there has been a tradition of accessibility" to the proceedings in question; and (2) whether public access would "play[] a particularly significant positive role in the actual functioning of the process in question." *Press-Enterprise Co. v. Superior Court of Cal.*, 478 U.S. 1, 8 (1986) (*Press-Enterprise II*); *In re Press Application*, 704 F. Supp. 3d at 173. The

government may overcome this right only by demonstrating that "closure is essential to preserve higher values and is narrowly tailored to serve that interest." *Press-Enterprise II*, 478 U.S. at 13–14 (citation omitted).

Both of the test's prongs are satisfied. Courts in this Circuit have recognized a historical tradition of public access to warrant proceedings. *In re Press Application*, 704 F. Supp. 3d at 173–74 (finding a tradition of access to warrant materials in the D.D.C. context). In addition, judicial authorization for a search is a check on executive overreach; that check is meaningful only if the public can scrutinize whether courts are performing it. Access to these materials would allow the public to assess whether the search warrant targeting Caputo was supported by genuine probable cause or reflected an abuse of the warrant process.

Moreover, the government cannot meet its burden under "experience and logic" test for the same reasons it cannot overcome the common law right to access. It has identified no higher value requiring closure, and the original rationale for sealing no longer exists. Caputo was never charged; indeed, as far as the public record reflects, no one was charged in this investigation. Even if some residual interest in confidentiality existed, sealing the materials in their entirety is not narrowly tailored to serve any such interest. *See Press-Enterprise II*, 478 U.S. at 13–14.

C. Michael Caputo has a right to the warrant materials under the Warrants Clause.

Separate from the public's right of access, Mr. Caputo has a personal interest in the warrant materials rooted in the Fourth Amendment and Federal Rule of Criminal Procedure 41. A person whose property or private data has been seized pursuant to a warrant has an obvious, cognizable interest in knowing whether the Fourth Amendment's requirements were met. Mr. Caputo cannot know if that occurred if the warrant materials remain sealed.

Movants could not locate a decision by either the D.C. Circuit or this Court directly on point. However, as Magistrate Judge Allison H. Goddard of the Southern District of California recently explained, numerous courts have recognized the distinction between the public's right of access to warrant materials and the right of access held by the subject of a search warrant. *Cactil, LLC v. United States*, No. 3:24-cv-01270-LL-AHG, 2024 U.S. Dist. LEXIS 162864, at *6 (S.D. Cal. Sep. 10, 2024). Judge Goddard further went on to explain that the right of the target is "rooted in the Warrant Clause of the Fourth Amendment, allowing an individual to inspect the probable cause affidavit leading to the warrant." *Id.* And that right is only "overcome where a compelling governmental interest is demonstrated requiring that the materials be kept under seal, and there is no less restrictive means, such as redaction, capable of serving that interest." *Id.* at **6-7.

In addition, Rule 41(g) provides that "[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return." Fed. R. Crim. P. 41(g). A Rule 41(g) motion obviously necessarily implicates the warrant materials themselves, because an individual cannot meaningfully challenge the legality of a seizure without access to the affidavit and application purported to justify it.

Although Mr. Caputo does not file a Rule 41(g) motion concurrently with this motion, the same logic applies: the government seized his entire online private life as reflected in his Google account, retained whatever it extracted, and never charged him with any crime. He cannot assess whether to seek return of his property or whether the warrant that authorized the seizure was constitutionally defective without first seeing the materials this Court is asked to unseal.

Mr. Caputo's individual interest reinforces rather than displaces the *Hubbard* analysis. His stake in the materials is directly relevant to factors one and four of that test. Where, as here,

the person most directly affected by the sealed record affirmatively seeks its disclosure and has a Fourth Amendment basis for doing so, those factors weigh decisively in favor of unsealing.

V. Conclusion.

For these reasons, Michael Caputo and Judicial Watch respectfully request that the Court allow them to intervene in this matter for the limited purpose of unsealing the search warrant materials related to the November 18, 2024 warrant directed at Caputo's Google account and unseal the search warrant materials related to the November 18, 2024 warrant directed at Caputo's Google account.

Dated: June 22, 2026

Respectfully submitted,

Michael Bekesha (D.C. Bar No. 995749)
Sean O'Donnell (D.C. Bar No. 90040392)
JUDICIAL WATCH, INC.
425 Third Street S.W., Suite 800
Washington, DC 20024
Tel: (202) 646-5172
Email: mbekesha@JudicialWatch.org

Counsel for Michael Caputo and Judicial Watch, Inc.

CERTIFICATE OF SERVICE

I, Michael Bekesha, certify that on June 22, 2026, a true and correct copy of the foregoing Motion to Intervene and Unseal Search Warrant Materials and the accompanying Memorandum in Support was served by U.S. Mail, certified postage prepaid, electronic return receipt requested, on the following counsel for the U.S. government with a courtesy copy transmitted by electronic mail, to:

Gregg Maisel
Deputy Chief, Criminal Division
Chief, National Security Section
U.S. Attorney's Office for the District of Columbia
601 D Street, NW
Washington, DC 20579
Gregg.Maisel@usdoj.gov

Evan Turgeon
Chief, Foreign Agent Registration Act Unit
Deputy Chief, Counterintelligence and Export Control Section
National Security Division
U.S. Department of Justice
175 N Street, NE
Constitution Square, Building 3 - Room 1.204
Washington, DC 20002
Evan.Turgeon@usdoj.gov

Michael Bekesha by SOO
Michael Bekesha

Exhibit A

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH SIX ACCOUNTS STORED AT PREMISES CONTROLLED BY ONE PROVIDER PURSUANT TO 18 U.S.C. 2703 FOR INVESTIGATION OF VIOLATIONS OF 18 U.S.C. § 951

) Case No. 24-sc-2315

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Jurisdiction of the District of Columbia
(identify the person or describe the property to be searched and give its location):

See Attachment A, hereby incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B, hereby incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before December 2, 2024 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to [redacted]

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of .

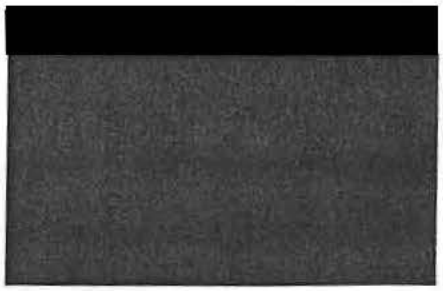
Date and time issued: 11/18/2024

City and state: Washington, D.C.

[redacted]

ATTACHMENT A
Property to Be Searched

This warrant applies to information which is associated with Google LLC account identified by:



which are stored at premises owned, maintained, controlled, or operated by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Google LLC ("PROVIDER") to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of PROVIDER, including any records that have been deleted but are still available to PROVIDER or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), PROVIDER is required to disclose the following information to the government corresponding to each account or identifier ("Account") listed in Attachment A:

a. For the time period **January 1, 2019, to April 1, 2021**: The contents of all communications and related transactional records for all PROVIDER services used by an Account subscriber/user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services, including but not limited to Google Drive, Google Voice, Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), and Web History (bookmarks and recorded browsing history); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); and Google Play (which allow users to purchase and download digital content, e.g., applications).incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic

communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies)[1];

b. For the time period **January 1, 2019, to April 1, 2021**: The contents of all other data and related transactional records for all PROVIDER services used by an Account user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services include electronic communication and remote computing services;

c. For the time period **January 1, 2019, to April 1, 2021**: The contents of all other data and related transactional records for all PROVIDER services used by an Account user (such as email services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services including all services identified in paragraph (a), and any information generated, modified, or stored by user(s) or PROVIDER in connection with the Account (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);

---

[1] These services include electronic communication services such as Gmail (electronic mail), Google Voice (voice calls, voicemail, and SMS text messaging), Chat (instant messaging and video chats, previously called Hangouts), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); Android (operating system); and Google Play (which allow users to purchase and download digital content, e.g., applications).

d. For the time period **January 1, 2019, to April 1, 2021**: All PROVIDER records concerning the online search and browsing history associated with the Account or its users (such as information collected through tracking cookies) including Google Search, Google Analytics, Web History, and Google Chrome;

e. For the time period **January 1, 2019, to April 1, 2021**: All records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

f. All records regarding identification of the Account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;

g. All records pertaining to devices associated with the Account and software used to create and access the Account, including device serial numbers, instrument numbers, model types/numbers, International Mobile Equipment Identities ("IMEI"), Mobile Equipment Identifiers ("MEID"), Global Unique Identifiers ("GUID"), Electronic Serial Numbers ("ESN"), Android Device IDs, phone numbers, Media Access Control ("MAC") addresses, operating system

information, browser information, mobile network information, information regarding cookies and similar technologies, and any other unique identifiers that would assist in identifying any such device(s).

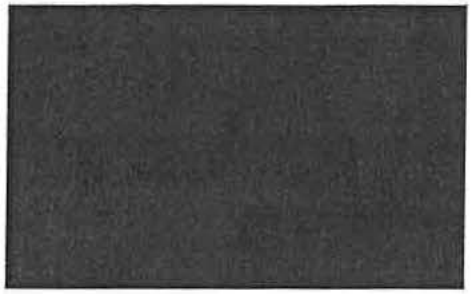
h. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703©(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any PROVIDER account (including both current and historical accounts) ever linked to the Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (*e.g.*, credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

i. For the time period **January 1, 2019, to April 1, 2021:** All information held by PROVIDER related to the location and location history of the user(s) of the Account, including geographic locations associated with the Account (including those collected for non-PROVIDER based applications), IP addresses, Global Positioning System ("GPS") information, and information pertaining to nearby devices, Wi-Fi access points, and cell towers;

j. For the time period **January 1, 2019, to April 1, 2021**: All records of communications between PROVIDER and any person regarding the Account, including contacts with support services and records of actions taken;

k. Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to the Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Account or associated user(s) (but not including confidential communications with legal counsel); and

Within 14 days of the issuance of this warrant, PROVIDER shall deliver the information set forth above via United States mail, courier, or e-mail to the following:



II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 951 (Agent of Foreign Government) and 22 U.S.C. § 611 et seq. (Foreign Agents Registration Act ("FARA")), as described in the affidavit submitted in support of this warrant, including, for each account, information pertaining to the following matters:

a. Information that constitutes evidence of the identification or location of the user(s) of the Account;

b. Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the Account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

c. For the time period **January 1, 2019, to April 1, 2021**: Information that constitutes evidence indicating the Account user's state of mind, *e.g.*, intent, absence of mistake, evidence indicating preparation or planning, or evidence indicating concealment of activities related to the criminal activity under investigation;

d. Information that constitutes evidence concerning how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;

j. For the time period **January 1, 2019, to April 1, 2021**: Information that relates to communications with the Government of the Russian Federation, to include officials and agents, agencies, organizations, or businesses;

l. For the time period **January 1, 2019, to April 1, 2021**: All banking records, financial applications, contracts, agreements, records, contracts, ledgers, financial documents, bank statements, brokerage accounts, virtual currency information, financial information (including cryptocurrency and international currency), and cash receipts by the User(s) of the account and any accomplices or coconspirators;

n. For the time period **January 1, 2019, to April 1, 2021**: All records, documents, information and material related to travel outside the United States.

o. For the time period **January 1, 2019, to April 1, 2021**: Search history related to the account;

p. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the account;

r. Records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" and "data" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photograph.

III. Government procedures for warrant execution

The United States government will conduct a search of the information produced by the PROVIDER and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the PROVIDER that does not fall within the scope of Section II and will not further review the information absent an order of the Court. Such sealed information may include retaining a digital copy of all information received pursuant to the warrant to be used for authentication at trial, as needed.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH SIX ACCOUNTS STORED AT PREMISES CONTROLLED BY ONE PROVIDER PURSUANT TO 18 U.S.C. § 2703 FOR INVESTIGATION OF VIOLATIONS OF 18 U.S.C. § 951	)	SC NO: 24-sc-2315

[PROPOSED] ORDER

The Court, having considered Michael Caputo's and Judicial Watch, Inc.'s Combined Motion to Intervene and Unseal Search Warrant Materials, hereby ORDERS that

1. The Motion is GRANTED;

2. Michael Caputo and Judicial Watch's may intervene in this matter for the limited purpose of unsealing the search warrant materials related to the November 18, 2024 warrant directed at Caputo's Google account; and

3. The search warrant materials related to the November 18, 2024 warrant directed at Caputo's Google account are unsealed.

IT IS SO ORDERED.

Dated: _____

_____
DISTRICT JUDGE