

Page 0027 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0028 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0029 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0030 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0031 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0032 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0033 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0034 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0035 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0036 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0037 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0038 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0039 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0040 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0041 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0042 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0043 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0044 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0045 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0046 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0047 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0048 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0049 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0050 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0051 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0052 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0053 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0054 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0055 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0056 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0057 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0058 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0059 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0060 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0061 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0062 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0063 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0064 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0065 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0066 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0067 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0068 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0069 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0070 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0071 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0072 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0073 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0074 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0075 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0076 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0077 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0078 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0079 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0080 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0081 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0082 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0083 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0084 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0085 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0086 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0087 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0088 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0089 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0090 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0091 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0092 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0093 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0094 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0095 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0096 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0097 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0098 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0099 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0100 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0101 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0102 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0103 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0104 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0105 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0106 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0107 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0108 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0109 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0110 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0111 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0112 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0113 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0114 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0115 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0116 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0117 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0118 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0119 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0120 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0121 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0122 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0123 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0124 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0125 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0126 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0127 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0128 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0129 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0130 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0131 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0132 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0133 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0134 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0135 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0136 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

Page 0137 of 3451

Withheld Pursuant to Exemption

(b)(5)

of the Freedom of Information & Privacy Act

From: (b)(6); (b)(7)(C) (LEG)
Sent: Wed, 16 Jun 2021 20:20:08 +0000
To: THOMAS HUSE (LEG); (b)(6) (LEG)
Cc: (b)(6); (b)(7)(C) (LEG)
Subject: RE: USSS News Briefing (6-16-21)
Attachments: USSS-GC-FOIA (b)(6) 0527 (004).pdf

(b)(5)

Regards,

(b)(6); (b)(7)(C)

Attorney-Advisor
Office of Chief Counsel
United States Secret Service
(b)(6); (b)(7)(C) (mobile)

From: THOMAS HUSE (LEG) <(b)(6); (b)(7)(C)>
Sent: Wednesday, June 16, 2021 2:54 PM
To: (b)(6) (LEG); (b)(6); @usss.dhs.gov; (b)(6); (b)(7)(C) (LEG); (b)(6); @usss.dhs.gov
Cc: (b)(6); (b)(7)(C) @usss.dhs.gov
Subject: FW: USSS News Briefing (6-16-21)

(b)(5)

Best,
Tom

From: (b)(6); CMR; (b)(6); @usss.dhs.gov
Sent: Wednesday, June 16, 2021 9:23 AM
To: dirstaff <dirstaff@usss.dhs.gov>; CMR-clips-list <CMR-clips-list@usss.dhs.gov>
Subject: Fwd: USSS News Briefing (6-16-21)

From: (b)(6); (IGL)
Sent: Mon, 5 Apr 2021 20:20:40 +0000
To: (b)(6); (PRO)
Subject: RE: *PLEASE EXPEDITE* - FOIA/PA Records Request - 20-10083

Thank you for providing your response! We appreciate it.

Regards,

(b)(6); (b)(7)(C)
Government Information Specialist
Freedom of Information Act & Privacy Act Program
Office of Intergovernmental and Legislative Affairs
United States Secret Service
Direct: (b)(6);
Fax: 202-406-5586



From: (b)(6); (PRO) (b)(6); @usss.dhs.gov>
Sent: Monday, April 5, 2021 4:00 PM
To: (b)(6); (IGL) (b)(6); @usss.dhs.gov>
Cc: (b)(6); (b)(7)(C) (PRO) (b)(6); (b)(7)(C) @usss.dhs.gov>
Subject: RE: *PLEASE EXPEDITE* - FOIA/PA Records Request - 20-10083

Good afternoon (b)(6);
USSS does not have any contracts with Venntel Inc.

(b)(6); (b)(7)(C)
Procurement Analyst
Procurement Division (PRO)
Office: TBA / Mobile: (b)(6); (b)(7)(C)
Email: (b)(6); @usss.dhs.gov





U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE

Washington, D.C. 20223

Freedom of Information Act and Privacy Act (FOIA/PA) Records Request

FOIA/PA Case Number:	20-10083	Request Date:	April 1, 2021	Suspense Date:	April 1, 2021
----------------------	----------	---------------	---------------	----------------	---------------

Office(s) Conducting Search	PRO	Office Point of Contact(s)	(b)(6); (b)(7)(C)
Program/Branch Task to Search	PRO	Person(s) Conducting Search	

FOIA/PA OFFICE CONTACT INFORMATION

FOIA/PA POC	(b)(6); (b)(7)(C)	Phone Number	N/A
-------------	-------------------	--------------	-----

REQUESTED RECORDS

All contracts with Venntel, Inc.

*****Please expedite this request as it is in litigation*****

INSTRUCTIONS FROM FOIA/PA OFFICE

☒	Search your records for responsive document(s), and if located, provide one (1) clean copy to the FOIA/PA Program.
☒	Record the time spent reviewing and coordinating the request.
☒	Complete form and return via one of the following options: 1. interoffice mail 2. scan and email to foia@usss.dhs.gov 3. hand carry

COMMENTS SECTION

I searched for Venntel Inc contract in FPDS-NG and the I-drive. I found zero USSS contracts between USSS and Venntel.

Please contact the FOIA/PA Program with any questions and/or comments at
202-406-6370 or foia@usss.dhs.gov

Directions for Conducting a Search for Records Requested under FOIA/PA

In responding to this request for information made pursuant to the Freedom of Information Act, 5 USC 552 and/or Privacy Act, 5 USC 552a, you must undertake a search that is *reasonably calculated to uncover all responsive materials* described in the request. You must search in ALL places where responsive records are likely to be found.

Once completed, this form will document the Agency's search efforts in this matter and may be utilized in a court of law.

Please conduct a thorough search of your records, both paper and electronic, for materials pertaining to this FOIA/PA request. You must search in every area within your components where responsive records may be located.

"Records" include: paper records, electronic records, E-mail correspondence, pictures, DVDs, video tapes, audio tapes, microfiche, or any other material recorded in any manner unless otherwise stated in the request.

Name of Individual(s) Conducting Search	Searcher's Grade/Level	Search Date	Total Search Time
(b)(6); (b)(7)(C)	GS-14	04/05/2021	2 hours

SEARCHES CONDUCTED

DATABASES	
List all databases searched	List the search terms used
FPDS	Verintel
Searched the I Drive	Verintel

DESKTOP/LAPTOP COMPUTERS				
What areas of the computer(s) did you search?				
Area	N/A?	No?	Yes?	List the Search Terms Used
Desktop	N/A ☐	No ☒	Yes ☐	
Hard drive (C:/)	N/A ☐	No ☒	Yes ☐	
Office Shared drive	N/A ☐	No ☐	Yes ☒	Venntel
Personal Drive (P:/)	N/A ☐	No ☒	Yes ☐	
All Other Electronic Storage (e.g., thumb drives, other shared drives, external drives):				
n/a				
For each of the areas identified above, describe your search (i.e., manual review of each folder individually, use search engine in the Start Menu, or some other electronic search command):				
n/a				

PAPER FILES			
Did you search any paper files?	Yes ☐	No ☒	N/A ☐
Were the paper files located in your office's file system(s)?	Yes ☐	No ☒	N/A ☐
Were the paper files work-related materials that are maintained by you or are located in your personal workspace?	Yes ☐	No ☒	N/A ☐
What file(s) were searched? Please describe.	n/a		
Describe below how the paper files are organized, maintained, and searched. (i.e., file cabinet, bookshelf, order, etc.)	n/a		

EMAIL (Outlook)				
	N/A?	No?	Yes?	List the search terms
Did you search Outlook for official messages concerning the subject of the request?	N/A ☐	No ☒	Yes ☐	
Did you search Outlook, to include individual email searches of your work account, for any other email(s) concerning the subject of the request?	N/A ☐	No ☒	Yes ☐	
How did you search Outlook? (i.e., manual review of every email in sent, deleted, incoming, outgoing, and personal folders, "Find" function in the Tools pull-down menu):				

OTHER RECORDS AND LOCATIONS			
Did you search any other records or locations not listed above? (i.e., video, audio, microfiche, etc)	Yes ☐	No ☐	N/A ☐
Where did you search?	n/a		
How did you search?	n/a		
List the search terms used;	n/a		

WERE RESPONSIVE RECORDS LOCATED?	
☐ YES ☒ NO	If yes, please forward the responsive documents to the FOIA/PA Program

SENSITIVITY (IF RECORDS WERE LOCATED)			
Are any of the records classified or otherwise sensitive? (i.e., secret, LES, etc.)	Yes ☐	No ☐	
Please explain			
Are any of the records related to an ongoing open investigation?	Yes ☐	No ☐	
Please explain			

I certify that a search which was reasonably calculated to locate all materials responsive to this request has been conducted.

Name of
Certifying Official

(b)(6); (b)(7)(C)

Title Procurement
Analyst

Date 04/05/2021

February 10, 2020

U.S. Department of Homeland Security
Chief Privacy Officer/Chief FOIA Officer
The Privacy Office
245 Murray Lane, SW, Stop 0655
Washington, D.C. 20528-0655

U.S. Customs and Border Protection
FOIA Officer
90 K Street, NE
FOIA Division
Washington, D.C. 20229

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street, SW, Stop 5009
Washington, D.C. 20536-5009

**Re: FOIA Request Concerning Purchase and Use of Cell Phone
Location Data
(Expedited Processing Requested)**

To Whom It May Concern:

The American Civil Liberties Union and the American Civil Liberties Union Foundation (together, the “ACLU”)¹ submit this Freedom of Information Act request (the “Request”). The Request seeks records pertaining to the purchase of cell phone location data by the Department of Homeland Security (“DHS”), U.S. Customs and Border Protection (“CBP”), and Immigration and Customs Enforcement (“ICE”).

I. Background

On February 7, 2020, the *Wall Street Journal* reported that DHS has “bought access to a commercial database that maps the movements of millions of cellphones in America and is using it for immigration and border

¹ The American Civil Liberties Union Foundation is a 26 U.S.C. § 501(c)(3) organization that provides legal representation free of charge to individuals and organizations in civil rights and civil liberties cases, and educates the public about civil rights and civil liberties issues across the country. The American Civil Liberties Union is a separate non-profit, 26 U.S.C. § 501(c)(4) membership organization that educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analysis of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

enforcement,” without obtaining a warrant.² This is the first time the media has reported on the federal government’s purchase of such data for law enforcement purposes. The report describes the commercial database as “one of the largest known troves of bulk data being deployed by law enforcement in the U.S.”³

Contracting records show that, since 2017, DHS and its components have been purchasing licenses and subscriptions for location data from Venntel Inc.⁴ According to the *Wall Street Journal*, “Venntel” in turn, purchased the information from private marketing companies that sell the location data of millions of cellphones to advertisers.”⁵ The data sold by Venntel is apparently pseudonymised, meaning that data is linked to an alphanumeric identifier, not the name of the cell phone’s owner. However, it is trivially easy to identify particular individuals using their location information, by following their pattern of movements to and from their homes, or by pairing the data with publicly available information.⁶

The *Wall Street Journal* report explains that ICE has used Venntel data to help identify immigrants who were later arrested, and that CBP uses the information to identify “cellphone activity in unusual places, such as remote stretches of desert that straddle the Mexican border.”⁷

These developments raise serious concerns that DHS, CBP, and ICE are seeking to circumvent fundamental Fourth Amendment protections for cell phone location data. In 2018, the Supreme Court in *Carpenter v. United States* held that the government must get a warrant to obtain cell phone location history, given its highly sensitive and revealing nature. Despite this precedent, government lawyers have reportedly approved the purchase of cell phone location information from commercial databases, on the theory that “the Carpenter ruling doesn’t apply” to such purchases.⁸ But the government cannot evade the warrant requirement simply by purchasing information that it would otherwise be unable to obtain without judicial oversight.

² Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>.

³ *Id.*

⁴ *See id.*

⁵ *Id.*

⁶ *See id.*; see also Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>. (explaining that “it’s child’s play to connect real names to the dots that appear on the maps” of cell phone location data).

⁷ Tau & Hackman, *supra* note 2.

⁸ *Id.*



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

The ACLU submits this FOIA request to provide the public with information about the purchase and use of cell phone location information by DHS, CBP, and ICE.

II. Requested Records

The ACLU requests the following records from DHS, CBP, and ICE. This Request seeks records created on or after January 1, 2017:

1. All contracts, memoranda of understanding, letters of commitment, licenses, subscription agreements, and other agreements with vendors, including but not limited to Venntel Inc., concerning government access to or receipt of data from commercial databases containing cell phone location information.
2. All communications with Venntel Inc. and all communications discussing or mentioning Venntel Inc.
3. All policies, procedures, guidelines, formal or informal guidance, advisories, directives, training materials, presentations, and memoranda concerning:
 - a. Access to commercial databases containing cell phone location information;
 - b. Acquisition, processing, retention, use, or dissemination of cell phone location information purchased from a commercial vendor;
 - c. The anonymization and de-anonymization of cell phone location information purchased from a commercial vendor;
 - d. The use of cell phone location information purchased from a commercial vendor in civil immigration enforcement actions;
 - e. The use of evidence in any court application, trial, hearing, or other proceeding that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor;
 - f. The use of “lead” or “tip” information that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor; and



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

- g. The circumstances under which the government notifies defendants or respondents of the use of evidence that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor, including notice of the information's provenance.
4. All formal legal analysis concerning access to commercial databases containing cell phone location information, or the acquisition, processing, retention, use, or dissemination of cell phone location information purchased from a commercial vendor, including the application of *Carpenter v. United States*, 138 S. Ct. 2206 (2018), to this information.
5. Records sufficient to show the volume of cell phone location data contained in the commercial databases for which DHS, CBP, and ICE have purchased access, and records sufficient to show the volume of data that the agencies have accessed from these databases.
6. Records sufficient to show the number of times each year that DHS, CBP, and ICE employees or contractors have accessed commercial databases containing cell phone location information, or have used location data obtained from such databases.
7. All records concerning the use of evidence in any court application, trial, hearing, or other proceeding that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor, including records concerning whether defendants or respondents received notice of the government's reliance on such information and its provenance.

With respect to the form of production, *see* 5 U.S.C. § 552(a)(3)(B), the ACLU requests that responsive records be provided electronically in their native file format, if possible. Alternatively, the ACLU requests that the records be provided electronically in a text-searchable, static-image format (PDF), in the best image quality in the agency's possession, and that the records be provided in separate, Bates-stamped files.

III. Application for Expedited Processing

The ACLU requests expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E).⁹ There is a "compelling need" for these records, as defined in the statute, because the information requested is "urgen[tly]" needed by

⁹ *See also* 6 C.F.R. § 5.5(e).

organizations primarily engaged in disseminating information “to inform the public concerning actual or alleged Federal Government activity.” 5 U.S.C. § 552(a)(6)(E)(v)(II).

A. *The ACLU is an organization primarily engaged in disseminating information in order to inform the public about actual or alleged government activity.*

The ACLU is “primarily engaged in disseminating information” within the meaning of the statute. *See id.*¹⁰ Obtaining information about government activity, analyzing that information, and widely publishing and disseminating it to the press and public are critical and substantial components of the ACLU’s work and are among its primary activities. *See ACLU v. Dep’t of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004) (finding non-profit public interest group that “gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience” to be “primarily engaged in disseminating information”).¹¹

The ACLU regularly publishes *STAND*, a print magazine that reports on and analyzes civil liberties-related current events. The magazine is disseminated to 850,000 people. The ACLU also publishes regular updates and alerts via email to 3.9 million subscribers (both ACLU members and non-members). These updates are additionally broadcast to 4.8 million social media followers. The magazine as well as the email and social-media alerts often include descriptions and analysis of information obtained through FOIA requests.

The ACLU also regularly issues press releases to call attention to documents obtained through FOIA requests, as well as other breaking news,¹²

¹⁰ *See also* 6 C.F.R. § 5.5(e)(1)(ii).

¹¹ Courts have found that the ACLU as well as other organizations with similar missions that engage in information-dissemination activities similar to the ACLU are “primarily engaged in disseminating information.” *See, e.g., Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005); *ACLU*, 321 F. Supp. 2d at 29 n.5; *Elec. Privacy Info. Ctr. v. DOD*, 241 F. Supp. 2d 5, 11 (D.D.C. 2003).

¹² Press Release, ACLU, Federal Court Rules Gov’t Cannot Unilaterally Detain U.S. Resident Indefinitely (Dec. 13, 2019), <https://www.aclu.org/press-releases/federal-court-rules-government-cannot-unilaterally-detain-us-resident-indefinitely>; Press Release, ACLU, Federal Court Permanently Blocks Billions of Dollars in Border Wall Construction (June 28, 2019), <https://www.aclu.org/press-releases/federal-court-permanently-blocks-billions-dollars-border-wall-construction>; Press Release, ACLU, New Documents Reveal NSA Improperly Collected Americans’ Call Records Yet Again (June 26, 2019), <https://www.aclu.org/press-releases/new-documents-reveal-nsa-improperly-collected-americans-call-records-yet-again>; Press Release, ACLU, ACLU and Center for Media Justice Sue FBI for Records on Surveillance of Black Activists (Mar. 21, 2019), <https://www.aclu.org/press-releases/aclu-and-center-media-justice-sue-fbi-records-surveillance-black-activists>; Press Release, ACLU,



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

and ACLU attorneys are interviewed frequently for news stories about documents released through ACLU FOIA requests.¹³

Similarly, the ACLU publishes reports about government conduct and civil liberties issues based on its analysis of information derived from various sources, including information obtained from the government through FOIA requests. This material is broadly circulated to the public and widely available to everyone for no cost or, sometimes, for a small fee. ACLU national projects regularly publish and disseminate reports that include a description and analysis of government documents obtained through FOIA requests.¹⁴ The ACLU also regularly publishes books, “know your rights” materials, fact sheets, and educational brochures and pamphlets designed to educate the



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

New Documents Reveal Government Plans to Spy on Keystone XL Protesters (Sept. 4, 2018), <https://www.aclu.org/news/new-documents-reveal-government-plans-spy-keystone-xl-protesters>; Press Release, ACLU, ACLU Obtains Documents Showing Widespread Abuse of Child Immigrants in U.S. Custody (May 22, 2018), <https://www.aclu.org/news/aclu-obtains-documents-showing-widespread-abuse-child-immigrants-us-custody>; Press Release, ACLU, ACLU Files Lawsuits Demanding Local Documents on Implementation of Muslim Ban (Apr. 12, 2017), <https://www.aclu.org/news/aclu-files-lawsuits-demanding-local-documents-implementation-trump-muslim-ban>. Press Release, ACLU, U.S. Releases Drone Strike ‘Playbook’ in Response to ACLU Lawsuit (Aug. 6, 2016), <https://www.aclu.org/news/us-releases-drone-strike-playbook-response-aclu-lawsuit>.

¹³ See, e.g., Charlie Savage, *N.S.A. Gathered Domestic Calling Records It Had No Authority to Collect*, N.Y. Times (June 26, 2019), <https://www.nytimes.com/2019/06/26/us/telecom-nsa-domestic-calling-records.html> (quoting ACLU attorney Patrick Toomey); Rachel Frazin, *ACLU Sues FBI Over Black Activist Surveillance Records*, Hill (Mar. 21, 2019), <https://thehill.com/policy/national-security/fbi/435143-fbi-sued-over-black-activist-surveillance-records> (quoting ACLU attorney Nusrat Choudhury); Cora Currier, *TSA’s Own Files Show Doubtful Science Behind Its Behavioral Screen Program*, Intercept (Feb. 8, 2017), <https://theintercept.com/2017/02/08/tsas-own-files-show-doubtful-science-behind-its-behavior-screening-program> (quoting ACLU attorney Hugh Handeyside); Larry Neumeister, *Judge Scolds Government over Iraq Detainee Abuse Pictures*, Associated Press (Jan. 18, 2017), <https://www.apnews.com/865c32eebf4d457499c017eb837b34dc> (quoting ACLU project director Hina Shamsi).

¹⁴ See, e.g., ACLU, *Bad Trip: Debunking the TSA’s ‘Behavior Detection’ Program* (2017), https://www.aclu.org/sites/default/files/field_document/dem17-tsa_detection_report-v02.pdf; Carl Takei, *ACLU-Obtained Emails Prove that the Federal Bureau of Prisons Covered Up Its Visit to the CIA’s Torture Site* (Nov. 22, 2016), <https://www.aclu.org/blog/speak-freely/aclu-obtained-emails-prove-federal-bureau-prisons-covered-its-visit-cias-torture>; Brett Max Kaufman, *Details Abound in Drone ‘Playbook’ – Except for the Ones That Really Matter Most* (Aug. 8, 2016), <https://www.aclu.org/blog/speak-freely/details-abound-drone-playbook-except-ones-really-matter-most>; ACLU, *Leaving Girls Behind: An Analysis of Washington D.C.’s “Empowering Males of Color” Initiative* (2016), <https://www.aclu.org/report/leaving-girls-behind>; Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida* (Feb. 22, 2015), <https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida>; Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights* (Oct. 30, 2015), <https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights>.

public about civil liberties issues and government policies that implicate civil rights and liberties.

The ACLU publishes a widely read blog where original editorial content reporting on and analyzing civil rights and civil liberties news is posted daily. See <https://www.aclu.org/blog>. The ACLU creates and disseminates original editorial and educational content on civil rights and civil liberties news through multi-media projects, including videos, podcasts, and interactive features. See <https://www.aclu.org/multimedia>. The ACLU also publishes, analyzes, and disseminates information through its frequently visited website, <https://www.aclu.org>. The website addresses civil rights and civil liberties issues in depth, provides features on civil rights and civil liberties issues in the news, and contains many thousands of documents relating to the issues on which the ACLU is focused. The ACLU's website also serves as a clearinghouse for news about ACLU cases, including analysis about case developments and an archive of case-related documents. Through these pages, and with respect to each specific civil liberties issue, the ACLU provides the public with educational material, recent news, analyses of relevant congressional or executive branch action, government documents obtained through FOIA requests, and further in-depth analytic and educational multi-media features.¹⁵

The ACLU website includes many features on information obtained through the FOIA. For example, the ACLU maintains an online "Torture Database," a compilation of over 100,000 pages of FOIA documents that allows researchers and the public to conduct sophisticated searches of its contents relating to government policies on rendition, detention, and

¹⁵ See, e.g., *ACLU v. ODNI*—FOIA Lawsuit Seeking Records About Government Surveillance Under the USA Freedom Act, ACLU Case Page, <https://www.aclu.org/cases/aclu-v-odni-foia-lawsuit-seeking-records-about-government-surveillance-under-usa-freedom-act>; *ACLU v. DOJ*—FOIA Lawsuit Seeking Information on Federal Agencies' Surveillance of Social Media, ACLU Case Page, <https://www.aclu.org/cases/aclu-v-doj-foia-lawsuit-seeking-information-federal-agencies-surveillance-social-media>; *ACLU v. DOJ*—FOIA Case for Records Relating to Targeted Killing Law, Policy, and Casualties, ACLU Case Page, <https://www.aclu.org/cases/aclu-v-doj-foia-case-records-relating-targeted-killing-law-policy-and-casualties>; Executive Order 12,333—FOIA Lawsuit, ACLU Case Page, <https://www.aclu.org/cases/executive-order-12333-foia-lawsuit>; ACLU Motions Requesting Public Access to FISA Court Rulings on Government Surveillance, ACLU Case Page, <https://www.aclu.org/cases/aclu-motions-requesting-public-access-fisa-court-rulings-government-surveillance>; FOIA Request for Justice Department Policy Memos on GPS Location Tracking, ACLU Case Page, <https://www.aclu.org/cases/foia-request-justice-department-policy-memos-gps-location-tracking>; Florida Stingray FOIA, ACLU Case Page, <https://www.aclu.org/cases/florida-stingray-foia>; Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida*, (Feb. 22, 2015) <https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida?redirect=blog/national-security-technology-and-liberty/aclu-obtained-documents-reveal-breadth-secretive-sting>.



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

interrogation.¹⁶ The ACLU has also published a number of charts and explanatory materials that collect, summarize, and analyze information it has obtained through the FOIA.¹⁷

The records requested are not sought for commercial use and the ACLU plans to analyze, publish, and disseminate the information disclosed as a result of this Request to the public at no cost.

B. The records sought are urgently needed to inform the public about actual or alleged government activity.

These records are urgently needed to inform the public about actual or alleged government activity. *See* 5 U.S.C. § 552(a)(6)(E)(v)(II).¹⁸ Specifically, the requested records relate to the purchase and use of cell phone location information by DHS, CBP, and ICE. Law enforcement's use of cell phone location information is already the subject of widespread public controversy and media attention,¹⁹ and the *Wall Street Journal's* new revelations about the



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

¹⁶ *The Torture Database*, ACLU Database, <https://www.thetorturedatabase.org>; *see also* *Countering Violent Extremism FOIA Database*, ACLU Database, <https://www.aclu.org/foia-collection/cve-foia-documents>; *TSA Behavior Detection FOIA Database*, ACLU Database, <https://www.aclu.org/foia-collection/tsa-behavior-detection-foia-database>; *Targeted Killing FOIA Database*, ACLU Database, <https://www.aclu.org/foia-collection/targeted-killing-foia-database>.

¹⁷ Summary of FISA Amendments Act FOIA Documents Released on November 29, 2010, ACLU (Nov. 29, 2010), https://www.aclu.org/files/pdfs/natsec/faafoia_20101129/20101129Summary.pdf; Index of Bush-Era OLC Memoranda Relating to Interrogation, Detention, Rendition and/or Surveillance, ACLU (Mar. 5, 2009), https://www.aclu.org/sites/default/files/pdfs/safe/free/olcmemos_2009_0305.pdf; Statistics on NSL's Produced by Department of Defense, ACLU, https://www.aclu.org/sites/default/files/field_document/nsl_stats.pdf.

¹⁸ *See also* 6 C.F.R. § 5.5(e)(1)(ii).

¹⁹ *See, e.g.,* Jose Pagliery, *ICE in New York Has a Spy Tool to Hunt Undocumented Immigrants Via Their Cell Phones*, Univision (Oct. 17, 2019), <https://www.univision.com/local/nueva-york-wxtv/ice-in-new-york-has-a-spy-tool-to-hunt-undocumented-immigrants-via-their-cell-phones>; Shirin Ghaffary, *The "Smarter" Wall: How Drones, Sensors, and AI Are Patrolling the Border*, Vox (May 16, 2019), <https://www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai> (updated Feb. 7, 2020); Ali Winston, *Did the Police Spy on Black Lives Matter Protesters? The Answer May Soon Come Out*, N.Y. Times (Jan. 14, 2019), <https://www.nytimes.com/2019/01/14/nyregion/nypd-black-lives-matter-surveillance.html>; Chantal Da Silva, *ICE Just Launched A \$2.4M Contract with a Secretive Data Surveillance Company That Tracks You In Real Time*, Newsweek (June 7, 2018), <https://www.newsweek.com/ice-just-signed-24m-contract-secretive-data-surveillance-company-can-track-you-962493>; Morgan Chalfant & Ali Breland, *'Stingray' Spying Prompts Fears About Surveillance*, Hill (June 6, 2018), <https://thehill.com/policy/national-security/390893-stingray-spying-prompts-fears-about-surveillance>; Robert Snell, *Feds Use Anti-Terror Tool to Hunt Undocumented Immigrants Amid Trump's Crackdown*, Detroit News (May 18, 2017), <https://www.detroitnews.com/story/news/local/detroitcity/2017/05/18/cell-snooping-fbi-immigrant/101859616>; Adolfo Flores, *DHS Has Used A Controversial Cell Phone-Tracking Device More Than 1,800 Times*, BuzzFeed News (Nov. 17, 2017),

purchase of this information from commercial vendors has resulted in further media scrutiny and calls for congressional hearings.²⁰ Representative Carolyn Maloney, who leads the House Committee on Oversight and Reform, has stated that the committee plans to “fully investigate this issue to ensure that Americans’ privacy is protected.”²¹ However, without access to information about DHS, CBP, and ICE policies and practices, lawmakers and the public cannot participate fully in the debate about whether and how acquisition and use of this information should be permitted. That debate is happening *now*, and there is a pressing need for the records sought in this Request.

Also of deep public concern are questions surrounding ICE and CBP operations targeting undocumented immigrants, including whether there are appropriate limits on agents’ discretion, whether particularly vulnerable populations are protected from unjustified targeting, and whether agents are using acceptable means to locate and detain people.²² Amid reports of increased arrests of undocumented immigrants by ICE and CBP under the current administration, there is a pressing need for accurate information about the means used by ICE and CBP to identify and locate immigrants whom the agencies seek to detain and potentially deport. The records sought relate to a matter of widespread and exceptional media interest: the government’s use of cell phone location information and the targeting of undocumented immigrants.



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

<https://www.buzzfeednews.com/article/adolfoflores/this-is-how-many-times-the-department-of-homeland-security>.

²⁰ See Tau & Hackman, *supra* note 2; Editorial, *Apps Are Selling Your Location Data. The U.S. Government is Buying.*, Wash. Post (Feb. 9, 2020), https://www.washingtonpost.com/opinions/apps-are-selling-your-location-data-the-us-government-is-buying/2020/02/09/9d09475e-49e2-11ea-b4d9-29cc419287eb_story.html; Editorial, *The Government Uses ‘Near Perfect Surveillance’ Data on Americans*, N.Y. Times (Feb. 7, 2020), <https://www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html>.

²¹ See Editorial, *The Government Uses ‘Near Perfect Surveillance’ Data on Americans*, *supra* note 20.

²² See, e.g., Daniel I. Morales, *et al.*, *DNA Collection at the Border Threatens the Privacy of All Americans*, N.Y. Times (Jan. 23, 2020), <https://www.nytimes.com/2020/01/23/opinion/dna-collection-border-privacy.html>; Hamed Aleaziz, *ICE Is Now Fingerprinting Immigrants As Young As 14 Years Old*, BuzzFeed News (Feb. 5, 2020), <https://www.buzzfeednews.com/article/hamedaleaziz/ice-immigration-customs-fingerprinting-refugees-teens>; Max Rivlin-Nadler, *How ICE Uses Social Media To Surveil and Arrest Immigrants*, Intercept (Dec. 22, 2019), <https://theintercept.com/2019/12/22/ice-social-media-surveillance>; McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. Times (Oct. 2, 2019), <https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html>; Sidney Fussell, *ICE and the Ever-Widening Surveillance Dragnet*, Atlantic (July 10, 2019), <https://www.theatlantic.com/technology/archive/2019/07/three-states-granted-ice-access-dmv-photos/593509>; Sam Levin, *US Uses Vast License Plate Database to Track Undocumented Immigrants*, Guardian (Mar. 13, 2019), <https://www.theguardian.com/us-news/2019/mar/13/us-immigration-ice-undocumented-immigrants-license-plates>.

Given the foregoing, ACLU has satisfied the requirements for expedited processing of this Request.

IV. Application for Waiver or Limitation of Fees

The ACLU requests a waiver of document search, review, and duplication fees on the grounds that disclosure of the requested records is in the public interest and because disclosure is “likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.” 5 U.S.C. § 552(a)(4)(A)(iii).²³ The ACLU also requests a waiver of search fees on the grounds that each organization qualifies as a “representative of the news media” and neither organization seeks the records for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

- A. *The Request is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the ACLU.*

As discussed above, media accounts underscore the substantial public interest in the records sought through this Request. *See supra* Section III.B. Given the ongoing and widespread media attention to immigration enforcement, as well as law enforcement’s use of cell phone location information, the records sought will significantly contribute to public understanding of matters of profound importance. Moreover, because so little information is publicly available concerning the government’s purchase and use of location data from commercial vendors, the records sought are critical to understanding the scope of this practice, the government’s purported legal justifications for it, and its broader implications for Fourth Amendment rights.

The ACLU is not filing this Request to further its respective commercial interest. As described above, any information disclosed by the ACLU as a result of this FOIA Request will be made available to the public at no cost. Thus, a fee waiver would fulfill Congress’s legislative intent in amending FOIA. *See Judicial Watch, Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) (“Congress amended FOIA to ensure that it be liberally construed in favor of waivers for noncommercial requesters.” (quotation marks omitted)).

- B. *The ACLU is a representative of the news media and the records are not sought for commercial use.*

The ACLU also requests a waiver of search fees on the basis that the ACLU qualifies as a “representative of the news media” and does not seek the

²³ *See also* 6 C.F.R. § 5.11(k)(1).



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

records for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).²⁴ The ACLU meets the statutory and regulatory definitions of a “representative of the news media” because it is an “entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience.” 5 U.S.C. § 552(a)(4)(A)(ii)(III)²⁵; *see also Nat’l Sec. Archive v. Dep’t of Defense*, 880 F.2d 1381, 1387 (D.C. Cir. 1989) (finding that an organization that gathers information, exercises editorial discretion in selecting and organizing documents, “devises indices and finding aids,” and “distributes the resulting work to the public” is a “representative of the news media” for purposes of the FOIA); *Serv. Women’s Action Network v. Dep’t of Defense*, 888 F. Supp. 2d 282 (D. Conn. 2012) (requesters, including ACLU, were representatives of the news media and thus qualified for fee waivers for FOIA requests to the Department of Defense and Department of Veterans Affairs); *ACLU of Wash. v. Dep’t of Justice*, No. C09-0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding that the ACLU of Washington is an entity that “gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience”); *ACLU*, 321 F. Supp. 2d at 30 n.5 (finding non-profit public interest group to be “primarily engaged in disseminating information”). The ACLU therefore is a “representative of the news media” for the same reasons that it is “primarily engaged in the dissemination of information.”

Furthermore, courts have found other organizations whose mission, function, publishing, and public education activities are similar in kind to the ACLU’s to be “representatives of the news media” as well. *See, e.g., Cause of Action v. IRS*, 125 F. Supp. 3d 145 (D.C. Cir. 2015); *Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 10–15 (finding non-profit public interest group that disseminated an electronic newsletter and published books was a “representative of the news media” for purposes of the FOIA); *Nat’l Sec. Archive*, 880 F.2d at 1387; *Judicial Watch, Inc. v. Dep’t of Justice*, 133 F. Supp. 2d 52, 53–54 (D.D.C. 2000) (finding Judicial Watch, self-described as a “public interest law firm,” to be a news media requester).²⁶ On account of these factors, fees associated with responding to FOIA requests are regularly waived for the ACLU as a “representative of the news media.”²⁷ As was true in those instances, the ACLU meets the requirements for a fee waiver here.

²⁴ *See also* 6 C.F.R. § 5.11(k)(2)(iii).

²⁵ *See also* 6 C.F.R. § 5.11(b)(6).

²⁶ Courts have found these organizations to be “representatives of the news media” even though they engage in litigation and lobbying activities beyond their dissemination of information and public education activities. *See, e.g., Elec. Privacy Info Ctr.*, 241 F. Supp. 2d 5; *Nat’l Sec. Archive*, 880 F.2d at 1387; *see also Leadership Conference on Human Rights*, 404 F. Supp. 2d at 260; *Judicial Watch, Inc.*, 133 F. Supp. 2d at 53–54.

²⁷ In August 2017, CBP granted a fee-waiver request regarding a FOIA request for records relating to a muster sent by CBP in April 2017. In May 2017, CBP granted a fee-

* * *

Pursuant to applicable statutes and regulations, the ACLU expects a determination regarding expedited processing within 10 days. *See* 5 U.S.C. § 552(a)(6)(E)(ii); 6 C.F.R. § 5.5(e)(4).

If the Request is denied in whole or in part, the ACLU asks that you justify all denials by reference to specific exemptions to FOIA. The ACLU expects the release of all segregable portions of otherwise exempt material. The ACLU reserves the right to appeal a decision to withhold any information or deny a waiver of fees.

Thank you for your prompt attention to this matter. Please furnish the applicable records to:

Nathan Freed Wessler
American Civil Liberties Union
125 Broad Street, 18th Floor
New York, New York 10004
T: 212-549-2500
F: 212-549-2654
nwessler@aclu.org

We affirm that the information provided supporting the request for expedited processing is true and correct to the best of our knowledge and belief. *See* 5 U.S.C. § 552(a)(6)(E)(vi).

waiver request regarding a FOIA request for documents related to electronic device searches at the border. In April 2017, the CIA and the Department of State granted fee waiver requests in relation to a FOIA request for records related to the legal authority for the use of military force in Syria. In March 2017, the Department of Defense Office of Inspector General, the CIA, and the Department of State granted fee waiver requests regarding a FOIA request for documents related to the January 29, 2017 raid in al Ghayil, Yemen. In May 2016, the FBI granted a fee waiver request regarding a FOIA request issued to the DOJ for documents related to Countering Violent Extremism Programs. In April 2013, the National Security Division of the DOJ granted a fee waiver request with respect to a request for documents relating to the FISA Amendments Act. Also in April 2013, the DOJ granted a fee-waiver request regarding a FOIA request for documents related to "national security letters" issued under the Electronic Communications Privacy Act. In August 2013, the FBI granted the fee-waiver request related to the same FOIA request issued to the DOJ. In June 2011, the DOJ National Security Division granted a fee waiver to the ACLU with respect to a request for documents relating to the interpretation and implementation of a section of the PATRIOT Act. In March 2009, the State Department granted a fee waiver to the ACLU with regard to a FOIA request for documents relating to the detention, interrogation, treatment, or prosecution of suspected terrorists.

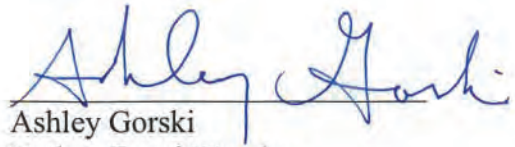


AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

Sincerely,



Ashley Gorski
Nathan Freed Wessler
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, New York 10004
T: 212-549-2500
F: 212-549-2654
agorski@aclu.org



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

From: KEVIN TYRRELL (IGL)
Sent: Fri, 2 Apr 2021 16:51:51 +0000
To: (b)(6); (IGL)
Subject: RE: PRIV RESPONSE RE REFERRAL TO USSS and USCG - ACLU v. DHS, et al. 20-10083

Thank you,

From: (b)(6); (IGL) (b)(6); @usss.dhs.gov>
Sent: Friday, April 2, 2021 12:15 PM
To: KEVIN TYRRELL (IGL) (b)(6); (b)(7)(C)
Subject: RE: PRIV RESPONSE RE REFERRAL TO USSS and USCG - ACLU v. DHS, et al. 20-10083

Correction: the hits for this file came back at 2,319. The search form from CIO is attached.

Thanks,

(b)(6);

From: KEVIN TYRRELL (IGL) (b)(6); (b)(7)(C)
Sent: Thursday, April 1, 2021 11:05 AM
To: (b)(6); (IGL) (b)(6); @usss.dhs.gov>
Subject: RE: PRIV RESPONSE RE REFERRAL TO USSS and USCG - ACLU v. DHS, et al. 20-10083

Ok, I will let DHS know, let's have them finish the search and hold the records as I'm sure this will come along soon.

From: (b)(6); (IGL) (b)(6); @usss.dhs.gov>
Sent: Thursday, April 1, 2021 11:00 AM
To: KEVIN TYRRELL (IGL) (b)(6); (b)(7)(C)
Subject: RE: PRIV RESPONSE RE REFERRAL TO USSS and USCG - ACLU v. DHS, et al. 20-10083

CIO's search hasn't finished yet and it has already pulled over 443,000 emails. So there are definitely records for Venntel, Inc.

Thanks,

(b)(6);
(b)(7)(C).

From: (b)(6); (IGL)
Sent: Thursday, April 1, 2021 9:39 AM
To: KEVIN TYRRELL (IGL) (b)(6); (b)(7)(C)
Subject: RE: PRIV RESPONSE RE REFERRAL TO USSS and USCG - ACLU v. DHS, et al. 20-10083

Got it!

Thanks,

(b)(6);

From: KEVIN TYRRELL (IGL) <(b)(6); (b)(7)(C)>
Sent: Thursday, April 1, 2021 9:27 AM
To: (b)(6); (IGL) (b)(6); @usss.dhs.gov>
Cc: KEVIN TYRRELL (IGL) (b)(6); (b)(7)(C)
Subject: RE: PRIV RESPONSE RE REFERRAL TO USSS and USCG - ACLU v. DHS, et al. 20-10083

Let's keep a note that file 20200991 and 20200711 also asked for info on Venntel put as part of a list of several key words.

I will let DHS know we might have records after all.

From: (b)(6); (IGL) (b)(6); @usss.dhs.gov>
Sent: Thursday, April 1, 2021 8:50 AM
To: KEVIN TYRRELL (IGL) (b)(6); (b)(7)(C)
Subject: RE: PRIV RESPONSE RE REFERRAL TO USSS and USCG - ACLU v. DHS, et al. 20-10083

These searches have been sent

Thanks,

(b)(6);

From: KEVIN TYRRELL (IGL) <(b)(6); (b)(7)(C)>
Sent: Thursday, April 1, 2021 7:32 AM
To: (b)(6); (IGL) (b)(6); @usss.dhs.gov>
Cc: KEVIN TYRRELL (IGL) (b)(6); (b)(7)(C)
Subject: FW: PRIV RESPONSE RE REFERRAL TO USSS and USCG - ACLU v. DHS, et al. 20-10083
Importance: High

Good Morning,

Can you expedite a records request to PRO to see if we have or ever had a contract with Venntel Inc. Also ask CIO to search to see if there is any email communication with Venntel Inc.

I suspect we will be getting a FOIA request very soon from ACLU on this.

From: (b)(6); (b)(7)(C) @hq.dhs.gov>
Sent: Wednesday, March 31, 2021 5:45 PM
To: (b)(6); (b)(7)(C) @uscg.mil>; KEVIN TYRRELL (IGL) (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C) @HQ.DHS.GOV>; (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) @hq.dhs.gov>

Subject: RE: PRIV RESPONSE RE REFERRAL TO USSS and USCG - ACLU v. DHS, et al. 20-10083

Importance: High

Good evening,

I've not had the chance to speak with either of you yet, but I joined DHS as its Director of FOIA Litigation in December. I believe you are the right contacts for this, but please let me know if I am mistaken.

This is regarding the attached request which is currently in litigation. I am also attaching the complaint.

PRIV did not refer the request at the administrative stage; it made a determination that request was not perfected. Now, there is a question of whether or not your components may have records relating to this request.

(b)(6); of OGC, (b)(6); (now Senior Director of FOIA litigation) and I have advised DOJ that we do not think it is proper to "refer" a FOIA request to component FOIA office when it is already in litigation. We asked DOJ to tell Plaintiff to submit new requests if they wish.

However, we have been asked by DOJ to confirm whether your components may have responsive records. Will you please let us know whether or not by tomorrow? Let us know if you have questions.

Thank you,

(b)(6);

(b)(6); (b)(7)(C)

Director

FOIA Litigation and Appeals

Privacy Office

U.S. Department of Homeland Security

Mobile: (b)(6);

Email: (b)(6); [@hq.dhs.gov](mailto:(b)(6);@hq.dhs.gov)



U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE

Washington, D.C. 20223

Freedom of Information Act and Privacy Act (FOIA/PA) Records Request

FOIA/PA Case Number:	20-10083	Request Date:	April 1, 2021	Suspense Date:	April 1, 2021
----------------------	-----------------	---------------	----------------------	----------------	----------------------

Office(s) Conducting Search	CIO	Office Point of Contact(s)	(b)(6); (b)(7)(C)
Program/Branch Task to Search	CIO	Person(s) Conducting Search	

FOIA/PA OFFICE CONTACT INFORMATION

FOIA/PA POC	(b)(6); (b)(7)(C)	Phone Number	N/A
-------------	-------------------	--------------	------------

REQUESTED RECORDS

Any and all communication with **Venntel, Inc.**

Date Range for Search: 1/1/2017 to 4/1/2021

Search Terms: emails including the term **"Venntel"**

*****Please expedite this request as it is in litigation*****

INSTRUCTIONS FROM FOIA/PA OFFICE

☒	Search your records for responsive document(s), and if located, provide one (1) clean copy to the FOIA/PA Program.
☒	Record the time spent reviewing and coordinating the request.
☒	Complete form and return via one of the following options: - interoffice mail - scan and email to foia@usss.dhs.gov - hand carry

COMMENTS SECTION

**Please contact the FOIA/PA Program with any questions and/or comments at
202-406-6370 or foia@uss.s.dhs.gov**

Directions for Conducting a Search for Records Requested under FOIA/PA

In responding to this request for information made pursuant to the Freedom of Information Act, 5 USC 552 and/or Privacy Act, 5 USC 552a, you must undertake a search that is *reasonably calculated to uncover all responsive materials* described in the request. You must search in ALL places where responsive records are likely to be found.

Once completed, this form will document the Agency's search efforts in this matter and may be utilized in a court of law.

Please conduct a thorough search of your records, both paper and electronic, for materials pertaining to this FOIA/PA request. You must search in every area within your components where responsive records may be located.

"Records" include: paper records, electronic records, E-mail correspondence, pictures, DVDs, video tapes, audio tapes, microfiche, or any other material recorded in any manner unless otherwise stated in the request.

Name of Individual(s) Conducting Search	Searcher's Grade/Level	Search Date	Total Search Time
(b)(6); (b)(7)(C)	GS-14	4/1/2021	overnight

SEARCHES CONDUCTED

DATABASES

List all databases searched	List the search terms used
Email Databases	Date Range for Search: 1/1/2017 to 4/1/2021 Search Terms: emails including the term "Venntel"

OTHER RECORDS AND LOCATIONS			
Did you search any other records or locations not listed above? (i.e., video, audio, microfiche, etc)	Yes ☐	No ☒	N/A ☐
Where did you search?			
How did you search?			
List the search terms used:			

WERE RESPONSIVE RECORDS LOCATED?	
☒ YES ☐ NO	If yes, please forward the responsive documents to the FOIA/PA Program

SENSITIVITY (IF RECORDS WERE LOCATED)			
Are any of the records classified or otherwise sensitive? (i.e., secret, LES, etc.)	Yes ☐	No ☐	
Please explain	To be determined by Liaison		
Are any of the records related to an ongoing open investigation?	Yes ☐	No ☐	
Please explain	To be determined by Liaison		

I certify that a search which was reasonably calculated to locate all materials responsive to this request has been conducted

Name of
Certifying Official

(b)(6); (b)(7)(C)

Title ATSAIC

Date 4/2/2021

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

AMERICAN CIVIL LIBERTIES UNION.

Plaintiff,

 $\mathbf{y}_i$

UNITED STATES DEPARTMENT OF
HOMELAND SECURITY; UNITED
STATES CUSTOMS AND BORDER
PROTECTION; and UNITED STATES
IMMIGRATION AND CUSTOMS
ENFORCEMENT.

Defendants.

Case No.

COMPLAINT

INTRODUCTION

1. The American Civil Liberties Union (“ACLU”) brings this action under the Freedom of Information Act (“FOIA”) to force the U.S. Department of Homeland Security (“DHS”), U.S. Customs and Border Protection (“CBP”), and U.S. Immigration and Customs Enforcement (“ICE”) (collectively, “Defendants” or “Defendant Agencies”) to release records about their purchases of cell phone location data for immigration enforcement and other purposes. Multiple news sources have confirmed these agencies’ purchase of access to databases containing precise location information for millions of people—information gathered by applications (“apps”) running on their smartphones. The agencies’ purchases raise serious concerns that they are evading Fourth Amendment protections for cell phone location information by paying for access instead of obtaining a warrant. Yet, more than nine months after the ACLU submitted its FOIA request (“the Request”), these agencies have produced no responsive records. The information

sought is of immense public significance, not only to shine a light on the government's use of powerful location-tracking data in the immigration context, but also to assess whether the government's purchase of this sensitive data complies with constitutional and legal limitations and is subject to appropriate oversight and control.

2. In *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018), the Supreme Court held that people have a reasonable expectation of privacy in the “all-encompassing record of the[ir] whereabouts” created when their cell phones interact with cellular service providers’ towers. The Court specified that “[a]lthough such records are generated for commercial purposes, that distinction does not negate [an individual’s] anticipation of privacy in his physical location.” *Id.* As a result, the Court held that “the Government must generally obtain a warrant supported by probable cause before acquiring such records.” *Id.* at 2221. The cell phone location information at issue in this suit—GPS coordinates captured by apps running on people’s phones, often without their knowledge, sold by the app providers to data aggregators, and then sold to law enforcement agencies—are no less revealing of individuals’ “privacies of life.” *Id.* at 2217. But while it has been widely reported that Defendant Agencies are acquiring this highly sensitive data without warrants, little is known about how they are using it, what controls are in place over such use, and how they square their practices with the *Carpenter* decision and other provisions of federal law.

3. The requested information is critical to informing the ongoing public debate about transparency and oversight of law enforcement as well as protection of vulnerable groups, such as immigrants and undocumented persons, from government abuses. In particular, there is deep public concern surrounding ICE and CBP operations targeting people for arrest, detention and deportation, including whether there are appropriate limits on agents’ discretion, whether

particularly vulnerable populations are being protected from unjustified targeting, and whether agents are using acceptable means to locate and detain people. Disclosure of the records that Plaintiff seeks through this action would contribute significantly to the public's understanding of how the Defendants use invasive surveillance technology both at the border and within American communities, and whether they are complying with constitutional and legal limitations on unreasonable searches. For example, "CBP officials [have] confirmed to Senate staff that the agency is using Venntel's location database to search for information collected from phones in the United States without any kind of court order," but the "agency refused a follow-up request for information about the legal analysis it conducted."¹ Without access to the records Plaintiff seeks, the public and lawmakers will lack information to engage in a fully informed debate about proper limits on Defendants' practices.

4. Plaintiff now asks the Court to issue an injunction requiring the Defendants to conduct adequate searches for records and produce responsive records. Plaintiff also seeks an order enjoining the Defendants from assessing fees for the processing of the Request.

JURISDICTION AND VENUE

5. This Court has jurisdiction pursuant to 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. § 1331.

6. Venue lies in the Southern District of New York pursuant to 5 U.S.C. § 552(a)(4)(B), including because it is the district in which the Plaintiff has its principal place of business.

PARTIES

7. The American Civil Liberties Union is a nationwide, non-profit, nonpartisan organization with its principal place of business in New York, New York. The ACLU's mission

¹ Letter from Sen. Ron Wyden, et al., to Hon. Joseph V. Cuffari, Inspector Gen., Dep't of Homeland Sec. (Oct. 23, 2020), <https://www.wyden.senate.gov/imo/media/doc/102320%20Wyden%20Warren%20Brown%20Markey%20Schatz%20Letter%20RE%20CBP%20Phone%20Tracking.pdf>.

is to maintain and advance civil rights and civil liberties and to ensure that the U.S. government acts in compliance with the Constitution and laws of the United States. Among the rights advanced by the ACLU that are implicated by the subject of the Request are the rights of people who are targeted, arrested, and detained by federal immigration authorities, the right to freedom of speech and association under the First Amendment, the right to be free of unreasonable government searches and seizures under the Fourth Amendment, and the right to due process under the Fifth and Fourteenth Amendments. The ACLU regularly publishes information and analysis concerning government activities derived from FOIA requests and other sources.

8. Defendant DHS is a federal agency within the meaning of 5 U.S.C. § 552(f)(1).

9. Defendant CBP is a component of DHS and is an agency within the meaning of 5 U.S.C. § 552(f)(1).

10. Defendant ICE is a component of DHS and is an agency within the meaning of 5 U.S.C. § 552(f)(1).

FACTS

Background: Defendants are Purchasing Access to Large Quantities of Cell Phone Location Data

11. On February 7, 2020, the *Wall Street Journal* reported that DHS has “bought access to a commercial database that maps the movements of millions of cellphones in America and is using it for immigration and border enforcement,” without obtaining a warrant.² This was the first time the media had reported on the federal government’s purchase of such data for law enforcement purposes. The report describes the commercial database, provided by Venntel Inc., as “one of the largest known troves of bulk data being deployed by law enforcement in the

² Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>.

U.S.”³ Subsequent reporting revealed that another company, Babel Street, was selling a similar database to CBP and ICE.⁴ Recently, *Buzzfeed News* reported on a DHS memorandum that purports to provide justification for Defendants’ warrantless acquisition and use of this data.⁵ Neither that memo, nor the other records concerning Defendants’ practices, have been publicly released.

The Records Requested

12. On February 10, 2020, Plaintiff submitted the Request to DHS, CBP, and ICE. A true and accurate copy of the Request is attached hereto as Exhibit A.

13. The Request sought seven categories of records, including:

- a. All contracts, memoranda of understanding, letters of commitment, licenses, subscription agreements, and other agreements with vendors, including but not limited to **Vennfel** Inc., concerning government access to or receipt of data from commercial databases containing cell phone location information.
- b. All communications with **Vennfel** Inc. and all communications discussing or mentioning **Vennfel** Inc.
- c. All policies, procedures, guidelines, formal or informal guidance, advisories, directives, training materials, presentations, and memoranda concerning: (1) Access to commercial databases containing cell phone location information; (2) Acquisition, processing, retention, use, or dissemination of cell phone location information purchased from a commercial vendor; (3) The anonymization and de-anonymization of cell phone location information purchased from a commercial vendor; (4) The use of cell phone location information purchased from a commercial vendor in civil immigration enforcement actions; (5) The use of evidence in any court application, trial, hearing, or other proceeding that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor; (6) The use

³ *Id.*

⁴ Charles Levinson, *Through Apps, Not Warrants, ‘Locate X’ Allows Federal Law Enforcement to Track Phones*, Protocol (Mar. 5, 2020), <https://www.protocol.com/government-buying-location-data>.

⁵ Hamed Aleaziz & Caroline Haskins, *DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People*, BuzzFeed News. (Oct. 30, 2020), <https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation>.

of “lead” or “tip” information that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor; and (7) The circumstances under which the government notifies defendants or respondents of the use of evidence that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor, including notice of the information’s provenance.

- d. All formal legal analysis concerning access to commercial databases containing cell phone location information, or the acquisition, processing, retention, use, or dissemination of cell phone location information purchased from a commercial vendor, including the application of *Carpenter v. United States*, 138 S. Ct. 2206 (2018), to this information.
- e. Records sufficient to show the volume of cell phone location data contained in the commercial databases for which DHS, CBP, and ICE have purchased access, and records sufficient to show the volume of data that the agencies have accessed from these databases.
- f. Records sufficient to show the number of times each year that DHS, CBP, and ICE employees or contractors have accessed commercial databases containing cell phone location information, or have used location data obtained from such databases.
- g. All records concerning the use of evidence in any court application, trial, hearing, or other proceeding that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor, including records concerning whether defendants or respondents received notice of the government’s reliance on such information and its provenance.

14. Plaintiff requested expedited processing of the request for records on the basis of a “compelling need” to “inform the public concerning actual or alleged Federal Government activity” pursuant to 5 U.S.C. § 552(a)(6)(E)(v)(II).

15. Plaintiff sought a waiver of search, review, and duplication fees on the ground that disclosure of the requested records is “in the public interest” and because it is “likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.” 5 U.S.C. § 552(a)(4)(A)(iii).

16. Plaintiff also sought a limitation of fees on the ground that Plaintiff qualifies as a “representative of the news media” and the records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Defendants’ Responses to the Request

CBP

17. On February 12, 2020, CBP sent Plaintiff a letter acknowledging receipt of the Request.

18. On March 6, 2020, CBP granted Plaintiff’s request for a fee waiver.

19. On April 23, 2020, CBP denied Plaintiff’s request for expedited processing.

20. On May 7, 2020, CBP sent Plaintiff an “interim response” letter stating that the agency was unable to respond to several categories of the Request. On May 8, 2020, CBP withdrew the May 7 letter and issued a “corrected interim response” letter that stated that “CBP is processing your request” and asserted that categories 5 and 6 of the request “fail to describe the records sought with sufficient particularity.” Via a May 8, 2020, email, CBP also inquired whether it “may proactively remove withheld in full documents which are protected pursuant to 5 USC 552(b)(5), such as deliberative, attorney-client privileged, and attorney-work product privileged records.”

21. On May 20, 2020, counsel for Plaintiff spoke by phone with Patrick Howard, Branch Chief of CBP’s FOIA Division, to discuss the issues raised by CBP’s May 8 communications. On May 21, 2020, counsel for Plaintiff emailed Mr. Howard to clarify and memorialize the matters discussed on the call. Specifically, Plaintiff:

- a. Stated that “we consent to the agency excluding draft documents withheld under the deliberative process privilege, but only if the agency is able to identify and

process a final version of the document. However, we do not consent to the exclusion of records that the agency seeks to withhold as subject to attorney-client or attorney-work-product privilege.”

- b. Offered substitute language for Categories 5 and 6 of the Request, specifically:
 - i. Category 5: Records reflecting the volume of cell phone location data contained in the commercial databases for which DHS, CBP, and ICE have purchased access, and records reflecting the volume of data that the agencies have accessed from these databases. Such records may include electronic communications, memoranda, marketing materials, responses to requests for proposals, contracts, memoranda of understanding, and similar documents. In responding to this category of the Request, the agency need not produce multiple records reflecting the same information.
 - ii. Category 6: Records reflecting the number of times each year that DHS, CBP, and ICE employees or contractors have accessed commercial databases containing cell phone location information, or have used location data obtained from such databases. Such records may include reports, presentations, procurement requests, memoranda, electronic communications between agency employees, with other agencies, or with private companies, and similar documents. In responding to this category of the Request, the agency need not produce multiple records reflecting the same information.
- c. Clarified the nature of the cell phone location information at issue in the Request.

22. Between May 21 and June 3, 2020, counsel for Plaintiff and Mr. Howard corresponded to clarify CBP’s obligations as to records withheld in full or in part under Exemption 5. On June 3, 2020, Mr. Howard stated via email that “I will be in touch if further questions come up.”

23. Plaintiff has received no further communication and no responsive records from CBP since June 3, 2020. A true and accurate copy of Plaintiff’s relevant correspondence with CBP is attached hereto as Exhibit B.

24. CBP possesses records responsive to the Request. Federal contracting records and press reports reveal that CBP has purchased access to cell phone location databases.

25. Plaintiff has exhausted administrative remedies with CBP.

DHS

26. On March 4, 2020, DHS sent Plaintiff a letter acknowledging receipt of the request and stating that the “request is too broad in scope or did not specifically identify the records which you are seeking.” The letter stated that “[t]his is not a denial of your request,” and invited submission of “a perfected request.”

27. On March 9, 2020, Plaintiff responded in detail via letter to DHS’s concerns about the scope and form of the request and explained why the request was sufficiently detailed and specific and why DHS was obligated to conduct a search for responsive records. Plaintiff also provided additional guidance to DHS regarding component offices that might possess responsive records, and about specific records for which the agency should search.

28. Plaintiff has received no further communication and no responsive records from DHS. DHS has not addressed Plaintiff’s request for expedited processing or a fee waiver. A true and accurate copy of Plaintiff’s relevant correspondence with DHS is attached hereto as Exhibit C.

29. DHS possesses records responsive to the Request. Federal contracting records and press reports reveal that DHS components have purchased access to cell phone location databases, and press reports state that DHS has produced a memorandum addressing the legal basis for the agency’s purchase and use of this data.

30. Plaintiff has exhausted administrative remedies with DHS.

ICE

31. On March 6, 2020, ICE acknowledged receipt of the Request, but did not address Plaintiff’s requests for expedited processing or fee waiver.

32. Plaintiff has received no further communication and no responsive records from ICE since March 6, 2020. A true and accurate copy of Plaintiff's relevant correspondence with ICE is attached hereto as Exhibit D.

33. ICE possesses records responsive to the Request. Federal contracting records and press reports reveal that ICE has purchased access to cell phone location databases.

34. Plaintiff has exhausted administrative remedies because ICE has failed to comply with the time limit for responding to FOIA requests.

CAUSES OF ACTION

35. Defendants have failed to produce records responsive to the Request.

36. Defendants' failure to promptly make available the records sought by the Request violates FOIA, 5 U.S.C. § 552(a)(3)(A), and Defendants' corresponding regulations.

37. Defendants' failure to conduct an adequate search for records responsive to the Request violates FOIA, 5 U.S.C. § 552(a)(3)(C), (D), and Defendants' corresponding regulations.

38. Plaintiff is entitled to a waiver of all search, review, processing, and duplication fees in connection with the Request, and ICE's and DHS's failure to grant Plaintiff's request for waiver and limitation of fees violates FOIA, 5 U.S.C. § 552(a)(4)(A), and Defendants' corresponding regulations.

39. Plaintiff has exhausted administrative remedies to the extent required by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff asks this Court to GRANT the following relief:

1. Order that Defendants shall conduct adequate searches for records responsive to the Request;

2. Order that Defendants shall produce all requested records forthwith, or alternatively on an expedited schedule established by the Court;
3. Enjoin Defendants from charging Plaintiff search, review, processing, and duplication fees in connection with responding to the Request;
4. Award Plaintiff costs and reasonable attorneys' fees in the action; and
5. Grant such other relief as the Court may deem just and proper.

Respectfully submitted,

/s/ Nathan Freed Wessler

NATHAN FREED WESSLER

ASHLEY GORSKI

American Civil Liberties Union Foundation

125 Broad Street, 18th Floor

New York, NY 10004

(212) 549-2500

nwessler@aclu.org

agorski@aclu.org

AMY BELSHER

ROBERT HODGSON

CHRISTOPHER DUNN

New York Civil Liberties Union Foundation

125 Broad St., 19th Floor

New York, NY 10004

(212) 607-3300

abelsher@nyclu.org⁶

December 2, 2020

⁶ Counsel thank ACLU Speech, Privacy, and Technology Project law-graduate fellow Shreya Tewari for her assistance in preparing this complaint.

February 10, 2020

U.S. Department of Homeland Security
Chief Privacy Officer/Chief FOIA Officer
The Privacy Office
245 Murray Lane, SW, Stop 0655
Washington, D.C. 20528-0655

U.S. Customs and Border Protection
FOIA Officer
90 K Street, NE
FOIA Division
Washington, D.C. 20229

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street, SW, Stop 5009
Washington, D.C. 20536-5009

**Re: FOIA Request Concerning Purchase and Use of Cell Phone
Location Data
(Expedited Processing Requested)**

To Whom It May Concern:

The American Civil Liberties Union and the American Civil Liberties Union Foundation (together, the “ACLU”)¹ submit this Freedom of Information Act request (the “Request”). The Request seeks records pertaining to the purchase of cell phone location data by the Department of Homeland Security (“DHS”), U.S. Customs and Border Protection (“CBP”), and Immigration and Customs Enforcement (“ICE”).

I. Background

On February 7, 2020, the *Wall Street Journal* reported that DHS has “bought access to a commercial database that maps the movements of millions of cellphones in America and is using it for immigration and border

¹ The American Civil Liberties Union Foundation is a 26 U.S.C. § 501(c)(3) organization that provides legal representation free of charge to individuals and organizations in civil rights and civil liberties cases, and educates the public about civil rights and civil liberties issues across the country. The American Civil Liberties Union is a separate non-profit, 26 U.S.C. § 501(c)(4) membership organization that educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analysis of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

enforcement,” without obtaining a warrant.² This is the first time the media has reported on the federal government’s purchase of such data for law enforcement purposes. The report describes the commercial database as “one of the largest known troves of bulk data being deployed by law enforcement in the U.S.”³

Contracting records show that, since 2017, DHS and its components have been purchasing licenses and subscriptions for location data from Venntel Inc.⁴ According to the *Wall Street Journal*, “Venntel” in turn, purchased the information from private marketing companies that sell the location data of millions of cellphones to advertisers.”⁵ The data sold by Venntel is apparently pseudonymised, meaning that data is linked to an alphanumeric identifier, not the name of the cell phone’s owner. However, it is trivially easy to identify particular individuals using their location information, by following their pattern of movements to and from their homes, or by pairing the data with publicly available information.⁶

The *Wall Street Journal* report explains that ICE has used Venntel data to help identify immigrants who were later arrested, and that CBP uses the information to identify “cellphone activity in unusual places, such as remote stretches of desert that straddle the Mexican border.”⁷

These developments raise serious concerns that DHS, CBP, and ICE are seeking to circumvent fundamental Fourth Amendment protections for cell phone location data. In 2018, the Supreme Court in *Carpenter v. United States* held that the government must get a warrant to obtain cell phone location history, given its highly sensitive and revealing nature. Despite this precedent, government lawyers have reportedly approved the purchase of cell phone location information from commercial databases, on the theory that “the Carpenter ruling doesn’t apply” to such purchases.⁸ But the government cannot evade the warrant requirement simply by purchasing information that it would otherwise be unable to obtain without judicial oversight.

² Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>.

³ *Id.*

⁴ *See id.*

⁵ *Id.*

⁶ *See id.*; see also Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>. (explaining that “it’s child’s play to connect real names to the dots that appear on the maps” of cell phone location data).

⁷ Tau & Hackman, *supra* note 2.

⁸ *Id.*



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

The ACLU submits this FOIA request to provide the public with information about the purchase and use of cell phone location information by DHS, CBP, and ICE.

II. Requested Records

The ACLU requests the following records from DHS, CBP, and ICE. This Request seeks records created on or after January 1, 2017:

1. All contracts, memoranda of understanding, letters of commitment, licenses, subscription agreements, and other agreements with vendors, including but not limited to Venntel Inc., concerning government access to or receipt of data from commercial databases containing cell phone location information.
2. All communications with Venntel Inc. and all communications discussing or mentioning Venntel Inc.
3. All policies, procedures, guidelines, formal or informal guidance, advisories, directives, training materials, presentations, and memoranda concerning:
 - a. Access to commercial databases containing cell phone location information;
 - b. Acquisition, processing, retention, use, or dissemination of cell phone location information purchased from a commercial vendor;
 - c. The anonymization and de-anonymization of cell phone location information purchased from a commercial vendor;
 - d. The use of cell phone location information purchased from a commercial vendor in civil immigration enforcement actions;
 - e. The use of evidence in any court application, trial, hearing, or other proceeding that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor;
 - f. The use of “lead” or “tip” information that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor; and



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

- g. The circumstances under which the government notifies defendants or respondents of the use of evidence that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor, including notice of the information's provenance.
4. All formal legal analysis concerning access to commercial databases containing cell phone location information, or the acquisition, processing, retention, use, or dissemination of cell phone location information purchased from a commercial vendor, including the application of *Carpenter v. United States*, 138 S. Ct. 2206 (2018), to this information.
5. Records sufficient to show the volume of cell phone location data contained in the commercial databases for which DHS, CBP, and ICE have purchased access, and records sufficient to show the volume of data that the agencies have accessed from these databases.
6. Records sufficient to show the number of times each year that DHS, CBP, and ICE employees or contractors have accessed commercial databases containing cell phone location information, or have used location data obtained from such databases.
7. All records concerning the use of evidence in any court application, trial, hearing, or other proceeding that consists of, was obtained from, or was derived from cell phone location information purchased from a commercial vendor, including records concerning whether defendants or respondents received notice of the government's reliance on such information and its provenance.

With respect to the form of production, *see* 5 U.S.C. § 552(a)(3)(B), the ACLU requests that responsive records be provided electronically in their native file format, if possible. Alternatively, the ACLU requests that the records be provided electronically in a text-searchable, static-image format (PDF), in the best image quality in the agency's possession, and that the records be provided in separate, Bates-stamped files.

III. Application for Expedited Processing

The ACLU requests expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E).⁹ There is a "compelling need" for these records, as defined in the statute, because the information requested is "urgen[tly]" needed by

⁹ *See also* 6 C.F.R. § 5.5(e).

organizations primarily engaged in disseminating information “to inform the public concerning actual or alleged Federal Government activity.” 5 U.S.C. § 552(a)(6)(E)(v)(II).

A. *The ACLU is an organization primarily engaged in disseminating information in order to inform the public about actual or alleged government activity.*

The ACLU is “primarily engaged in disseminating information” within the meaning of the statute. *See id.*¹⁰ Obtaining information about government activity, analyzing that information, and widely publishing and disseminating it to the press and public are critical and substantial components of the ACLU’s work and are among its primary activities. *See ACLU v. Dep’t of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004) (finding non-profit public interest group that “gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience” to be “primarily engaged in disseminating information”).¹¹

The ACLU regularly publishes *STAND*, a print magazine that reports on and analyzes civil liberties-related current events. The magazine is disseminated to 850,000 people. The ACLU also publishes regular updates and alerts via email to 3.9 million subscribers (both ACLU members and non-members). These updates are additionally broadcast to 4.8 million social media followers. The magazine as well as the email and social-media alerts often include descriptions and analysis of information obtained through FOIA requests.

The ACLU also regularly issues press releases to call attention to documents obtained through FOIA requests, as well as other breaking news,¹²

¹⁰ *See also* 6 C.F.R. § 5.5(e)(1)(ii).

¹¹ Courts have found that the ACLU as well as other organizations with similar missions that engage in information-dissemination activities similar to the ACLU are “primarily engaged in disseminating information.” *See, e.g., Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005); *ACLU*, 321 F. Supp. 2d at 29 n.5; *Elec. Privacy Info. Ctr. v. DOD*, 241 F. Supp. 2d 5, 11 (D.D.C. 2003).

¹² Press Release, ACLU, Federal Court Rules Gov’t Cannot Unilaterally Detain U.S. Resident Indefinitely (Dec. 13, 2019), <https://www.aclu.org/press-releases/federal-court-rules-government-cannot-unilaterally-detain-us-resident-indefinitely>; Press Release, ACLU, Federal Court Permanently Blocks Billions of Dollars in Border Wall Construction (June 28, 2019), <https://www.aclu.org/press-releases/federal-court-permanently-blocks-billions-dollars-border-wall-construction>; Press Release, ACLU, New Documents Reveal NSA Improperly Collected Americans’ Call Records Yet Again (June 26, 2019), <https://www.aclu.org/press-releases/new-documents-reveal-nsa-improperly-collected-americans-call-records-yet-again>; Press Release, ACLU, ACLU and Center for Media Justice Sue FBI for Records on Surveillance of Black Activists (Mar. 21, 2019), <https://www.aclu.org/press-releases/aclu-and-center-media-justice-sue-fbi-records-surveillance-black-activists>; Press Release, ACLU,



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

and ACLU attorneys are interviewed frequently for news stories about documents released through ACLU FOIA requests.¹³

Similarly, the ACLU publishes reports about government conduct and civil liberties issues based on its analysis of information derived from various sources, including information obtained from the government through FOIA requests. This material is broadly circulated to the public and widely available to everyone for no cost or, sometimes, for a small fee. ACLU national projects regularly publish and disseminate reports that include a description and analysis of government documents obtained through FOIA requests.¹⁴ The ACLU also regularly publishes books, “know your rights” materials, fact sheets, and educational brochures and pamphlets designed to educate the



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

New Documents Reveal Government Plans to Spy on Keystone XL Protesters (Sept. 4, 2018), <https://www.aclu.org/news/new-documents-reveal-government-plans-spy-keystone-xl-protesters>; Press Release, ACLU, ACLU Obtains Documents Showing Widespread Abuse of Child Immigrants in U.S. Custody (May 22, 2018), <https://www.aclu.org/news/aclu-obtains-documents-showing-widespread-abuse-child-immigrants-us-custody>; Press Release, ACLU, ACLU Files Lawsuits Demanding Local Documents on Implementation of Muslim Ban (Apr. 12, 2017), <https://www.aclu.org/news/aclu-files-lawsuits-demanding-local-documents-implementation-trump-muslim-ban>. Press Release, ACLU, U.S. Releases Drone Strike ‘Playbook’ in Response to ACLU Lawsuit (Aug. 6, 2016), <https://www.aclu.org/news/us-releases-drone-strike-playbook-response-aclu-lawsuit>.

¹³ See, e.g., Charlie Savage, *N.S.A. Gathered Domestic Calling Records It Had No Authority to Collect*, N.Y. Times (June 26, 2019), <https://www.nytimes.com/2019/06/26/us/telecom-nsa-domestic-calling-records.html> (quoting ACLU attorney Patrick Toomey); Rachel Frazin, *ACLU Sues FBI Over Black Activist Surveillance Records*, Hill (Mar. 21, 2019), <https://thehill.com/policy/national-security/fbi/435143-fbi-sued-over-black-activist-surveillance-records> (quoting ACLU attorney Nusrat Choudhury); Cora Currier, *TSA’s Own Files Show Doubtful Science Behind Its Behavioral Screen Program*, Intercept (Feb. 8, 2017), <https://theintercept.com/2017/02/08/tsas-own-files-show-doubtful-science-behind-its-behavior-screening-program> (quoting ACLU attorney Hugh Handeyside); Larry Neumeister, *Judge Scolds Government over Iraq Detainee Abuse Pictures*, Associated Press (Jan. 18, 2017), <https://www.apnews.com/865c32eebf4d457499c017eb837b34dc> (quoting ACLU project director Hina Shamsi).

¹⁴ See, e.g., ACLU, *Bad Trip: Debunking the TSA’s ‘Behavior Detection’ Program* (2017), https://www.aclu.org/sites/default/files/field_document/dem17-tsa_detection_report-v02.pdf; Carl Takei, *ACLU-Obtained Emails Prove that the Federal Bureau of Prisons Covered Up Its Visit to the CIA’s Torture Site* (Nov. 22, 2016), <https://www.aclu.org/blog/speak-freely/aclu-obtained-emails-prove-federal-bureau-prisons-covered-its-visit-cias-torture>; Brett Max Kaufman, *Details Abound in Drone ‘Playbook’ – Except for the Ones That Really Matter Most* (Aug. 8, 2016), <https://www.aclu.org/blog/speak-freely/details-abound-drone-playbook-except-ones-really-matter-most>; ACLU, *Leaving Girls Behind: An Analysis of Washington D.C.’s “Empowering Males of Color” Initiative* (2016), <https://www.aclu.org/report/leaving-girls-behind>; Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida* (Feb. 22, 2015), <https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida>; Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights* (Oct. 30, 2015), <https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights>.

public about civil liberties issues and government policies that implicate civil rights and liberties.

The ACLU publishes a widely read blog where original editorial content reporting on and analyzing civil rights and civil liberties news is posted daily. See <https://www.aclu.org/blog>. The ACLU creates and disseminates original editorial and educational content on civil rights and civil liberties news through multi-media projects, including videos, podcasts, and interactive features. See <https://www.aclu.org/multimedia>. The ACLU also publishes, analyzes, and disseminates information through its frequently visited website, <https://www.aclu.org>. The website addresses civil rights and civil liberties issues in depth, provides features on civil rights and civil liberties issues in the news, and contains many thousands of documents relating to the issues on which the ACLU is focused. The ACLU's website also serves as a clearinghouse for news about ACLU cases, including analysis about case developments and an archive of case-related documents. Through these pages, and with respect to each specific civil liberties issue, the ACLU provides the public with educational material, recent news, analyses of relevant congressional or executive branch action, government documents obtained through FOIA requests, and further in-depth analytic and educational multi-media features.¹⁵

The ACLU website includes many features on information obtained through the FOIA. For example, the ACLU maintains an online "Torture Database," a compilation of over 100,000 pages of FOIA documents that allows researchers and the public to conduct sophisticated searches of its contents relating to government policies on rendition, detention, and

¹⁵ See, e.g., *ACLU v. ODNI*—FOIA Lawsuit Seeking Records About Government Surveillance Under the USA Freedom Act, ACLU Case Page, <https://www.aclu.org/cases/aclu-v-odni-foia-lawsuit-seeking-records-about-government-surveillance-under-usa-freedom-act>; *ACLU v. DOJ*—FOIA Lawsuit Seeking Information on Federal Agencies' Surveillance of Social Media, ACLU Case Page, <https://www.aclu.org/cases/aclu-v-doj-foia-lawsuit-seeking-information-federal-agencies-surveillance-social-media>; *ACLU v. DOJ*—FOIA Case for Records Relating to Targeted Killing Law, Policy, and Casualties, ACLU Case Page, <https://www.aclu.org/cases/aclu-v-doj-foia-case-records-relating-targeted-killing-law-policy-and-casualties>; Executive Order 12,333—FOIA Lawsuit, ACLU Case Page, <https://www.aclu.org/cases/executive-order-12333-foia-lawsuit>; ACLU Motions Requesting Public Access to FISA Court Rulings on Government Surveillance, ACLU Case Page, <https://www.aclu.org/cases/aclu-motions-requesting-public-access-fisa-court-rulings-government-surveillance>; FOIA Request for Justice Department Policy Memos on GPS Location Tracking, ACLU Case Page, <https://www.aclu.org/cases/foia-request-justice-department-policy-memos-gps-location-tracking>; Florida Stingray FOIA, ACLU Case Page, <https://www.aclu.org/cases/florida-stingray-foia>; Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida*, (Feb. 22, 2015) <https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida?redirect=blog/national-security-technology-and-liberty/aclu-obtained-documents-reveal-breadth-secretive-sting>.



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

interrogation.¹⁶ The ACLU has also published a number of charts and explanatory materials that collect, summarize, and analyze information it has obtained through the FOIA.¹⁷

The records requested are not sought for commercial use and the ACLU plans to analyze, publish, and disseminate the information disclosed as a result of this Request to the public at no cost.

B. The records sought are urgently needed to inform the public about actual or alleged government activity.

These records are urgently needed to inform the public about actual or alleged government activity. *See* 5 U.S.C. § 552(a)(6)(E)(v)(II).¹⁸ Specifically, the requested records relate to the purchase and use of cell phone location information by DHS, CBP, and ICE. Law enforcement's use of cell phone location information is already the subject of widespread public controversy and media attention,¹⁹ and the *Wall Street Journal's* new revelations about the



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

¹⁶ *The Torture Database*, ACLU Database, <https://www.thetorturedatabase.org>; *see also Countering Violent Extremism FOIA Database*, ACLU Database, <https://www.aclu.org/foia-collection/cve-foia-documents>; *TSA Behavior Detection FOIA Database*, ACLU Database, <https://www.aclu.org/foia-collection/tsa-behavior-detection-foia-database>; *Targeted Killing FOIA Database*, ACLU Database, <https://www.aclu.org/foia-collection/targeted-killing-foia-database>.

¹⁷ Summary of FISA Amendments Act FOIA Documents Released on November 29, 2010, ACLU (Nov. 29, 2010), https://www.aclu.org/files/pdfs/natsec/faafoia_20101129/20101129Summary.pdf; Index of Bush-Era OLC Memoranda Relating to Interrogation, Detention, Rendition and/or Surveillance, ACLU (Mar. 5, 2009), https://www.aclu.org/sites/default/files/pdfs/safe/free/olcmemos_2009_0305.pdf; Statistics on NSL's Produced by Department of Defense, ACLU, https://www.aclu.org/sites/default/files/field_document/nsl_stats.pdf.

¹⁸ *See also* 6 C.F.R. § 5.5(e)(1)(ii).

¹⁹ *See, e.g.,* Jose Pagliery, *ICE in New York Has a Spy Tool to Hunt Undocumented Immigrants Via Their Cell Phones*, Univision (Oct. 17, 2019), <https://www.univision.com/local/nueva-york-wxtv/ice-in-new-york-has-a-spy-tool-to-hunt-undocumented-immigrants-via-their-cell-phones>; Shirin Ghaffary, *The "Smarter" Wall: How Drones, Sensors, and AI Are Patrolling the Border*, Vox (May 16, 2019), <https://www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai> (updated Feb. 7, 2020); Ali Winston, *Did the Police Spy on Black Lives Matter Protesters? The Answer May Soon Come Out*, N.Y. Times (Jan. 14, 2019), <https://www.nytimes.com/2019/01/14/nyregion/nypd-black-lives-matter-surveillance.html>; Chantal Da Silva, *ICE Just Launched A \$2.4M Contract with a Secretive Data Surveillance Company That Tracks You In Real Time*, Newsweek (June 7, 2018), <https://www.newsweek.com/ice-just-signed-24m-contract-secretive-data-surveillance-company-can-track-you-962493>; Morgan Chalfant & Ali Breland, *'Stingray' Spying Prompts Fears About Surveillance*, Hill (June 6, 2018), <https://thehill.com/policy/national-security/390893-stingray-spying-prompts-fears-about-surveillance>; Robert Snell, *Feds Use Anti-Terror Tool to Hunt Undocumented Immigrants Amid Trump's Crackdown*, Detroit News (May 18, 2017), <https://www.detroitnews.com/story/news/local/detroitcity/2017/05/18/cell-snooping-fbi-immigrant/101859616>; Adolfo Flores, *DHS Has Used A Controversial Cell Phone-Tracking Device More Than 1,800 Times*, BuzzFeed News (Nov. 17, 2017),

purchase of this information from commercial vendors has resulted in further media scrutiny and calls for congressional hearings.²⁰ Representative Carolyn Maloney, who leads the House Committee on Oversight and Reform, has stated that the committee plans to “fully investigate this issue to ensure that Americans’ privacy is protected.”²¹ However, without access to information about DHS, CBP, and ICE policies and practices, lawmakers and the public cannot participate fully in the debate about whether and how acquisition and use of this information should be permitted. That debate is happening *now*, and there is a pressing need for the records sought in this Request.

Also of deep public concern are questions surrounding ICE and CBP operations targeting undocumented immigrants, including whether there are appropriate limits on agents’ discretion, whether particularly vulnerable populations are protected from unjustified targeting, and whether agents are using acceptable means to locate and detain people.²² Amid reports of increased arrests of undocumented immigrants by ICE and CBP under the current administration, there is a pressing need for accurate information about the means used by ICE and CBP to identify and locate immigrants whom the agencies seek to detain and potentially deport. The records sought relate to a matter of widespread and exceptional media interest: the government’s use of cell phone location information and the targeting of undocumented immigrants.



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

<https://www.buzzfeednews.com/article/adolfoflores/this-is-how-many-times-the-department-of-homeland-security>.

²⁰ See Tau & Hackman, *supra* note 2; Editorial, *Apps Are Selling Your Location Data. The U.S. Government is Buying.*, Wash. Post (Feb. 9, 2020), https://www.washingtonpost.com/opinions/apps-are-selling-your-location-data-the-us-government-is-buying/2020/02/09/9d09475e-49e2-11ea-b4d9-29cc419287eb_story.html; Editorial, *The Government Uses ‘Near Perfect Surveillance’ Data on Americans*, N.Y. Times (Feb. 7, 2020), <https://www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html>.

²¹ See Editorial, *The Government Uses ‘Near Perfect Surveillance’ Data on Americans*, *supra* note 20.

²² See, e.g., Daniel I. Morales, *et al.*, *DNA Collection at the Border Threatens the Privacy of All Americans*, N.Y. Times (Jan. 23, 2020), <https://www.nytimes.com/2020/01/23/opinion/dna-collection-border-privacy.html>; Hamed Aleaziz, *ICE Is Now Fingerprinting Immigrants As Young As 14 Years Old*, BuzzFeed News (Feb. 5, 2020), <https://www.buzzfeednews.com/article/hamedaleaziz/ice-immigration-customs-fingerprinting-refugees-teens>; Max Rivlin-Nadler, *How ICE Uses Social Media To Surveil and Arrest Immigrants*, Intercept (Dec. 22, 2019), <https://theintercept.com/2019/12/22/ice-social-media-surveillance>; McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. Times (Oct. 2, 2019), <https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html>; Sidney Fussell, *ICE and the Ever-Widening Surveillance Dragnet*, Atlantic (July 10, 2019), <https://www.theatlantic.com/technology/archive/2019/07/three-states-granted-ice-access-dmv-photos/593509>; Sam Levin, *US Uses Vast License Plate Database to Track Undocumented Immigrants*, Guardian (Mar. 13, 2019), <https://www.theguardian.com/us-news/2019/mar/13/us-immigration-ice-undocumented-immigrants-license-plates>.

Given the foregoing, ACLU has satisfied the requirements for expedited processing of this Request.

IV. Application for Waiver or Limitation of Fees

The ACLU requests a waiver of document search, review, and duplication fees on the grounds that disclosure of the requested records is in the public interest and because disclosure is “likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.” 5 U.S.C. § 552(a)(4)(A)(iii).²³ The ACLU also requests a waiver of search fees on the grounds that each organization qualifies as a “representative of the news media” and neither organization seeks the records for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

- A. *The Request is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the ACLU.*

As discussed above, media accounts underscore the substantial public interest in the records sought through this Request. *See supra* Section III.B. Given the ongoing and widespread media attention to immigration enforcement, as well as law enforcement’s use of cell phone location information, the records sought will significantly contribute to public understanding of matters of profound importance. Moreover, because so little information is publicly available concerning the government’s purchase and use of location data from commercial vendors, the records sought are critical to understanding the scope of this practice, the government’s purported legal justifications for it, and its broader implications for Fourth Amendment rights.

The ACLU is not filing this Request to further its respective commercial interest. As described above, any information disclosed by the ACLU as a result of this FOIA Request will be made available to the public at no cost. Thus, a fee waiver would fulfill Congress’s legislative intent in amending FOIA. *See Judicial Watch, Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) (“Congress amended FOIA to ensure that it be liberally construed in favor of waivers for noncommercial requesters.” (quotation marks omitted)).

- B. *The ACLU is a representative of the news media and the records are not sought for commercial use.*

The ACLU also requests a waiver of search fees on the basis that the ACLU qualifies as a “representative of the news media” and does not seek the

²³ *See also* 6 C.F.R. § 5.11(k)(1).



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

records for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).²⁴ The ACLU meets the statutory and regulatory definitions of a “representative of the news media” because it is an “entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience.” 5 U.S.C. § 552(a)(4)(A)(ii)(III)²⁵; *see also Nat’l Sec. Archive v. Dep’t of Defense*, 880 F.2d 1381, 1387 (D.C. Cir. 1989) (finding that an organization that gathers information, exercises editorial discretion in selecting and organizing documents, “devises indices and finding aids,” and “distributes the resulting work to the public” is a “representative of the news media” for purposes of the FOIA); *Serv. Women’s Action Network v. Dep’t of Defense*, 888 F. Supp. 2d 282 (D. Conn. 2012) (requesters, including ACLU, were representatives of the news media and thus qualified for fee waivers for FOIA requests to the Department of Defense and Department of Veterans Affairs); *ACLU of Wash. v. Dep’t of Justice*, No. C09-0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding that the ACLU of Washington is an entity that “gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience”); *ACLU*, 321 F. Supp. 2d at 30 n.5 (finding non-profit public interest group to be “primarily engaged in disseminating information”). The ACLU therefore is a “representative of the news media” for the same reasons that it is “primarily engaged in the dissemination of information.”

Furthermore, courts have found other organizations whose mission, function, publishing, and public education activities are similar in kind to the ACLU’s to be “representatives of the news media” as well. *See, e.g., Cause of Action v. IRS*, 125 F. Supp. 3d 145 (D.C. Cir. 2015); *Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 10–15 (finding non-profit public interest group that disseminated an electronic newsletter and published books was a “representative of the news media” for purposes of the FOIA); *Nat’l Sec. Archive*, 880 F.2d at 1387; *Judicial Watch, Inc. v. Dep’t of Justice*, 133 F. Supp. 2d 52, 53–54 (D.D.C. 2000) (finding Judicial Watch, self-described as a “public interest law firm,” to be a news media requester).²⁶ On account of these factors, fees associated with responding to FOIA requests are regularly waived for the ACLU as a “representative of the news media.”²⁷ As was true in those instances, the ACLU meets the requirements for a fee waiver here.

²⁴ *See also* 6 C.F.R. § 5.11(k)(2)(iii).

²⁵ *See also* 6 C.F.R. § 5.11(b)(6).

²⁶ Courts have found these organizations to be “representatives of the news media” even though they engage in litigation and lobbying activities beyond their dissemination of information and public education activities. *See, e.g., Elec. Privacy Info Ctr.*, 241 F. Supp. 2d 5; *Nat’l Sec. Archive*, 880 F.2d at 1387; *see also Leadership Conference on Human Rights*, 404 F. Supp. 2d at 260; *Judicial Watch, Inc.*, 133 F. Supp. 2d at 53–54.

²⁷ In August 2017, CBP granted a fee-waiver request regarding a FOIA request for records relating to a muster sent by CBP in April 2017. In May 2017, CBP granted a fee-

* * *

Pursuant to applicable statutes and regulations, the ACLU expects a determination regarding expedited processing within 10 days. *See* 5 U.S.C. § 552(a)(6)(E)(ii); 6 C.F.R. § 5.5(e)(4).

If the Request is denied in whole or in part, the ACLU asks that you justify all denials by reference to specific exemptions to FOIA. The ACLU expects the release of all segregable portions of otherwise exempt material. The ACLU reserves the right to appeal a decision to withhold any information or deny a waiver of fees.

Thank you for your prompt attention to this matter. Please furnish the applicable records to:

Nathan Freed Wessler
American Civil Liberties Union
125 Broad Street, 18th Floor
New York, New York 10004
T: 212-549-2500
F: 212-549-2654
nwessler@aclu.org

We affirm that the information provided supporting the request for expedited processing is true and correct to the best of our knowledge and belief. *See* 5 U.S.C. § 552(a)(6)(E)(vi).

waiver request regarding a FOIA request for documents related to electronic device searches at the border. In April 2017, the CIA and the Department of State granted fee waiver requests in relation to a FOIA request for records related to the legal authority for the use of military force in Syria. In March 2017, the Department of Defense Office of Inspector General, the CIA, and the Department of State granted fee waiver requests regarding a FOIA request for documents related to the January 29, 2017 raid in al Ghayil, Yemen. In May 2016, the FBI granted a fee waiver request regarding a FOIA request issued to the DOJ for documents related to Countering Violent Extremism Programs. In April 2013, the National Security Division of the DOJ granted a fee waiver request with respect to a request for documents relating to the FISA Amendments Act. Also in April 2013, the DOJ granted a fee-waiver request regarding a FOIA request for documents related to "national security letters" issued under the Electronic Communications Privacy Act. In August 2013, the FBI granted the fee-waiver request related to the same FOIA request issued to the DOJ. In June 2011, the DOJ National Security Division granted a fee waiver to the ACLU with respect to a request for documents relating to the interpretation and implementation of a section of the PATRIOT Act. In March 2009, the State Department granted a fee waiver to the ACLU with regard to a FOIA request for documents relating to the detention, interrogation, treatment, or prosecution of suspected terrorists.

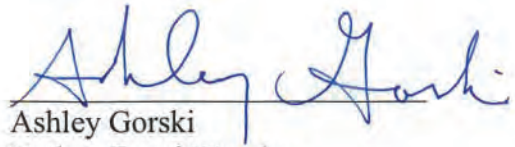


AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org

Sincerely,



Ashley Gorski
Nathan Freed Wessler
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, New York 10004
T: 212-549-2500
F: 212-549-2654
agorski@aclu.org



AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

LEGAL DEPARTMENT

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2564
aclu.org



INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

February 18, 2021

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Elizabeth Warren
United States Senate
309 Hart Senate Office Building
Washington, DC 20510

Dear Senator Wyden and Senator Warren:

This letter is in response to your September 24, 2020, correspondence to the Treasury Inspector General for Tax Administration (TIGTA) regarding concerns about the Internal Revenue Service (IRS) Criminal Investigation's (CI) use of a database provided by a contractor named **Venntel**. You requested TIGTA review CI's use of commercial databases containing peoples' location information, including but not limited to information from **Venntel**, and examine the legal analysis that IRS lawyers performed to authorize this practice with respect to *Carpenter v. United States*.¹ The *Carpenter* decision issued in June 2018 holds that the Government must generally obtain a search warrant supported by probable cause before acquiring cell-site location information (CSLI) from a wireless carrier.

We reviewed CI's purchase and use of the **Venntel** web-based subscription license of location information from cell phone users. According to the purchase order, the subscription was for one year from September 9, 2017, through September 8, 2018, at the cost of \$19,872. CI stated that the single-user license subscription was used exclusively by a single field office in the Cyber Crimes Unit, and **Venntel** was only utilized on a few specific occasions and did not produce effective results. According to CI, the last use of this database was in March 2018; however, the IRS did not track the subscription usage or maintain an access log.

Furthermore, we requested and obtained the two case files for which CI identified that its special agents used the **Venntel** subscription service. Our review of the CI-provided documents (which included case summaries, memoranda of interviews, communications with subjects, Currency Transaction Reports, Suspicious Activity Reports, and other information) from the two case files found no mention of the use of cell phone tracking data. Based on our review of case actions and results, we

¹ *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

concluded that the web-based subscription access to cell phone location information did not produce useful results and was not used as a significant tool in those two investigations. Our discussion of the cases with CI officials confirmed this conclusion.

Our effort also included a review of other web-based subscription services used by CI. CI provided us a listing of nineteen web-based subscriptions or products used for open source intelligence.² We researched each subscription and reviewed the associated purchase contract, if applicable. We found the subscriptions include a wide range of tools and some potentially include cell phone location data access as part of their offered services. We specifically identified eight web-based subscription contracts that CI has in place that, based on the broad use of contract terms, could theoretically cover cell phone data, although none of these contracts explicitly indicates that CI was contracting for cell phone data. This type of web-based subscription information is being marketed increasingly to both private and government entities for location tracking. However, CI officials clearly stated during our review that they are not currently using any web-based subscription services/tools similar to **Venntel** and have no plans at this time for using either Global Positioning Satellite (GPS) or CSLI cell phone data.

Our research indicates that two different kinds of location data can be collected from cell phones: CSLI collected by wireless carriers and GPS data mostly collected by applications ("Apps") running on cell phones and sold by marketers.³ The GPS cell phone data sold by marketers does not identify the owner of the phone by name or telephone number but rather by an alphanumeric code. The **Venntel** subscription service used by CI utilized GPS data. In contrast, the CSLI identifies the telephone number of the phone that is being tracked. In the *Carpenter* decision, the Court noted that while GPS data is more precise than CSLI data in terms of identifying the location of the user of the phone, the CSLI technology is rapidly approaching GPS-level precision.⁴

We requested information on IRS's legal analysis regarding the need for warrants in using the **Venntel** data. In response, IRS officials provided the following statement:

IRS-CI obtains a search warrant when conducting activity that would be considered a search under the Fourth Amendment. Before *Carpenter*, it was well-settled Supreme Court precedent that individuals could claim no legitimate expectation of privacy in information that was voluntarily turned over to a third party. With respect to the **Venntel** product, it is our

² According to CI, Open Source Intelligence (OSINT) is the collection and analysis of information that is gathered from public, or open, sources.

³ CI describes opt-in data as data that allows service providers (e.g., App creators) to collect information on the user. Cell-site location information refers to the information collected as a cell phone identifies its location to nearby cell towers.

⁴ *Carpenter*, at p. 2219.

understanding that the information available had been voluntarily turned over through individual permissions.

As noted in their statement, before the *Carpenter* decision, CI officials did not view GPS data, such as the information obtained from Venntel, as subject to the warrant requirement under the Fourth Amendment since the information obtained was voluntarily turned over by the phone user through individual permissions. In *Carpenter*, the Supreme Court rejected the use of CSLI data without a warrant for two reasons. First, the Court found that the information is not truly “voluntarily” shared as that term is commonly used since “[i]n the first place, cell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society.”⁵ Second, the Court found that the CSLI data is generated by virtually any activity on the cell phone (e.g., receiving e-mails and texts) and that short of turning off the cell phone, there is no way to avoid leaving a trail of CSLI. The *Carpenter* decision did not directly address the use of GPS data, but future courts may apply the same logic to limit the use of GPS data without a warrant.

We asked whether IRS Counsel provided CI with any written opinions or approvals related to the use of cell phone location data and were told that no such written opinions were given. We also requested the IRS’s position on the impact that *Carpenter* has on IRS’s use of commercial databases without a warrant. IRS officials stated the following:

Carpenter v. U.S. was decided in June 2018. The last known attempt to use the Venntel product was March 2018, before the Supreme Court decision. Nevertheless, it is our understanding that the *Carpenter* decision concerned historical Cell Site Location Information which is distinct from the opt-in app data available on the Venntel platform.

The above statement sets out CI’s position that data obtained from marketers of information like Venntel is not subject to a warrant because the data is collected by Apps loaded on cell phones to which the phone users voluntarily granted access. Our concern is that the Supreme Court rejected the Government’s argument in *Carpenter* that CSLI is truly voluntarily provided to the phone carriers. The Court’s rationale was that phone users do not truly voluntarily agree to share the information given the necessity of phones in our society. Courts may apply similar logic to GPS data sold by marketers, particularly if the Government identifies ways to translate the alphanumeric code to identify the phone’s owner or has other means of identifying the phone’s owner.

We shared this concern with CI and recommended to the IRS a periodic review of CI’s use of all types of cell phone information by the IRS’s Office of Chief Counsel. CI indicated that it is no longer using any cell phone-related data from any vendor because the data proved not to be useful in investigations. Further, CI indicated that under its previous procedures, it used local Area Counsel to evaluate legal issues such as the Fourth Amendment’s requirement to obtain warrants for the search and seizure

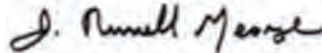
⁵ *Carpenter*, at p. 2220.

of information. CI now has changed its approach and has incorporated a national office review by Criminal Tax Counsel (who reports to the Office of Chief Counsel) to review whether new investigative tools (including cell phone-related data, if CI should ever resume vendor contracts for such data) require a warrant.

In conclusion, we found no evidence that the cell phone tracking data capability was widely used. In the two cases where the technology was used, it was determined to be ineffective, and the technology did not play a material role in the cases. According to CI officials, they no longer use cell phone data from vendor contracts; however, if CI should in the future resume the use of such data, CI will utilize its national office Criminal Tax Counsel to assess whether a warrant is required before obtaining the information.

If you have any questions or require further information regarding this matter, please do not hesitate to call me at [REDACTED], or have a member of our staff contact Michael McKenney, Deputy Inspector General of Audit, at [REDACTED]

Sincerely,



J. Russell George
Inspector General

From: (b)(6); (b)(7)(C) (IGL)
Sent: Wed, 9 Dec 2020 13:17:36 -0500
To: (b)(6); (b)(7)(C) (IGL)
Subject: FW: Subject access request (GDPR) - Secret Service

FYI.

From: Holzer, James
Sent: Monday, December 7, 2020 9:30 AM
To: (b)(6); (b)(7)(C) (IGL)
Subject: RE: Subject access request (GDPR) - Secret Service

Good morning (b)(6);

I'd thought you'd be interested in this article. This is the same guy who made the GDPR request to Secret Service.

[Vice reports it obtained documents showing **Venntel** gathers information from applications on mobile phones around the world. The government contractor sells location data to law enforcement agencies, including U.S. Immigration and Customs Enforcement and the Federal Bureau of Investigation. Journalist Martin Gundersen [requested](#) a copy of information **Venntel** had about him, receiving information on where he'd been 75,406 times. "Suddenly I could retrace my every step — on a hike, out for a drink, and visiting my grandmother in Southern Norway," he wrote. [Full Story](#)]

Regards,

James

James V.M.L. Holzer, DM, CIPP/G
Deputy Chief Privacy Officer
Department of Homeland Security



WARNING: This document is FOR OFFICIAL USE ONLY (FOUO); it contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

From: (b)(6); (b)(7)(C) (IGL)
Sent: Tuesday, November 17, 2020 11:33 AM
To: Holzer, James
Subject: Re: Subject access request (GDPR) - Secret Service

From: (b)(6); (b)(7)(C) @gmail.com>
Sent: Monday, November 2, 2020 6:06 AM
To: Privacy (b)(6); (b)(7)(C)
Subject: Subject access request (GDPR) - Secret Service

This is a transparency request under the General Data Protection Regulation, including a subject access request, a portability request, and other specific provisions.

I would like to request a copy of all my personal data held and/or undergoing processing. This is both a subject access request and a portability request.

The background for the request is media reports mentioning that your agency or similar agencies may use a tool by the company **Venntel**, Inc. or buy access to their location data. I have included all information needed to enable you to confirm whether you are processing personal data about me.

Copies of my personal data

Article 20

For data falling within the right to data portability (GDPR, art 20), which includes all data I have provided *and* which have been indirectly observed about me^[2] and where lawful bases for processing include consent or contract, I wish to have that data:

- **sent to me in commonly used, structured, machine-readable format**, such as a CSV file. A PDF is not a machine-readable format.^[3]
- accompanied with an **intelligible description of all variables**.

Article 15

For all personal data not falling within portability, I would like to request, under the right to access (GDPR, art 15):

- **a copy sent to me in electronic format**. This includes any data derived about me, such as opinions, inferences, settings and preferences.^[4] For data that is available to the controller in machine readable format, it must be provided to me in that form in accordance with the principle of fairness and provision of data protection by design.

If your organisation considers me a controller for whom you process

Furthermore, if your business considers me the controller of any personal data for which your business acts as processor, please provide me **with all the data you process on my behalf in machine readable format** in accordance with your obligation to respect my to determination of the means and purposes of processing.

Metadata on processing

This request also includes the metadata I am entitled to under the GDPR.

Information on controllers, processors, source and transfers

- The **identity of of all joint controllers** of my personal data.
- Any **third parties to whom data has been disclosed**, named with contact details in accordance with Article 15(1)(c). Please note that the European data protection regulators have stated that by default, controllers should name precise recipients and not "categories" of recipients. If they do choose to name categories, they must justify why this is fair, and be specific, naming "the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.^{[3][1]} Please note that in the case of any transferred data processed on the basis of consent, there is no option to just name categories of recipients without invalidating that legal basis.^[5]
- If any data was not collected, observed or inferred from me directly, **please provide precise information about the source of that data**, including the name and contact email of the data controller(s) in question ("from which source the personal data originate", Article 14(2)(f)/15(1)(g)).
- Please confirm where my personal data is physically stored (including backups) and at the very least **whether it has exited the EU at any stage (if so, please also detail the legal grounds and safeguards for such data transfers)**.

Information on purposes and legal basis

- All **processing purposes and the lawful basis for those purposes by category of personal data**. This list must be broken down by purpose, lawful basis aligned to purposes, and categories of data concerned aligned to purposes and lawful bases. Separate lists where these three factors do not correspond are not acceptable.^[6] A table may be the best way to display this information.
- The **specified legitimate interest** where legitimate interest is relied upon (Article 14(2)(b)).

Information on storage

- Please confirm for how long each category of personal data is stored, or the criteria used to make this decision, in accordance with the storage limitation principle and Article 15(1)(d).

To help identify me, I have attached the following personal information:

Name: (b)(6); (b)(7)(C)
Mmail: (b)(6); (b)(7)(C) [@gmail.com](#)

Nationality: **Norway**

Android Advertising ID: (b)(6); (b)(7)(C)

Phone model number:

Addresses linked to me:

Public

(b)(6); (b)(7)(C)

A copy of my driver's license has also been included to confirm my identity.

If you do not normally deal with these requests, please pass this email to your Data Protection Officer.

In accordance with the law, I look forward to hearing from you within one month of receipt.

Regards,

(b)(6); (b)(7)(C)

1. Information Commissioner's Office, 'Subject Access Code of Practice' (9 June 2017) p 13; Information Commissioner's Office, 'Guide to the GDPR: Right to access' (22 May 2019) (stating that 'even if you have a form, you should note that a subject access request is valid if it is submitted by any means, so you will still need to comply with any requests you receive in a letter, a standard email or verbally [...] although you may invite individuals to use a form, you must make it clear that it is not compulsory'). [↩](#)
2. Article 29 Working Party, *Guidelines on the Right to Data Portability (WP 242)* (13 December 2016) 8. [↩](#)
3. Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (WP260 rev.01, 11 April 2018). [↩](#) [↩](#)
4. Note that opinions, inferences and the like are considered personal data. See Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994, 34. [↩](#)
5. Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (WP259 rev.01, 10 April 2018) 13. [↩](#)
6. Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (WP260 rev.01, 11 April 2018), page 35. [↩](#)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other

disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6); (b)(7)(C) (LEG)
Sent: Tue, 1 Sep 2020 14:14:16 -0400
To: (b)(6); (b)(7)(C) (LEG)
Subject: RE: Wall Street Journal FOIA - Commercially available services or databases
Attachments: USSS-GC-FOIA (b)(6); (b)(7)(C) 0527 (004).pdf, (b)(6); (b)(7)(C) docx

(b)(5)

Regards,

(b)(6); (b)(7)(C)

Attorney-Advisor
Office of Chief Counsel
United States Secret Service

(b)(6); (b)(7)(C) (mobile)

(b)(6);

Reporter, Wall Street Journal
1025 Connecticut Ave NW, Suite 800
Washington, D.C. 20036

May 27, 2020

Subject: New Freedom of Information Act Request

United States Secret Service
Communications Center (FOIA/PA)
245 Murray Lane
Building T-5
Washington, D.C. 20223

VIA EMAIL

To whom it may concern,

My name is (b)(6); I'm a reporter that covers the Department of Justice, federal law enforcement, legal issues, and other matters for the *Wall Street Journal*.

This is a request under the Freedom of Information Act ("FOIA"). I request the department provide the following records within 20 business days:

- All legal memos or training materials in the possession of the U.S. Secret Service Office of the Chief Counsel concerning the use of commercially-available data or metadata products, services or databases, including but not limited to: anonymized mobile phone geolocation/GPS data, social media monitoring, data related to transaction or financial records or any other commercially-available data source or product.
- Any privacy impact assessment or other memorandum or document concerning privacy produced by the USSS Office of the Chief Counsel concerning the use of commercially-available data or metadata products, services or databases, including but not limited to: anonymized mobile phone geolocation/GPS data, social media feeds, transaction or financial records or any other commercially-available data source or product.
- Any records mentioning or pertaining to commercial software products sold by the private entities Babel Street, Venntel, Gravy Analytics, Geofeedia or Planet Risk in the possession of the U.S. Secret Service Office of the Chief Counsel.
- Failure to respond to this Request within the time period required by FOIA could serve as a constructive denial of the Request, and the Wall Street Journal may be deemed to have exhausted its administrative remedies. See 5 U.S.C. § 552(a)(6)(C)[i].

I request a search of records regardless of format or medium to include but not limited to: paper records, electronic records, audiotapes, videotapes, photographs, data, and graphical material. The request should be understood to include but not be limited: correspondence, letters, emails, text messages, facsimiles, telephone messages, voice mail messages, transcripts, notes, and minutes. The request should also be understood to include attachments and supporting documents.

Exclusion of media clippings or agency press releases

The agency may exclude any record that appears to consist solely of media clips or clippings from an internal or external media monitoring service in order to speed up processing time of this request. Records that consist of government officials commenting on or about news media clippings should not be excluded, nor should records that consist of interactions between government officials and members of the news media.

Vaughn index requested

If the agency's position is that records are exempt from disclosure, please provide an index as required under Vaughn v. Rosen 484 F.2d 820 (D.C. Cir. 1973.)

Search of personal devices and accounts requested

If any government employee used a personal account, device or other communications method or medium for any government activity, I request a search of those devices and accounts to see if they contain federal records.

Preservation hold requested

Please institute a preservation hold on any records responsive to this request. Acting either institutionally through the Wall Street Journal in consultation with legal counsel or as an individual in my personal capacity, I intend to pursue all legal avenues for my right of access to public records. The agency should be on notice that litigation is reasonably foreseeable.

Fee waiver requested

I am employed as a full-time reporter with The Wall Street Journal and therefore a member of the news media engaged primarily in the dissemination of information that is in the public's interest and hereby request a fee waiver. I certify that my statements concerning a fee waiver are true and correct to the best of my knowledge and belief.

If my fee waiver is denied, I am willing to pay up to **\$500** for favorable disposition of my request.

Expedited processing requested

I am employed as a full-time reporter with The Wall Street Journal. As a member of the news media engaged primarily in the dissemination of information that is in the public's interest, I hereby request expedited processing on the grounds that I am seeking information that is urgently needed to inform the public about the use of commercial data products by the U.S. government and their privacy impacts on Americans.

On Feb. 7, 2020, the Wall Street Journal reported on the U.S. federal government's purchase of commercially-available GPS location data of millions of U.S. cell phones through a company called **Venntel**, Inc.¹ On March 5, 2020, the publication Protocol reported that the US USSS has purchased access to such tools through a company called Babel Street — raising questions about the privacy impact on Americans and what kind of legal controls were being put on this kind of government surveillance program.² The records I seek go to the heart of the question about the government's legal authorization and privacy controls on such sensitive data.

I certify that my statements concerning the need for expedited processing are true and correct to the best of my knowledge and belief

Sincerely,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Federal Agencies Use Cellphone Location Data for Immigration Enforcement. WALL ST. J. (Feb. 7, 2020), <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>

(b)(6); (b)(7)(C) through apps, not warrants, 'Locate X' allows federal law enforcement to track phones. PROTOCOL (March 5, 2020), <https://www.protocol.com/government-buying-location-data>

From: (b)(6);@hq.dhs.gov (b)(6);@hq.dhs.gov> On Behalf Of WCM DHS
Sent: Thursday, August 20, 2020 12:40 AM
To: FOIA <Foia@uss.dhs.gov>
Subject: Form submission from: DHS FOIA / Privacy Act Request Submission Form

Submitted on Thursday, August 20, 2020 - 00:39 Submitted by user: Anonymous Submitted values are:

Select the DHS component you wish to submit your request to : United States Secret Service (USSS)

Title:

First Name: (b)(6);

Middle Initial:

Last Name (b)(6);

Suffix:

Email Address (b)(6); (b)(7)(C) requests.muckrock.com

Country: United States

Address 1: MuckRock News DEPT MR 101057

Address 2: 411A Highland Ave

City: Somerville

State: Massachusetts

Zip Code: 02144

Telephone Number (b)(6); (b)(7)(C)

Fax Number:

Are you requesting records on yourself? No If yes, you must check the perjury statement:

By initialing here you are providing your electronic signature.:

Please describe the records you are seeking as clearly and precisely as possible:

To Whom It May Concern:

Pursuant to the Freedom of Information Act, I hereby request the following records:

Background

A number of government agencies have purchased products that grant them access to location data generated by ordinary mobile phone apps installed on peoples' phones. An example of one of these purchases is described in this media report:

https://www.vice.com/en_us/article/jgk3g/secret-service-phone-location-data-babel-street

Products that sell these sorts of products to government clients include Venntel, Babel Street, and Anomaly Six.

My request concerns records related to these sorts of products.

Request

- Emails, memos, letters, directives, mentioning or referring to location data from apps, "Venntel," "Babel Street," "Anomaly Six," "Locate X," "Gravy Analytics."

- Legal opinions, legal guidance, legal memos mentioning or referring to location data from apps, from 1st January 2015 to the present.
- Any instruction manuals, user manuals, user guides, for "Locate X," or products from "Babel Street," "Anomaly Six," "Gravy Analytics," "Venntel."
- Any presentation slides, powerpoint slides for "Venntel," "Babel Street," "Anomaly Six," "Locate X," "Gravy Analytics."

Please provide any cross-referenced records relevant to my inquiry.

In order to help to determine my status to assess fees, you should know that I am a journalist writing for Motherboard, the technology section of VICE, and that this request is being made as part of news gathering.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 20 business days, as the statute requires.

Sincerely,

(b)(6); (b)(7)(C)

Upload documents directly:

https://https://www.muckrock.comhttps://accounts.muckrock.com/accounts/login/?url_auth_token=AAjy-FAQM1KXzns09svsFIL5Ac%3A1k8cJ6%3AAnsfnFLDiQm7WoFWSUw6y1eEQS5o&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Funit-ed-states-secret-service-71%252Flegal-documents-on-location-data-products-united-states-secret-service-101057%252F%253F

I am willing to pay fees for this request up to the amount of: \$: 25 Select from the list below: A representative of the news media seeking information as part of a news gathering effort and not for commercial use.

I request a waiver of all fees for this request.: I request a waiver of all fees for this request.

Please provide an explanation for your request for a fee waiver:

In order to help to determine my status to assess fees, you should know that I am a journalist writing for Motherboard, the technology section of VICE, and that this request is being made as part of news gathering.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

Please select and describe in detail if you believe your request warrants expeditious handling:

Please provide information to support your selection:

From: (b)(6); (b)(7)(C) LEG
Sent: Tue, 1 Sep 2020 13:54:03 -0400
To: (b)(6); (b)(7)(C) LEG
Subject: FW: FOIA Assistance
Attachments: USSS-GC-FOIA (b)(6) 0527 (004).pdf

(b)(5)

Regards,

(b)(6); (b)(7)(C)

Attorney-Advisor
Office of Chief Counsel
United States Secret Service

(b)(6); (b)(7)(C) mobile)

From: (b)(6); (b)(7)(C) (LEG)
Sent: Tue, 1 Sep 2020 13:50:21 -0400
To: (b)(6); (b)(7)(C) (LEG)
Subject: FW: FOIA Assistance
Attachments: USSS-GC-FOIA-(b)(6)0527 (004).pdf

(b)(5)

(b)(6); (b)(7)(C)

Attorney-Advisor
Office of Chief Counsel
United States Secret Service

(b)(6); (b)(7)(C) (mobile)

From: (b)(6); (b)(7)(C) (LEG)
Sent: Monday, June 1, 2020 1:42 PM
To: (b)(6); (b)(7)(C) (LEG)
Subject: FOIA Assistance

(b)(5)

(b)(6); (b)(7)(C)

Attorney-Advisor

Office of Chief Counsel

United States Secret Service

(b)(6); (b)(7)(C) (mobile)

If my fee waiver is denied, I am willing to pay up to **\$500** for favorable disposition of my request.

Expedited processing requested

I am employed as a full-time reporter with The Wall Street Journal. As a member of the news media engaged primarily in the dissemination of information that is in the public's interest, I hereby request expedited processing on the grounds that I am seeking information that is urgently needed to inform the public about the use of commercial data products by the U.S. government and their privacy impacts on Americans.

On Feb. 7, 2020, the Wall Street Journal reported on the U.S. federal government's purchase of commercially-available GPS location data of millions of U.S. cell phones through a company called Venntel, Inc.¹ On March 5, 2020, the publication Protocol reported that the US USSS has purchased access to such tools through a company called Babel Street — raising questions about the privacy impact on Americans and what kind of legal controls were being put on this kind of government surveillance program.² The records I seek go to the heart of the question about the government's legal authorization and privacy controls on such sensitive data.

I certify that my statements concerning the need for expedited processing are true and correct to the best of my knowledge and belief

Sincerely,

(b)(6); (b)(7)(C)

¹ Byron Tau and Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*. WALL ST. J. (Feb. 7, 2020), <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>

² Charles Levinson, *Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones*. PROTOCOL (March 5, 2020), <https://www.protocol.com/government-buying-location-data>

From: (b)(6); (b)(7)(C) @hq.dhs.gov>
Sent: Tuesday, March 10, 2020 10:08 AM
To: (b)(6); (b)(7)(C) @hq.dhs.gov>
Subject: FYSA: Protocol Article

This is what LLV was talking about during our meeting.

From: EDNA RUCKER (LIA) (b)(6); (b)(7)(C)
Sent: Tuesday, March 10, 2020 9:25 AM
To: (b)(6); (b)(7)(C) @hq.dhs.gov>
Cc: (b)(6); (b)(7)(C) @hq.dhs.gov>; (b)(6); (b)(7)(C) @hq.dhs.gov>
Subject: RE: Protocol Article

(b)(6);

So far I found out that TAKS does not use Locate X but I think we may use it internally on or USSS phones.

Stay tuned,

Gayle Rucker

(b)(6);

From: (b)(6); (b)(7)(C) @hq.dhs.gov>
Sent: Monday, March 9, 2020 2:44 PM
To: EDNA RUCKER (LIA) (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C) @hq.dhs.gov>; (b)(6); (b)(7)(C) @hq.dhs.gov>
Subject: Protocol Article

Hi Gayle,

Did you see the article below? It specifically calls out USSS as a user of Locate X. Is USSS using this service? As you may already know, OGC is currently working on an opinion regarding the use of AdID location tracking (from when it started coming out that the Department was working with Venntel).

(b)(6);
(b)(7)(C);

<https://www.protocol.com/government-buying-location-data>

Through apps, not warrants, ‘Locate X’ allows federal law enforcement to track phones

Federal agencies have big contracts with Virginia-based Babel Street. Depending on where you've traveled, your movements may be in the company's data.

[Charles Levinson](#)

March 5, 2020

U.S. law enforcement agencies signed millions of dollars worth of contracts with a Virginia company after it rolled out a powerful tool that uses data from popular mobile apps to track the movement of people's cell phones, according to federal contracting records and six people familiar with the software.

The product, called Locate X and sold by [Babel Street](#), allows investigators to draw a digital fence around an address or area, pinpoint mobile devices that were within that area, and see where else those devices have traveled, going back months, the sources told Protocol.

They said the tool tracks the location of devices anonymously, using data that popular cell phone apps collect to enable features like mapping or targeted ads, or simply to sell it on to data brokers.

Get what matters in tech, in your inbox every morning. [Sign up for Source Code.](#)

Babel Street has kept Locate X a secret, not mentioning it in public-facing marketing materials and stipulating in federal contracts that even the existence of the data is "confidential information." Locate X must be "used for internal research purposes only," according to [terms of use](#) distributed to agencies, and law enforcement authorities are forbidden from using the technology as evidence — or mentioning it at all — in legal proceedings.

Federal records show that U.S. Customs and Border Protection purchased Locate X, and the Secret Service and U.S. Immigration and Customs Enforcement also use the location-tracking technology, according to a former Babel Street employee. Numerous other government agencies have active contracts with Reston-based Babel Street, records show, but publicly available contract information does not specify whether other agencies besides CBP bought Locate X or other products and services offered by the company.

None of the federal agencies, including CBP, would confirm whether they used the location-tracking software when contacted by Protocol. Babel Street's other products include an analytics

tool it has widely marketed that sifts through streams of social media to "chart sentiment" about topics and brands.

A former government official familiar with Locate X provided an example of how it could be used, referring to the aftermath of a car bombing or kidnapping. Investigators could draw what is known as a geo-fence around the site, identify mobile devices that were in the vicinity in the days before the attack, and see where else those devices had traveled in the days, weeks or months leading up to the attack, or where they traveled afterward.

"If you see a device that a month ago was in Saudi Arabia, then you know maybe Saudis were involved," this person said. "It's a lead generator. You get a data point, and from there you use your other resources to figure out if it's valid."

A former Babel Street employee said the technology was deployed in a [crackdown on credit card skimming](#), in which thieves install illegal card readers on gas station pumps, capturing customers' card data to use or sell online. The Secret Service was the lead agency in those investigations, which, according to published reports, led to arrests and the seizure of devices.

A spokesperson for the Secret Service declined to comment on its work with Babel Street, saying the agency does not reveal methods used to carry out missions.

While federal records show that CBP purchased Locate X and last year upgraded, paying for "premium" licenses, the records neither describe what Locate X does nor define the difference between a basic and premium license. A CBP spokesperson would not comment in detail about the use of the tool, but said the agency follows the law when deploying "open-source information."

Told of Protocol's reporting on Babel Street, Sen. Ron Wyden, a Democrat from Oregon who has pushed for tougher privacy legislation, questioned whether uses of the technology might violate the Fourth Amendment ban on unreasonable searches.

The Supreme Court, in the landmark case [Carpenter v. United States](#), ruled in June 2018 that the government must obtain a search warrant to access cell-tower location data for individual phone accounts. The court "recognized that the government needs a warrant to get someone's location data," Wyden said. "Now the government is using its checkbook to try to get around Carpenter. Americans won't stand for that kind of loophole when it comes to our Fourth Amendment rights."

A spokesperson for Babel Street, Lacy Talton, declined to answer specific questions about the company's government sales or its Locate X technology, but said the firm handles data carefully to comply with both the law and internet terms of service. There is no indication Babel Street is doing anything illegal.

Sen. Ron Wyden said the U.S. Supreme Court has "recognized that the government needs a warrant to get someone's location data." Photo: Sarah Silbiger via Getty Images

"Although data content is freely available without restriction from thousands of vendors and suppliers, Babel Street employs a variety of measures to ensure appropriate use of the data," Talton said in a statement to Protocol. "This is not required by most vendors but stems from Babel Street's ethos of proper data compliance. The company regularly ensures that the data accessed through its software is in compliance with ever-changing global privacy regulations, data use rights, and terms of service."

The details of Babel Street's location-tracking technology and its contracts with the federal government have not been reported before. Last month, [The Wall Street Journal reported](#) that border and immigration agents were tracking the location of cell phones, and looking for activity in suspicious places near the border, after buying data from [Venntel Inc.](#) of Herndon, Virginia.

Venntel is a subsidiary of location-based marketing company Gravy Analytics of Dulles, Virginia. Gravy Analytics has provided location data to Babel Street, according to former employees of both firms.

Taken together, the revelations suggest that the sale of personal location data from commercial firms to the government is more widespread and has been going on longer than previously known. The emergence of the technology comes amid growing, broader concern over the tracking of people's movements, whether through [facial recognition](#), their [license plates](#) or the phones in their pockets.

While consumers enable location-based services on their cell phone apps, privacy advocates said people are generally unaware of how far their personal information could travel — and in particular that it could be piped to law enforcement.

The sources who spoke to Protocol, who independently described the location-tracking technology, were three former Babel Street employees, a former government official with firsthand knowledge of the company's products, and two former employees of Gravy Analytics. They requested anonymity because the information is sensitive, and some feared retribution from employers for speaking to the media.

A spokesperson for Gravy Analytics declined to comment on the company's relationship with Babel Street. She said [Venntel](#) is a "wholly owned subsidiary of Gravy Analytics that supports public sector initiatives."

She pointed to the company's [privacy policy](#) on its Web site: "We take consumer privacy seriously and ensure that our data platform remains fully transparent and compliant with industry and legal requirements," the policy reads. "Gravy ensures that 100% of our data complies with all local privacy laws, including required consumer consent and opt-out provisions."

From brand to threat management

While there is little public information about Locate X, government contracting records provide a picture of Babel Street's growth and increasing popularity in federal law enforcement circles. The company [registered Locate X](#) with the U.S. Patent and Trademark Office in May 2017, and

sales to federal agencies shot up afterward — from \$64,000 in fresh contracts in 2016 to more than \$2.1 million in 2017 to nearly \$5.3 million in 2018.

Babel Street's sales spike was fueled in large part by four new customers: CBP, which signed \$3.2 million in contracts, ICE (\$1.1 million), the State Department's Bureau of Diplomatic Security (\$710,000), and the Secret Service's Criminal Investigations Division (\$313,858), the records show.

CBP signed a [first contract worth \\$981,000](#) for "Babel software" in September 2017. The Targeting and Analysis Systems Directorate, the CBP branch that purchased the software, apparently liked what it received. A year later, the [agency signed a fresh contract](#) worth \$2.2 million for "Babel software licenses." In March 2019, CBP [filed an amended contract](#), worth an extra \$130,000, to "upgrade the current Babel Street Locate X licensing from basic to premium licenses as well as add an additional 10 licenses."

Asked about its use of Locate X, a CBP spokesperson told Protocol the agency uses a "variety of tools" that "may include tools to facilitate access to open-source data relevant to its border security mission. All CBP operations in which open-source information may be used are undertaken in furtherance of CBP's responsibility to enforce U.S. law at the border and in accordance with relevant legal, policy and privacy requirements."

In September 2018, ICE officials [signed a one-year, \\$1.1 million contract](#) with Babel Street. The deal included Locate X, according to a former Babel Street employee. Last August, [ICE signed a fresh five-year deal](#) worth up to \$6.5 million with Babel Street for "data subscription services," records show.

A spokesperson for ICE said, "We do not discuss specific law enforcement tactics or techniques, or discuss the existence or absence of specific law-enforcement-sensitive capabilities." She also said, referring to cell phone location data, "ICE does not generally use this type of information for routine enforcement operations."

Other agencies with active Babel Street contracts include the Department of Justice, the U.S. Marshals Service, the Army, the Coast Guard, the Drug Enforcement Administration and the Department of Transportation's Office of Intelligence, Security and Emergency Response. The contract records are from [USAspending.gov](#), the official source for U.S. government spending.

A spokesperson for the Department of Transportation, which signed a yearlong contract with Babel Street last May, said the Office of Intelligence, Security and Emergency Response "utilizes Babel Street software features depending on the nature of particular incidents."

Spokespeople for the Army, the Bureau of Diplomatic Security, the DEA and the Marshals Service declined to comment on the contracts with Babel Street. The Department of Justice and the Coast Guard did not respond to requests for comment.

A spokesperson for a regional DEA office in El Paso, Texas, which signed a separate \$12,978 contract for a one-year Babel Street software license last September, denied that the agency had purchased the location-tracking data tool.

The technology was controversial enough that some agencies, including the FBI and the ATF, declined to purchase Locate X after those agencies' lawyers nixed it, a former Babel Street employee said.

A spokesperson for the FBI declined to comment. A spokesperson for the ATF, April Langwell, declined to comment on ATF procurement decisions. "ATF always works within DOJ guidelines with regard to the investigative techniques that we use and ensure that they are consistent with federal law and subject to court approval," Langwell said.

The former Babel Street employees and the former government official said Babel Street was careful about its clients for location data technology. For example, they said, it did not sell to commercial clients, local law enforcement agencies or foreign governments.

The software included pop-ups that reminded users it was to be used only in the investigation of serious crimes and matters of national security, one former employee said. However, after users complained that the pop-ups were annoying, the company removed them, the employee said. Babel Street did not respond to emailed questions about the pop-ups.

Secrecy to the extreme

Despite the apparent power of the tool, Protocol could not find a single instance in which a federal agency had publicly described using Locate X, in an investigation or in any other capacity. And Babel Street appears to have taken a number of steps to keep the technology secret. The company advertises other products on its website and in press releases, but makes no mention of Locate X or the tracking of mobile devices.

Locate X's terms of use, spelled out in a single [document](#) published online by the General Services Administration, require government clients to agree that the product "will be used for internal research purposes only. Locate X data may not be used as the basis for any legal process in any country, including as the basis for a warrant or subpoena, or any other legal or administrative action." The terms state that Locate X data may not be "cited in any court/investigation-related document."

2. Locate X Data. EIS, as Reseller to Babel Street, shall provide the Locate X Data to Customer pursuant to the terms of the applicable Order Form. For avoidance of doubt, Locate X Data constitutes a "Data Feed" as defined in the Terms and, as such, shall be subject to the applicable Terms. In addition, the following additional terms shall also apply to the Locate X Data:

2.1. The existence and terms and conditions of this Addendum, and the Locate X Data in its entirety, shall be considered "Confidential Information" of Babel Street subject to the Terms. In addition, notwithstanding Section 9.1 of the Terms, Locate X Data may not be disclosed by Customer to any third party (including consultants, advisors, and/or independent contractors) without the prior written consent of an authorized representative of Babel Street; and

2.2. Any and all Locate X Data, including, but not limited to, results generated by Customer's use of the Locate X Data, will be used for internal research purposes only. Locate X Data may not be used as the basis for any legal process in any country, including as the basis for a warrant, subpoena, or any other legal or administrative action (nor may the Locate X Data be cited in any court/investigation-related document).

Terms of use for Babel Street's Locate X product state that the data "may not be used as the basis for any legal process." Illustration: 615 Productions

Protocol shared the terms of use in the Locate X contract with Nathan Wessler, a lawyer with the ACLU's Speech, Privacy, and Technology Project who argued the *Carpenter v. United States* case before the Supreme Court. He called the secrecy provisions "tremendously disturbing," raising the possibility that a criminal defendant might not know the tool had factored into a case — and therefore wouldn't be able to challenge its legality.

"These secrecy provisions prevent the courts from providing oversight," Wessler said. "That is really corrosive to our system of checks and balances."

In the past, Wessler noted, courts have been critical of nondisclosure agreements with law enforcement that are designed to protect sensitive surveillance technologies, notably in cases involving devices that mimic cell towers in order to capture phone information, often referred to by the brand name StingRays.

Scores of U.S. law enforcement agencies deployed the devices for years in secret without judicial scrutiny or public transparency. When use of the technology began to be exposed in criminal trials, the courts did not take a favorable view of the secrecy agreements. One of the more

pointed opinions came in a 2016 ruling by a Maryland state appeals court judge, involving Baltimore police and an attempted murder suspect.

The use of a nondisclosure agreement to protect the technology is "inimical to the constitutional principles we revere," [Judge Andrea M. Leahy wrote](#) for the three-member court panel.

In 2015, both the [Department of Justice](#) and [Homeland Security](#) updated their policies to require law enforcement to disclose the use of cell site simulator technologies to the courts when used as part of an investigation. "In all circumstances, candor to the court is of paramount importance," the Homeland Security policy reads. "Applications for the use of a cell site simulator must include sufficient information to ensure that the courts are aware that the technology may be used."

The limits of anonymity

One of the former Babel Street employees who spoke to Protocol cited another example of how Locate X could be used to protect U.S. national security. Investigators, this person said, could identify mobile devices carried near popular border crossing points into the U.S. and pull up the historical location data for those devices, viewing where they've been in the preceding months.

"If you are thinking about attack planning, and you know these devices were just at a Hezbollah or ISIS training camp, and now they're sitting in Juarez, maybe that matters," the former employee said.

Still, privacy experts told of Protocol's reporting on Locate X asserted that law enforcement officials' practice of buying data they would otherwise need a warrant to access amounts to a form of data laundering.

"That consumers can have data being collected that tracks their location, and the government, instead of getting a warrant, which they would normally need to do, can just go to a private company and buy it directly, that's hugely concerning," said Serge Egelman, a computer science professor at UC Berkeley who works on privacy issues.

In the Supreme Court's *Carpenter v. United States* case, [the court held](#) that investigators violated the Fourth Amendment by obtaining cell tower records without a warrant that placed a robbery suspect near the crimes. Chief Justice John Roberts wrote, in the majority opinion, that authorities in that case had failed "to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years."

But whether courts would hold anonymous location data culled from mobile apps to the same standard is an open question.

A spokesperson for Wyden said the senator's aides had a phone call with [Venntel](#) attorneys on Feb. 20, in response to The Wall Street Journal article, to discuss the company's sale of location data to the government. A Wyden aide said [Venntel's](#) counsel declined to answer most questions,

would not identify the company's government clients, and would not reveal the source of the data.

Babel Street's sale of location data to the government could also raise potential liability issues for app developers under the Stored Communications Act, said Wessler, the ACLU lawyer. The 1986 law prohibits providers of computing services or electronic communication to the public from knowingly divulging customer information to any government entity.

"The question for the app companies themselves is whether, now that they know that Babel Street is taking their customers' location data and providing it to law enforcement, are those companies themselves now liable under the Stored Communications Act," Wessler said.

Location data culled from mobile apps is said to be anonymized, with each device masked behind a nameless ID number. But experts say data can be traced back to individual users, based on their particular movements.

The New York Times reviewed a database of location data and [reported](#) in December 2018 that it was able to identify a woman as she traveled to her dermatologist's office, hiked with her dog and stayed over at her ex-boyfriend's home. Babel Street did not respond to an emailed question about whether Locate X data can be de-anonymized.

Big sales, big hires

Babel Street was founded in 2009 as Agincourt Solutions by former U.S. Navy Officer Jeff Chapman, and became Babel Street in 2014. On its website and in marketing materials, it describes itself as "the world's data-to-knowledge company," focusing on a service that analyzes streams of social media activity in multiple languages, often for brand management and sometimes linked to locations such as sports arenas.

Early on, the promise of gleaning meaningful intelligence from Twitter feeds and other social media applications drew clients to Babel Street, according to government records, published reports and the former employees. The [NFL has used](#) Babel Street's analytics software. So, too, have at least 10 local law enforcement agencies around the country, according to the [Brennan Center for Justice](#) at New York University Law School.

[Motherboard](#) and [The Washington Post](#) wrote about the company's social media analytics software in 2017, noting heavy interest from police agencies overseeing major events like Super Bowls. On the government side, the [FBI](#) and the [Army](#) were among Babel Street's early customers. Michael Flynn, who served briefly as President Trump's national security adviser and later pleaded guilty to lying to the FBI, was once an adviser to the firm, according to [Flynn's financial disclosure forms](#).

Just before the rollout of Locate X, the company hired a veteran Department of Justice privacy lawyer, Jill Maze, to be the company's chief privacy officer, according to former employees and Maze's LinkedIn account.

Subsequent hires suggest the company viewed location data as a growth area. In February 2019, Babel Street [hired retired Maj. Gen. Mark Quantock](#), a former director of intelligence for U.S. Central Command, which includes the Middle East and Central Asia, and the former director of operations for the National Geospatial Intelligence Agency, essentially the government's headquarters for location data intelligence.

Three months later, the company hired a 20-year Pentagon veteran, [Dave Dillow](#), who since 2003 has worked with special operations forces focused on integrating "publicly available information," or PAI, into the intelligence pipeline for those forces. Commercial location data is one type of PAI.

Get in touch with us: Share information securely with Protocol via encrypted Signal or WhatsApp message, at 415-214-4715 or [through our anonymous SecureDrop](#).

The data used by Babel Street, said the former employees of Babel Street and Gravy Analytics, comes largely from third-party data aggregators who broker deals with mobile app developers, offering revenue in return and sometimes detailed analysis about how users are engaging with the app. Data aggregators who spoke to Protocol said they enable services like mapping and marketing, and comply with privacy regulations, which include requiring all app users to give their consent to sharing their data.

Privacy advocates say such consumer opt-ins are often buried in small print or otherwise clouded in vague or bureaucratic language, and that users have little visibility into how their data is used.

"That's the fundamental problem," said Egelman, the UC Berkeley professor. "The trafficking in this data is totally opaque to everyone who isn't a party to these transactions."

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: EDNA RUCKER (LIA) (b)(6); (b)(7)(C)
Sent: Tuesday, March 10, 2020 9:25 AM
To: (b)(6); (b)(7)(C) @hq.dhs.gov>
Cc: (b)(6); (b)(7)(C) @hq.dhs.gov>; (b)(6); (b)(7)(C) @hq.dhs.gov>
Subject: RE: Protocol Article

(b)(6);

So far I found out that TAKS does not use Locate X but I think we may use it internally on or USSS phones.

Stay tuned,

Gayle Rucker

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) @hq.dhs.gov>
Sent: Monday, March 9, 2020 2:44 PM
To: EDNA RUCKER (LIA) (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C) @hq.dhs.gov>; (b)(6); (b)(7)(C) @hq.dhs.gov>
Subject: Protocol Article

Hi Gayle,

Did you see the article below? It specifically calls out USSS as a user of Locate X. Is USSS using this service? As you may already know, OGC is currently working on an opinion regarding the use of AdID location tracking (from when it started coming out that the Department was working with Venntel).

(b)(6);
(b)(7)(C)

<https://www.protocol.com/government-buying-location-data>

Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones

Cc: KEVIN TYRRELL (IGL) (b)(6); (b)(7)(C)

Subject: Good Afternoon FYI

Good Afternoon Tom,

We received the attached FOIA request recently asking for records concerning the Chief Counsel Office, so I just wanted to bring it to your attention. We will proceed as normal, just an FYI. Please let me know if you have any questions or concerns.

Requester: Washington Post (20200711)

Date: 5/27/2020

Requested: -All legal memos or training materials in the possession of the U.S. Secret Service Office of the Chief Counsel concerning the use of commercially-available data or metadata products, services or databases, including but not limited to: anonymized mobile phone geolocation/GPS data, social media monitoring, data related to transaction or financial records or any other commercially-available data source or product.

- Any privacy impact assessment or other memorandum or document concerning privacy produced by the USSS Office of the Chief Counsel concerning the use of commercially-available data or metadata products, services or databases, including but not limited to: anonymized mobile phone geolocation/GPS data, social media feeds, transaction or financial records or any other commercially-available data source or product.

- Any records mentioning or pertaining to commercial software products sold by the private entities Babel Street, Venntel, Gravy Analytics, Geofeedia or Planet Risk in the possession of the U.S. Secret Service Office of the Chief Counsel.

Kevin L. Tyrrell

Chief Disclosure Officer

OFFICE OF INTERGOVERNMENTAL AND LEGISLATIVE AFFAIRS

United States Secret Service

Office (b)(6); (b)(7)(C)

(b)(6)

Reporter, Wall Street Journal
1025 Connecticut Ave NW, Suite 800
Washington, D.C. 20036

May 27, 2020

Subject: New Freedom of Information Act Request

United States Secret Service
Communications Center (FOIA/PA)
245 Murray Lane
Building T-5
Washington, D.C. 20223

VIA EMAIL

To whom it may concern,

My name is (b)(6); in a reporter that covers the Department of Justice, federal law enforcement, legal issues, and other matters for the *Wall Street Journal*.

This is a request under the Freedom of Information Act ("FOIA"). I request the department provide the following records within 20 business days:

- All legal memos or training materials in the possession of the U.S. Secret Service Office of the Chief Counsel concerning the use of commercially-available data or metadata products, services or databases, including but not limited to: anonymized mobile phone geolocation/GPS data, social media monitoring, data related to transaction or financial records or any other commercially-available data source or product.
- Any privacy impact assessment or other memorandum or document concerning privacy produced by the USSS Office of the Chief Counsel concerning the use of commercially-available data or metadata products, services or databases, including but not limited to: anonymized mobile phone geolocation/GPS data, social media feeds, transaction or financial records or any other commercially-available data source or product.
- Any records mentioning or pertaining to commercial software products sold by the private entities Babel Street, Venntel, Gravy Analytics, Geofeedia or Planet Risk in the possession of the U.S. Secret Service Office of the Chief Counsel.
- Failure to respond to this Request within the time period required by FOIA could serve as a constructive denial of the Request, and the Wall Street Journal may be deemed to have exhausted its administrative remedies. See 5 U.S.C. § 552(a)(6)(C)[i].

I request a search of records regardless of format or medium to include but not limited to: paper records, electronic records, audiotapes, videotapes, photographs, data, and graphical material. The request should be understood to include but not be limited: correspondence, letters, emails, text messages, facsimiles, telephone messages, voice mail messages, transcripts, notes, and minutes. The request should also be understood to include attachments and supporting documents.

Exclusion of media clippings or agency press releases

The agency may exclude any record that appears to consist solely of media clips or clippings from an internal or external media monitoring service in order to speed up processing time of this request. Records that consist of government officials commenting on or about news media clippings should not be excluded, nor should records that consist of interactions between government officials and members of the news media.

Vaughn index requested

If the agency's position is that records are exempt from disclosure, please provide an index as required under Vaughn v. Rosen 484 F.2d 820 (D.C. Cir. 1973.)

Search of personal devices and accounts requested

If any government employee used a personal account, device or other communications method or medium for any government activity, I request a search of those devices and accounts to see if they contain federal records.

Preservation hold requested

Please institute a preservation hold on any records responsive to this request. Acting either institutionally through the Wall Street Journal in consultation with legal counsel or as an individual in my personal capacity, I intend to pursue all legal avenues for my right of access to public records. The agency should be on notice that litigation is reasonably foreseeable.

Fee waiver requested

I am employed as a full-time reporter with The Wall Street Journal and therefore a member of the news media engaged primarily in the dissemination of information that is in the public's interest and hereby request a fee waiver. I certify that my statements concerning a fee waiver are true and correct to the best of my knowledge and belief.

If my fee waiver is denied, I am willing to pay up to **\$500** for favorable disposition of my request.

Expedited processing requested

I am employed as a full-time reporter with The Wall Street Journal. As a member of the news media engaged primarily in the dissemination of information that is in the public's interest, I hereby request expedited processing on the grounds that I am seeking information that is urgently needed to inform the public about the use of commercial data products by the U.S. government and their privacy impacts on Americans.

On Feb. 7, 2020, the Wall Street Journal reported on the U.S. federal government's purchase of commercially-available GPS location data of millions of U.S. cell phones through a company called Venntel, Inc.¹ On March 5, 2020, the publication Protocol reported that the US USSS has purchased access to such tools through a company called Babel Street — raising questions about the privacy impact on Americans and what kind of legal controls were being put on this kind of government surveillance program.² The records I seek go to the heart of the question about the government's legal authorization and privacy controls on such sensitive data.

I certify that my statements concerning the need for expedited processing are true and correct to the best of my knowledge and belief

Sincerely,

(b)(6); (b)(7)(C)

¹ Byron Tau and Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*. WALL ST. J. (Feb. 7, 2020), <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>

² Charles Levinson, *Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones*. PROTOCOL (March 5, 2020), <https://www.protocol.com/government-buying-location-data>

From: (b)(6); (b)(7)(C) (LEG)
Sent: Fri, 29 May 2020 15:17:45 -0400
To: (b)(6); (b)(7)(C)
Subject: FW: Good Afternoon FYI
Attachments: USSS-GC-FOIA (b)(6) 0527.pdf

(b)(6); (b)(7)(C) – For tracking, when this search request officially comes in from FOIA, it will be assigned to (b)(6); (b)(7)(C). Let me know if you have any questions.

Thanks

(b)(6); (b)(7)(C)

From: THOMAS HUSE (LEG)
Sent: Thursday, May 28, 2020 5:40 PM
To: (b)(6); (b)(7)(C)
Subject: FW: Good Afternoon FYI

All:

Please see the attached FOIA request. Maybe we can discuss it tomorrow? Are you all free around 1 p.m.?

Thanks,
Tom

From: KEVIN TYRRELL (IGL) (b)(6); (b)(7)(C)
Sent: Thursday, May 28, 2020 12:21 PM
To: THOMAS HUSE (LEG) (b)(6); (b)(7)(C)
Cc: KEVIN TYRRELL (IGL)
Subject: Good Afternoon FYI

Good Afternoon Tom,

We received the attached FOIA request recently asking for records concerning the Chief Counsel Office, so I just wanted to bring it to your attention. We will proceed as normal, just an FYI. Please let me know if you have any questions or concerns.

Requester: Washington Post (20200711)

Date: 5/27/2020

Requested: -All legal memos or training materials in the possession of the U.S. Secret Service Office of the Chief Counsel concerning the use of commercially-available data or metadata products, services or databases, including but not limited to: anonymized mobile phone geolocation/GPS data, social media monitoring, data related to transaction or financial records or any other commercially-available data source or product.

- Any privacy impact assessment or other memorandum or document concerning privacy produced by the USSS Office of the Chief Counsel concerning the use of commercially-available data or metadata products, services or databases, including but not limited to: anonymized mobile phone geolocation/GPS data, social media feeds, transaction or financial records or any other commercially-available data source or product.

- Any records mentioning or pertaining to commercial software products sold by the private entities Babel Street, Venntel, Gravy Analytics, Geofeedia or Planet Risk in the possession of the U.S. Secret Service Office of the Chief Counsel.

Kevin L. Tyrrell

Chief Disclosure Officer

OFFICE OF INTERGOVERNMENTAL AND LEGISLATIVE AFFAIRS

United States Secret Service

Office: (b)(6); (b)(7)(C)

(b)(6)

Reporter, Wall Street Journal
1025 Connecticut Ave NW, Suite 800
Washington, D.C. 20036

May 27, 2020

Subject: New Freedom of Information Act Request

United States Secret Service
Communications Center (FOIA/PA)
245 Murray Lane
Building T-5
Washington, D.C. 20223

VIA EMAIL

To whom it may concern,

My name is (b)(6); I'm a reporter that covers the Department of Justice, federal law enforcement, legal issues, and other matters for the *Wall Street Journal*.

This is a request under the Freedom of Information Act ("FOIA"). I request the department provide the following records within 20 business days:

- All legal memos or training materials in the possession of the U.S. Secret Service Office of the Chief Counsel concerning the use of commercially-available data or metadata products, services or databases, including but not limited to: anonymized mobile phone geolocation/GPS data, social media monitoring, data related to transaction or financial records or any other commercially-available data source or product.
- Any privacy impact assessment or other memorandum or document concerning privacy produced by the USSS Office of the Chief Counsel concerning the use of commercially-available data or metadata products, services or databases, including but not limited to: anonymized mobile phone geolocation/GPS data, social media feeds, transaction or financial records or any other commercially-available data source or product.
- Any records mentioning or pertaining to commercial software products sold by the private entities Babel Street, Venntel, Gravy Analytics, Geofeedia or Planet Risk in the possession of the U.S. Secret Service Office of the Chief Counsel.
- Failure to respond to this Request within the time period required by FOIA could serve as a constructive denial of the Request, and the Wall Street Journal may be deemed to have exhausted its administrative remedies. See 5 U.S.C. § 552(a)(6)(C)[i].

I request a search of records regardless of format or medium to include but not limited to: paper records, electronic records, audiotapes, videotapes, photographs, data, and graphical material. The request should be understood to include but not be limited: correspondence, letters, emails, text messages, facsimiles, telephone messages, voice mail messages, transcripts, notes, and minutes. The request should also be understood to include attachments and supporting documents.

Exclusion of media clippings or agency press releases

The agency may exclude any record that appears to consist solely of media clips or clippings from an internal or external media monitoring service in order to speed up processing time of this request. Records that consist of government officials commenting on or about news media clippings should not be excluded, nor should records that consist of interactions between government officials and members of the news media.

Vaughn index requested

If the agency's position is that records are exempt from disclosure, please provide an index as required under Vaughn v. Rosen 484 F.2d 820 (D.C. Cir. 1973.)

Search of personal devices and accounts requested

If any government employee used a personal account, device or other communications method or medium for any government activity, I request a search of those devices and accounts to see if they contain federal records.

Preservation hold requested

Please institute a preservation hold on any records responsive to this request. Acting either institutionally through the Wall Street Journal in consultation with legal counsel or as an individual in my personal capacity, I intend to pursue all legal avenues for my right of access to public records. The agency should be on notice that litigation is reasonably foreseeable.

Fee waiver requested

I am employed as a full-time reporter with The Wall Street Journal and therefore a member of the news media engaged primarily in the dissemination of information that is in the public's interest and hereby request a fee waiver. I certify that my statements concerning a fee waiver are true and correct to the best of my knowledge and belief.

If my fee waiver is denied, I am willing to pay up to **\$500** for favorable disposition of my request.

Expedited processing requested

I am employed as a full-time reporter with The Wall Street Journal. As a member of the news media engaged primarily in the dissemination of information that is in the public's interest, I hereby request expedited processing on the grounds that I am seeking information that is urgently needed to inform the public about the use of commercial data products by the U.S. government and their privacy impacts on Americans.

On Feb. 7, 2020, the Wall Street Journal reported on the U.S. federal government's purchase of commercially-available GPS location data of millions of U.S. cell phones through a company called Venntel, Inc.¹ On March 5, 2020, the publication Protocol reported that the US USSS has purchased access to such tools through a company called Babel Street — raising questions about the privacy impact on Americans and what kind of legal controls were being put on this kind of government surveillance program.² The records I seek go to the heart of the question about the government's legal authorization and privacy controls on such sensitive data.

I certify that my statements concerning the need for expedited processing are true and correct to the best of my knowledge and belief

Sincerely,

(b)(6); (b)(7)(C)

¹ Byron Tau and Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*. WALL ST. J. (Feb. 7, 2020), <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>

² Charles Levinson, *Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones*. PROTOCOL (March 5, 2020), <https://www.protocol.com/government-buying-location-data>

Sent from my iPhone

Begin forwarded message:

From: (b)(6); (b)(7)(C) @hq.dhs.gov>
Date: March 23, 2020 at 12:41:46 PM EDT
To: "EDNA RUCKER (LIA)" <(b)(6); (b)(7)(C)>
Cc: (b)(6); (b)(7)(C) @usss.dhs.gov>
Subject: RE: Protocol Article

Hi Gayle,

I am not aware of anything being issued from the Law Enforcement Group at DHS Policy. As far as an OGC contact, I would start with (b)(6); believe (b)(6); is leading a working group.

(b)(6);

From: EDNA RUCKER (LIA) (b)(6); (b)(7)(C)
Sent: Monday, March 23, 2020 12:10 PM
To: (b)(6); (b)(7)(C) @hq.dhs.gov>
Cc: (b)(6); (b)(7)(C) @usss.dhs.gov>
Subject: RE: Protocol Article

H (b)(6);

A couple of follow-up questions... Has the Law Enforcement group within DHS Policy issued anything regarding the use of AdID or Locate X?

Further, Is there a contact in OGC with whom our Counsel can talk about the forthcoming OGC ruling/decision?

Thanks,

Gayle Rucker

(b)(6); (b)(7)(C)

If USSS is using Locate X, that is more concerning to us. Locate X uses AdID from cell phones for location tracking. My understanding is that Locate X buys data from Venntel and packages it with a nice interface. It is not clear to me whether there is any social media integration in the Babel Locate X tool. We previously raised concerns to OGC regarding the Department's use of AdID tracking as it relates to the Supreme Court case Carpenter v. U.S., which held that the collection of cell-site location information constituted a search under the Fourth Amendment. OGC is currently working on providing a legal opinion on the use of Venntel and AdID. If USSS is using Locate X, we also need a PTA, but I will let you know that we are not adjudicating AdID PTAs until we hear from OGC regarding the legal boundaries for the technology's use.

(b)(6);
(b)(7)(C)

From: EDNA RUCKER (LIA) (b)(6); (b)(7)(C)
Sent: Tuesday, March 17, 2020 3:30 PM
To: (b)(6); (b)(7)(C) @hq.dhs.gov>
Cc: (b)(6); (b)(7)(C) @hq.dhs.gov>; (b)(6); (b)(7)(C) @hq.dhs.gov>
Subject: RE: Protocol Article

(b)(6):

I didn't ask that question but I will try to find out. What are you looking to know about it? What's the concern?

E. Gayle Rucker

USSS Privacy Officer

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) @hq.dhs.gov
Sent: Tuesday, March 17, 2020 3:23 PM
To: EDNA RUCKER (LIA) (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C) @hq.dhs.gov; (b)(6); (b)(7)(C) @hq.dhs.gov
Subject: RE: Protocol Article

Hi Gayle,

Thanks. Are they using Locate X or the Babel social media product, or both?

(b)(6);

From: EDNA RUCKER (LIA) (b)(6); (b)(7)(C)
Sent: Tuesday, March 17, 2020 3:22 PM
To: (b)(6); (b)(7)(C) @hq.dhs.gov
Cc: (b)(6); (b)(7)(C) @hq.dhs.gov; (b)(6); (b)(7)(C) @hq.dhs.gov
Subject: RE: Protocol Article

(b)(6);

It has been confirmed that our Protective Intelligence Division uses this product in its criminal investigations. The collection and use will be a part of the update to DHS/USSS SORN.001.

E. Gayle Rucker

USSS Privacy Officer

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) @hq.dhs.gov>
Sent: Monday, March 9, 2020 2:44 PM
To: EDNA RUCKER (LIA) <(b)(6); (b)(7)(C)>
Cc: (b)(6); (b)(7)(C) @hq.dhs.gov>; (b)(6); (b)(7)(C) @hq.dhs.gov>
Subject: Protocol Article

Hi Gayle,

Did you see the article below? It specifically calls out USSS as a user of Locate X. Is USSS using this service? As you may already know, OGC is currently working on an opinion regarding the use of AdID location tracking (from when it started coming out that the Department was working with Venntel).

(b)(6);
(b)(7)(C)

<https://www.protocol.com/government-buying-location-data>

Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones

From: (b)(6); (b)(7)(C)
Sent: Tue, 8 Oct 2019 12:02:07 -0400
To: J (b)(6); (b)(7)(C) (FSD)
Subject: Reaching back out

(b)(6);

I hope this email finds you well and family issues resolved. As requested, I am reaching back out to see if it makes sense to get together. I still have the requested data available and want to see how to proceed.

Let me know.

Best,

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); @venntel.com

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Fri, 20 Sep 2019 17:02:32 +0000
To: (b)(6); (PRO)
Cc: (b)(6); (b)(7)(C) PID
Subject: Order (b)(6); (b)(7)(C) - OpeniO Disclosure - Clarification
Attachments: OpeniO Disclosure-Govt - Rev1.pdf

(b)(6); (b)(7)(C)

We received a question from a Customer with regards to our previously provided OpeniO disclosure that we wanted to clarify:

In an attempt to state that some of the commercial-proprietary data sets, including Advertising Technology (Ad-Tech) data, which is also known within the United States Government as Commercial Telemetry Data (CTD), is not available through subscription to the general public, it was incorrectly stated that "Some of the commercial-proprietary data sets, including Ad-Tech/CTD are not publicly available for free or through subscription." These commercial-proprietary data sets, including Ad-Tech/CTD, are made available through subscription to select commercial clients including the United States Government and Contractors working in support of the United States Government.

Creative Radicals includes a number of commercial-proprietary data sets within OpeniO and also offers advanced commercial-proprietary data sets for integration into OpeniO. These data sets provide a wide range of data to the End User and each Customer is encouraged to work with Creative Radicals to ensure their OpeniO configuration meets the Customer's full needs.

An updated disclosure statement is attached to this email.

Thanks,

(b)(6);

Creative Radicals

Director of Contracts

P:

C: (b)(6); (b)(7)(C)

1765 Greensboro Station Place, Ste 475, McLean VA 22102

www.creativeradicals.com

CREATIVE  **RADICALS**

This message may contain confidential, proprietary, and/or privileged information. If you are not the intended recipient, any review, disclosure, copying, distribution or use of the contents of this message is strictly prohibited. If you have received this message in error, please notify the sender immediately and delete or destroy any copy of this message.

From: (b)(6); (b)(7)(C)
Sent: Wednesday, September 11, 2019 12:14 PM

To: (b)(6); (b)(7)(C) (PRO)
Cc: (b)(6); (b)(7)(C) (PID)
Subject: Order (b)(6); (b)(7)(C) OpeniO Disclosure
Importance: High

(b)(6); (b)(7)(C)

With regards to our existing order (b)(6); (b)(7)(C) for OpeniO licenses we are providing the attached OpeniO Disclosure. This disclosure is to provide some clarity/definition into what OpeniO does and does not do and how Advertising Technology (Ad-Tech) data, which is also known within the United States Government as Commercial Telemetry Data (CTD), is integrated and operates within OpeniO.

Please let me know if you have any questions or concerns with regards to the attached.

Thanks,

(b)(6);

Creative Radicals

Director of Contracts

P:

C: (b)(6); (b)(7)(C)

1765 Greensboro Station Place, Ste 475, McLean VA 22102

www.creativeradicals.com



This message may contain confidential, proprietary, and/or privileged information. If you are not the intended recipient, any review, disclosure, copying, distribution or use of the contents of this message is strictly prohibited. If you have received this message in error, please notify the sender immediately and delete or destroy any copy of this message.

Page 3281 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

From: (b)(6); (b)(7)(C)
Sent: Wed, 28 Aug 2019 11:43:18 -0400
To: (b)(6); (b)(7)(C); (FSD)
Subject: Re: Data

My apologies (b)(6) I'll put a note on my calendar to reach out in Oct. I hope everything works out.

Best,

(b)(6);
(b)(7)(C)

On Wed, Aug 28, 2019 at 11:41 AM (b)(6); (b)(7)(C) (FSD)
(b)(6); (b)(7)(C) <[@usss.dhs.gov](mailto:(b)(6); (b)(7)(C)@usss.dhs.gov)> wrote:

(b)(6)

I appreciate your patience with me on getting the data, I am dealing with family emergency I will need to postpone the data acquisition for a few months.

I will reach out to you in October.

(b)(6); (b)(7)(C)

Lead Geospatial Specialist

Department of Homeland Security

United States Secret Service



Office

(b)(6); (b)(7)(C)

Cell: 2

Email: (b)(6); <[@usss.dhs.gov](mailto:(b)(6);@usss.dhs.gov)>

From: (b)(6); (b)(7)(C) <[@usss.dhs.gov](mailto:(b)(6); (b)(7)(C)@usss.dhs.gov)>

Sent: Wednesday, August 28, 2019 10:35 AM

To: (b)(6); (b)(7)(C) (FSD) (b)(6); (b)(7)(C) <[@usss.dhs.gov](mailto:(b)(6); (b)(7)(C)@usss.dhs.gov)>

Subject: Data

Hey (b)(6);

Sorry to pester you on this but I have my data team asking about what to do with the data that we pulled for your evaluation. If we need to postpone getting you the data for a month or two, I can have them take it offline and we can connect at a later date.

Let me know what you'd like to do.

Best regards,

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); venntel.com

(b)(6); (b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

--

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); venntel.com

(b)(6); (b)(7)(C)

From: (b)(6);
Sent: Tue, 20 Aug 2019 11:37:24 -0400
To: (b)(6); (b)(7)(C) (FSD)
Subject: Data

Hey (b)(6);

Trying to see when would be a good time to connect so that we can get you the raw data and also get you trained on our portal.

Let me know.

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); @venntel.com

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Fri, 16 Aug 2019 11:40:22 -0400
To: (b)(6); (b)(7)(C) (FSD)
Subject: Checking In

Hey (b)(6);

I hope everything worked out. Just circling back to see when might be a good time to get together for a brief and to work on getting you data.

Let me know.

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); venntel.com

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Thu, 8 Aug 2019 08:15:05 -0400
To: (b)(6); (b)(7)(C) (FSD)
Subject: Re: Information for Friday

Of course. Hope everything is ok.

(b)(6);

Sent from my iPhone

On Aug 8, 2019, at 7:46 AM, (b)(6); (b)(7)(C) (FSD)
(b)(6); (b)(7)(C) @usss.dhs.gov wrote:

(b)(6);

I am going to have to reschedule our meeting. I had a family emergency and am out of the office this week. Can get back with you Monday or Tuesday next week to reschedule?

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) @venntel.com>
Sent: Wednesday, August 7, 2019 10:27 AM
To: (b)(6); (b)(7)(C) (FSD) (b)(6); (b)(7)(C) @usss.dhs.gov>
Subject: Information for Friday

Hey (b)(6);
(b)(7)(C)

Here is my information,

(b)(6); (b)(7)(C)

Let me know if you need SSN.

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); venntel.com

(b)(6); (b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.



Office:

(b)(6); (b)(7)(C)

Cell:

Email:

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) @venntel.com>

Sent: Monday, July 29, 2019 2:44 PM

To: (b)(6); (b)(7)(C) (FSD) (b)(6); (b)(7)(C) @usss.dhs.gov>

Cc: (b)(6); (b)(7)(C) venntel.com>

Subject: Re: Portal / Data Status Update

Good Afternoon (b)(6); (b)(7)(C)

I am contacting you regarding scheduling training for an evaluation of the **Venntel** portal. This is a separate platform from the data sample that you will be receiving later this week.

The training takes about an hour and can be administered via the web or in-person depending upon your location and preference.

Currently, I have availability on the following days and times:

Wednesday, July 31, 2019, from 2 - 4 PM EST

Thursday, August 1, 2019, from 10 - 4 PM EST

Friday, August 2, 2019, from 10 - 3 PM EST

If there is not an hour in there dates/times above that works for your schedule please let me know and I will see what I can do.

Thank you, I look forward to hearing from you.

Best,

Bridget

On Tue, Jul 23, 2019 at 11:17 AM (b)(6); (b)(7)(C) <[REDACTED]@venntel.com> wrote:

(b)(6);
(b)(7)(C)

I've made the request to our data team and we expect to have 2 weeks of US data for you by mid-next week. I am also copying in (b)(6); (b)(7)(C) Director of Customer Success who will be providing you with trial access to the Venntel Portal and work to schedule training for you or whomever you designate as the user if it is not you - (she will need the name and contact information for the user - our portal is a named-user environment).

I'd also like to schedule time to better understand the use-case(s) to ensure that we meet the expectations of you and your team. At that time, I can also provide a briefing for any other possible users of the data/system. Please let me know if when might be a good time to connect (I am local to the DC area).

Again, please feel free to reach out to me if you have any questions.

v/r

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); <[REDACTED]@venntel.com>

(b)(6); (b)(7)(C)

--

(b)(6); (b)(7)(C)

Vice President - Customer Experience

(b)(6); (b)(7)(C)

(b)(6); venntel.com

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

--

(b)(6); (b)(7)(C)

From: (b)(6);
Sent: Wed, 31 Jul 2019 10:46:00 -0400
To: (b)(6); (b)(7)(C) (FSD)
Cc: (b)(6); (b)(7)(C)
Subject: Dataset

Hey (b)(6);
(b)(7)(C)

So here are the statistics for the 2 weeks worth of data in the US.

Sample Date: 6/30/19 - 7/13/19
Total Signals : 60,901,446,392
Distinct Devices : 203,594,217
Total File Size : 606.2GB

I am also introducing (b)(6); (b)(7)(C) who can help with the delivery of the data, provide the schema and answer any questions you might have. As always, feel free to call me or (b)(6); (b)(7)(C) or include us in any communication and/or need assistance.

Please let me know a good date/time to come brief you and your team on the capabilities of our data.

v/r

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); [venntel.com](mailto:(b)(6);@venntel.com)

(b)(6); (b)(7)(C)

From: (b)(6);
Sent: Mon, 22 Jul 2019 11:41:48 -0400
To: (b)(6); (b)(7)(C) (FSD)
Cc:
Subject: Re: Data Test.

Awesome. Will be in touch shortly.

(b)(6);
(b)(7)(C)

On Mon, Jul 22, 2019 at 11:36 AM, (b)(6); (b)(7)(C) (FSD)
(b)(6); (b)(7)(C) @usss.dhs.gov> wrote:

(b)(6);

Thanks for the information. I have both storage and processing power to handle this type of big data.

V/r (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) @venntel.com>
Sent: Monday, July 22, 2019 11:25 AM
To: (b)(6); (b)(7)(C) (FSD) (b)(6); (b)(7)(C) @usss.dhs.gov>
Cc: (b)(6); (b)(7)(C) @venntel.com>
Subject: Re: Data Test.

Hey (b)(6);
(b)(7)(C)

Roger that. Just to give you perspective, and so you can scope it out on your end, two weeks of US data will conservatively be approximately 56B records and most likely be 600GB (compressed) in size.

Best,

(b)(6);

On Mon, Jul 22, 2019 at 11:19 AM, (b)(6); (b)(7)(C) (FSD)
(b)(6); (b)(7)(C) @usss.dhs.gov> wrote:

(b)(6);

I as I mentioned to (b)(6); would like data for all the US for the last 14 day's to run my test on if that is possible.

V/r (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) @venntel.com>
Sent: Monday, July 22, 2019 10:59 AM
To: (b)(6); (b)(7)(C) @venntel.com>

Cc: (b)(6); (b)(7)(C) FSD) (b)(6); (b)(7)(C) @usss.dhs.gov>
Subject: Re: Data Test.

Thanks (b)(6);
(b)(7)(C)

(b)(6); it's a pleasure to meet you virtually. A (b)(6); mentioned, I am responsible for DHS within Venntel. I will work with (b)(6); to get you trial license to our portal and your data request. Is there a particular area of the US that you'd like data for?

Please feel free to reach out to me if you have any questions.

My contact information is below.

v/r

(b)(6);
(b)(7)(C)

On Mon, Jul 22, 2019 at 10:33 AM (b)(6); (b)(7)(C) @venntel.com> wrote:

(b)(6); (b)(7)(C)

Thanks for reaching out. I am CC'ing my counterpart (b)(6); who covers our work at DHS. We will get these requests in and be in contact shortly.

Thanks,

(b)(6); (b)(7)(C)

Venntel | Director of Government Sales



E // (b)(6) @venntel.com

P // (b)(6);
(b)(7)(C)

W // <http://www.venntel.com>

On Jul 22 2019, at 10:28 am, (b)(6); (b)(7)(C) FSD)

(b)(6); (b)(7)(C) @usss.dhs.gov> wrote:

(b)(6);

It was good to speak to you over the phone. Per our conversation let me first say that this email in no way obligates the U.S. Secret Service to the Purchase of any products or data from Venntel nor does it obligate any funds for this trail material.

With that being said, I am interested in trail account of your software and 14 days' worth of data over the US.

(b)(6); (b)(7)(C)

Lead Geospatial Specialist

Department of Homeland Security

United States Secret Service

Office

(b)(6); (b)(7)(C)

Cell:

Email: (b)(6); (b)(7)(C)@uss.s.dhs.gov

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

--

(b)(6); (b)(7)(C)

Vennetel, Inc.

(b)(6); (b)(7)(C)@vennetel.com

(b)(6); (b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

--

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); @venntel.com

(b)(6); (b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

--

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); @venntel.com

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Mon, 29 Jul 2019 14:44:26 -0400
To: (b)(6); (b)(7)(C) (FSD)
Cc: (b)(6);
Subject: Re: Portal / Data Status Update

Good Afternoon (b)(6); (b)(7)(C)

I am contacting you regarding scheduling training for an evaluation of the **Venn**tel portal. This is a separate platform from the data sample that you will be receiving later this week.

The training takes about an hour and can be administered via the web or in-person depending upon your location and preference.

Currently, I have availability on the following days and times:

Wednesday, July 31, 2019, from 2 - 4 PM EST
Thursday, August 1, 2019, from 10 - 4 PM EST
Friday, August 2, 2019, from 10 - 3 PM EST

If there is not an hour in there dates/times above that works for your schedule please let me know and I will see what I can do.

Thank you, I look forward to hearing from you.

Best,

(b)(6); (b)(7)(C)

On Tue, Jul 23, 2019 at 11:17 AM (b)(6); (b)(7)(C) <@venntel.com> wrote:

(b)(6);

I've made the request to our data team and we expect to have 2 weeks of US data for you by mid-next week. I am also copying in (b)(6); (b)(7)(C) Director of Customer Success who will be providing you with trial access to the **Venn**tel Portal and work to schedule training for you or whomever you designate as the user if it is not you - (she will need the name and contact information for the user - our portal is a named-user environment).

I'd also like to schedule time to better understand the use-case(s) to ensure that we meet the expectations of you and your team. At that time, I can also provide a briefing for any other possible users of the data/system. Please let me know if when might be a good time to connect (I am local to the DC area).

Again, please feel free to reach out to me if you have any questions.

v/r

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6)@venntel.com

(b)(6); (b)(7)(C)

--

(b)(6); (b)(7)(C)

Vice President - Customer Experience

(b)(6); (b)(7)(C)

(b)(6);
(b)(7)(C)@venntel.com

From: (b)(6); (b)(7)(C) (FSD)
Sent: Mon, 22 Jul 2019 15:33:29 +0000
To:
Cc: (b)(6); (b)(7)(C)
Subject: RE: Data Test.

(b)(6);

Thanks for the information. I have both storage and processing power to handle this type of big data.

(b)(6); (b)(7)(C)

From: (b)(6);
Sent: Monday, July 22, 2019 11:25 AM
To: (b)(6); (b)(7)(C) (FSD)
Cc:
Subject: Re: Data Test.

Hey (b)(6); (b)(7)(C)

Roger that. Just to give you perspective, and so you can scope it out on your end, two weeks of US data will conservatively be approximately 56B records and most likely be 600GB (compressed) in size.

Best,

(b)(6);

On Mon, Jul 22, 2019 at 11:19 AM (b)(6); (b)(7)(C) (FSD)
(b)(6); (b)(7)(C) @usss.dhs.gov wrote:
Mike,

I as I mentioned to (b)(6); (b)(7)(C) would like data for all the US for the last 14 day's to run my test on if that is possible.

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) @venntel.com>
Sent: Monday, July 22, 2019 10:59 AM
To: (b)(6); (b)(7)(C) @venntel.com>
Cc: (b)(6); (b)(7)(C) (FSD) (b)(6); (b)(7)(C) @usss.dhs.gov>
Subject: Re: Data Test.

Thanks (b)(6); (b)(7)(C)

(b)(6); it's a pleasure to meet you virtually. A (b)(6); mentioned, I am responsible for DHS within Vennitel. I will work with (b)(6); to get you trial license to our portal and your data request. Is there a particular area of the US that you'd like data for?

Please feel free to reach out to me if you have any questions.

My contact information is below.

v/r

(b)(6);

On Mon, Jul 22, 2019 at 10:33 AM (b)(6); (b)(7)(C) <(b)(6);@venntel.com> wrote:

(b)(6);

Thanks for reaching out. I am CC'ing my counterpart (b)(6); who covers our work at DHS. We will get these requests in and be in contact shortly.

Thanks,

(b)(6); (b)(7)(C)

Vennitel | Director of Government Sales



(b)(6); <(b)(6);@venntel.com>

P // (b)(6);

W // <http://www.venntel.com>

On Jul 22 2019, at 10:28 am, (b)(6); (b)(7)(C) (FSD)

(b)(6); (b)(7)(C) <(b)(6);@uss.dhs.gov> wrote:

(b)(6);

It was good to speak to you over the phone. Per our conversation let me first say that this email in no way obligates the U.S. Secret Service to the Purchase of any products or data from Vennitel nor does it obligate any funds for this trail material.

With that being said. I am interested in trail account of your software and 14 days' worth of data over the US.

(b)(6); (b)(7)(C)

Lead Geospatial Specialist

Department of Homeland Security

United States Secret Service

Office:

(b)(6); (b)(7)(C)

Cell:

Email: (b)(6); @usss.dhs.gov

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); @venntel.com

(b)(6); (b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); venntel.com

(b)(6); (b)(7)(C)

P // (b)(6);
W // <http://www.venntel.com>
On Jul 22 2019, at 10:28 am, (b)(6); (b)(7)(C) (FSD)
(b)(6); (b)(7)(C) [@usss.dhs.gov](mailto:usss.dhs.gov) wrote:

(b)(6);
(b)(7)(C)

It was good to speak to you over the phone. Per our conversation let me first say that this email in no way obligates the U.S. Secret Service to the Purchase of any products or data from **Venntel** nor does it obligate any funds for this trail material.

With that being said. I am interested in trail account of your software and 14 days' worth of data over the US.

(b)(6); (b)(7)(C)

Lead Geospatial Specialist

Department of Homeland Security

United States Secret Service

Office: (b)(6);
Cell: (b)(7)(C)

Email: (b)(6); [@usss.dhs.gov](mailto:usss.dhs.gov)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other

disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

(b)(6); (b)(7)(C)

Venntel, Inc.

(b)(6); @venntel.com

(b)(6); (b)(7)(C)

Page 3345 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3346 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3347 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3348 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3349 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3350 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3351 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3352 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3353 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3354 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3355 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3356 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3357 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3358 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3359 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3360 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3361 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3362 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3363 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3364 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3365 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3385 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3386 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3387 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3388 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3389 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3390 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3391 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3392 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3393 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3394 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3395 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3396 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

From: (b)(6); (b)(7)(C)
Sent: Tue, 9 Oct 2018 15:37:44 +0000
To: (b)(6); (b)(7)(C) (CTR); (b)(6); (b)(7)(C) (ISD)
Cc: (b)(6); (b)(7)(C) (ID)
Subject: FW: (b)(6); (b)(7)(C)
Attachments: June 2018 Portal User Guide .pdf, location-data-accuracy-v3.pdf, ATM SKIMMING TEST.pptx

Please see attached and below.

(b)(6); (b)(7)(C)

National Case Coordinator | Operations (J3)
DHS - Joint Task Force Investigations
500 12th Street SW
Washington, DC 20536

(b)(6); (b)(7)(C) desk
(b)(6); (b)(7)(C) cell

From: (b)(6); (b)(7)(C)
Sent: Tuesday, October 09, 2018 9:27 AM
To: (b)(6); (b)(7)(C) @ice.dhs.gov; (b)(6); (b)(7)(C) @ice.dhs.gov; (b)(6); (b)(7)(C) @ice.dhs.gov
Subject: RE: (b)(6); (b)(7)(C) CONTACT LIST

(b)(6); (b)(7)(C)

My apologies for not getting this to you sooner. I was taken out by a vicious cold. Attached is the geolocation software (VENNTEL) user guide and an article on geolocation accuracy. We have run several experiments with this software and are still evaluating it.

The PowerPoint is a test I did on an ATM skimming incident reported by the New York State Police Fusion Center. The experiment was to use the geolocation software to ID locations an ATM skimmer may have visited. The problem was, although we had a photo, not timestamp was provided on the image. We had the date and location of the ATM, but that was it. It led to some interesting results. We think we may have ID'd a couple of banks the suspect visited and also a residence. The problem turned out that there were numerous people associated with the residence so we stopped there. It would be necessary to run all the known individuals at the residence to find a viable suspect. I am hoping that if given a photo with a timestamp and a location, we may be able to obtain similar results by utilizing the same methodology. In this manner, we may be able to ID other ATMs the suspect hit and possible stash houses.

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Tuesday, October 2, 2018 1:18 PM
To: (b)(6); (b)(7)(C) @ice.dhs.gov; (b)(6); (b)(7)(C)

Page 3401 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3402 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3403 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3404 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3405 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3406 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3407 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3408 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3409 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3410 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3411 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3412 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3413 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3414 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3415 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3416 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3417 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3418 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3419 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3420 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3440 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3441 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3442 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3443 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3444 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3445 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3446 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3447 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3448 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3449 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3450 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act

Page 3451 of 3451

Withheld Pursuant to Exemption

(b)(4)

of the Freedom of Information & Privacy Act