

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:**  
**Subject:** FW: ES#: 20-0001481 - Tasker Response Due Date: 9/14/2020 1:00 PM - HAC-HS inquiry Contract Awards to Venntel  
**Date:** Friday, September 11, 2020 2:25:00 PM  
**Attachments:** [CBP - OPO Contracts with Venntel Response 9.9.2020.docx](#)  
[INCOMING.msg](#)

---

(b)(6) - I asked S&T Exec Sec to make sure S&T was tasked to review the tasker. I'll submit the same comment we submitted to OGC Exec Sec to S&T Exec Sec to ensure consistency.

---

(b)(6)  
Attorney - Technology Programs Law Division  
Office of the General Counsel  
Department of Homeland Security  
(b)(6) Office)  
(b)(6) Cell)  
(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

---

**From:** S&T Exec Sec <SandTExecSec@hq.dhs.gov>  
**Sent:** Friday, September 11, 2020 2:20 PM

(b)(6)

(b)(6)

**Subject:** ES#: 20-0001481 - Tasker Response Due Date: 9/14/2020 1:00 PM - HAC-HS inquiry  
Contract Awards to Venntel

S & T Tasking Tracker

---

**ES#:** 20-0001481

**Subject:** HAC-HS inquiry Contract Awards to Venntel

**Summary:** The HAC-HS has questions regarding a contract award from DHS to Venntel. Congress has been looking into this on the basis of privacy concerns. The specific questions from the Hill are as follows

1. What office made this purchase and what is the plan for the usage of the software?
2. Has DHS purchased this service or software before (or Similar software/service)?
3. If we have purchased similar software, when and how much was awarded and how was it used?

Attached for clearance is the DHS OCPO response to the HAC-HS inquiry, including information on S&T contracts.

**Special Instructions:** FBD, please take lead. OSE- Steve Dennis and Jamie Johnson are already aware of this tasker and should be expecting it. Please review and add any information if any is missing and/or edit the information provided about S&T's contracts with this company. Please let us know if you have any questions. Please send your response no later than 1PM on Monday, 9/14/20.

Thank you,

(b)(6)

**Assignees:**

**S&T Division(s):** SPO;AGC;MCS;OSE;OIC;Privacy;FBD;OLA

**Primary Division:** FBD

**Individual(s):**

**Response Due Date:** 9/14/2020 1:00 PM

**Exec Sec Action Officer:** (b)(6)

Click [here](#) to view your Taskers.

---

For general assistance from the S&T Collaborative Solutions Team, [click here](#) to open a new ticket.

**From:** (b)(6)  
**Sent:** 10 Sep 2020 14:50:15 +0000  
**To:** OGC Exec Sec;PLCY EXEC SEC;OLA Exec Sec  
**Cc:** (b)(6)  
**Subject:** FOR DHS CLEARANCE: Contract Awards to Venntel  
**Attachments:** CBP\_\_OPO Contracts with Venntel Response 9.9.2020.docx, RE: Requests to vendors for information on use of DHS tools, Requests to vendors for information on use of DHS tools

Good Morning,

Attached for clearance is the DHS OCPO response to the HAC-HS inquiry asking the Department to identify any contracts awarded to Venntel, who is believed to collect location data from smart phones and sell it to clients. Congress has been looking into this on the basis of privacy concerns. .

Also, for your awareness, the SAC-HS Majority Clerk reached out to Holly Mehringer, Budget Director, informing her that Senator Wyden (D-OR) sent a letter directly to Venntel for information instead of working through the Department. Please see the attached emails.

Clearance is requested from PLCY, OLA, and OGC Oversight. Please provide comments or edits **NLT 10:00 AM tomorrow, September 11, 2020.**

If you have any questions, please let me know.

V/r,

(b)(6)

(b)(6)

Deputy Assistant Director, Budget Division  
Office of the Chief Financial Officer  
U.S. Department of Homeland Security

Office: (b)(6)

Cell: (b)(6)

(b)(6)

**From:** Babb, Peter (Appropriations)  
**Sent:** 25 Aug 2020 20:08:18 +0000  
**To:** (b)(6)  
**Cc:** Harper, Justin (Appropriations); White, Kamela (Appropriations)  
**Subject:** RE: Requests to vendors for information on use of DHS tools

Were Policy and other relevant folks aware of this? There was some press on this today related to a CBP contract:

<https://www.businessinsider.com/cbp-venntel-contract-phone-location-data-2020-8>

---

**From:** Babb, Peter (Appropriations)  
**Sent:** Friday, July 31, 2020 1:01 PM  
**To:** (b)(6)  
**Cc:** Harper, Justin (Appropriations); (b)(6); White, Kamela (Appropriations); (b)(6)  
**Subject:** Requests to vendors for information on use of DHS tools

Good day,

I just wanted you to be aware that Senator Wyden's staff has requested all correspondence from CBP/ICE from a couple vendors (Venntel, Babel Street) on some products/services DHS purchases, and wanted you to be aware of the potential sharing of this information. I would guess that Senator Wyden is requesting information from vendors, rather than from DHS for reasons of expedience.

I have known of one of the product's uses for years, and know that DHS uses some of the described data to help keep the homeland safe. Senator Wyden's staff indicated to others in industry that are some more "big articles" coming out soon and they are calling more companies for information and will possibly send letters. Attached is a letter from the House Oversight Committee and below are two related articles. There's a lot going on with civil liberties (in line with the email from Scott/me earlier today). I don't have a real ask here, other than making sure that folks in Policy and elsewhere are aware of these requests, as if these tools are critical for legitimate law enforcement purposes, it probably makes sense for DHS to present a united front in responding to these inquiries and justifying the use of these tools.

Thanks,  
Peter

[Academic Project Used Marketing Data to Monitor Russian Military Sites](#)

And

[House Investigating Company Selling Phone Location Data to Government Agencies](#)

**From:** Babb, Peter (Appropriations)  
**Sent:** 31 Jul 2020 17:01:04 +0000  
**To:** (b)(6)  
**Cc:** Harper, Justin (Appropriations); White, Kamela (Appropriations)  
**Subject:** Requests to vendors for information on use of DHS tools  
**Attachments:** House Oversight, Wyden, Venntel letter.pdf

Good day,

I just wanted you to be aware that Senator Wyden's staff has requested all correspondence from CBP/ICE from a couple vendors (Venntel, Babel Street) on some products/services DHS purchases, and wanted you to be aware of the potential sharing of this information. I would guess that Senator Wyden is requesting information from vendors, rather than from DHS for reasons of expedience.

I have known of one of the product's uses for years, and know that DHS uses some of the described data to help keep the homeland safe. Senator Wyden's staff indicated to others in industry that are some more "big articles" coming out soon and they are calling more companies for information and will possibly send letters. Attached is a letter from the House Oversight Committee and below are two related articles. There's a lot going on with civil liberties (in line with the email from Scott/me earlier today). I don't have a real ask here, other than making sure that folks in Policy and elsewhere are aware of these requests, as if these tools are critical for legitimate law enforcement purposes, it probably makes sense for DHS to present a united front in responding to these inquiries and justifying the use of these tools.

Thanks,  
Peter

[Academic Project Used Marketing Data to Monitor Russian Military Sites](#)

And

[House Investigating Company Selling Phone Location Data to Government Agencies](#)

**Congress of the United States**  
**Washington, DC 20515**

June 24, 2020

Mr. Chris Gildea  
President  
Venntel, Inc.  
2201 Cooperative Way, Suite 600  
Herndon, VA 20171

Dear Mr. Gildea:

We are investigating the collection and sale of sensitive mobile phone location data that reveals the precise movements of millions of American adults, teens, and even children. We seek information about your company's provision of consumer location data to federal government agencies for law enforcement purposes without a warrant and for any other purposes, including in connection with the response to the coronavirus crisis.

The vast majority of Americans carry cell phones with apps capable of collecting precise location information 24 hours a day, 7 days a week. This location-tracking raises serious privacy and security concerns. As Chief Judge Roberts wrote in the *Carpenter* opinion, "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."<sup>1</sup> This location data can reveal where we go and with whom we associate, tracking us in our homes, at the doctor, or at church.<sup>2</sup>

With Americans installing contact-tracing apps as part of the effort to limit the spread of COVID-19, it has become increasingly important to make sure that the American public has a full understanding of who is collecting their location data, how it may be provided to the government, and what the government is doing with it.

It was recently reported that a contact-tracing app recommended to residents by the governors of North Dakota and South Dakota was sending location data to a third party—in violation of promises made to users.<sup>3</sup> According to that third party, the data was not used; nevertheless, this example shows that Americans may increasingly be unwittingly handing over their location data to unknown third party data brokers such as Venntel. There are limited restrictions on how this data may be sold to and used by the federal government.

---

<sup>1</sup> *Carpenter v. United States*, 138 S.Ct. 2206 (2018).

<sup>2</sup> *The Government Uses 'Near Perfect Surveillance' Data on Americans*, New York Times (Feb. 7, 2020) (online at [www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html](http://www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html)).

<sup>3</sup> *One of the First Contact-Tracing Apps Violates Its Own Privacy Policy*, Washington Post (May 21, 2020) (online at [www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/](http://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/)).

In February, the Wall Street Journal reported that Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) purchased consumers' location data from Venntel and used it without a warrant to identify, locate, and arrest migrants.<sup>4</sup> According to the report:

The Trump administration 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. ... The location data is drawn from ordinary cellphone apps, including those for games, weather and e-commerce, for which the user has granted permission to log the phone's location.<sup>5</sup>

Federal spending records indicate that the Drug Enforcement Agency (DEA), Federal Bureau of Investigation (FBI), and Internal Revenue Service (IRS) also may have obtained data or data services from your company.<sup>6</sup> Furthermore, federal, state, and local governments reportedly are using or considering the use of cell phone location data to track the spread of the coronavirus.<sup>7</sup>

The Supreme Court has held that the government must obtain a warrant before agencies can obtain location data from wireless phone companies and technology companies like Facebook and Google. By acting as an intermediary in the sale of this data, your company may be selling data to the government that it otherwise would need a warrant to compel, impacting the privacy of millions of people, including vulnerable populations like children.<sup>8</sup>

Consumers often do not understand that popular apps for weather, travel, shopping, and other purposes—which may have legitimate needs for location data—may be selling this data to brokers.<sup>9</sup> An investigation in 2018 by the New York Times uncovered 75 companies that were

---

<sup>4</sup> *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall Street Journal (Feb. 7, 2020) (online at [www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600](http://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600)).

<sup>5</sup> *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall Street Journal (Feb. 7, 2020) (online at [www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600](http://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600)).

<sup>6</sup> *USASpending.gov* (accessed June 22, 2020).

<sup>7</sup> *U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus*, Washington Post (Mar. 17, 2020) (online at [www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/](http://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/)); *Government Tracking How People Move Around in Coronavirus Pandemic*, Wall Street Journal (Mar. 28, 2020) (online at [www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202](http://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202));

<sup>8</sup> See 18 U.S.C. § 2702.

<sup>9</sup> *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, New York Times (June 12, 2019) (online at [www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html](http://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html)); Federal Trade Commission, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers* (Dec. 5, 2013) (online at [www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived](http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived)).



buying and selling mobile app-derived location data.<sup>10</sup> Location-targeted advertising sales are predicted to reach an estimated \$27 billion this year.<sup>11</sup>

The scale of this data collection is staggering. For example, Venntel's reported parent company, Gravy Analytics,<sup>12</sup> has revealed that it collects location data from software "embedded within tens of thousands of apps."<sup>13</sup> According to its website, Gravy Analytics "processes billions of pseudonymous mobile location signals every day from millions of mobile devices."<sup>14</sup> Despite claims that anonymization protects privacy, computer scientists and journalists repeatedly have demonstrated the ease with which individuals in purportedly anonymized data sets may be identified.<sup>15</sup>

Reports also indicate that location data is vulnerable to hacking and that this data could lead to individuals being targeted for commercial or political purposes, stalking, or discrimination.<sup>16</sup> In 2017, the Massachusetts Attorney General reached a settlement with a company that targeted advertisements to "abortion-minded women" entering reproductive health facilities and methadone clinics in multiple states.<sup>17</sup> Media reports have also identified companies targeting advertisements to people in emergency rooms<sup>18</sup> and dialysis centers.<sup>19</sup> In

---

<sup>10</sup> *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, New York Times (Dec. 10, 2018) (online at [www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html](http://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html)).

<sup>11</sup> *Location Targeted Mobile Advertising Spending in the United States from 2016 to 2023*, Statista (Nov. 8, 2019) (online at [www.statista.com/statistics/274837/local-and-national-mobile-us-ad-spending-since-2009/](http://www.statista.com/statistics/274837/local-and-national-mobile-us-ad-spending-since-2009/)).

<sup>12</sup> *Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones*, Protocol (Mar. 5, 2020) (online at [www.protocol.com/government-buying-location-data](http://www.protocol.com/government-buying-location-data)).

<sup>13</sup> Gravy Analytics, *Location Data & COVID-19* (online at [gravyanalytics.com/covid-19/](http://gravyanalytics.com/covid-19/)) (accessed June 22, 2020).

<sup>14</sup> Gravy Analytics, *Our Data* (online at [gravyanalytics.com/our-data/](http://gravyanalytics.com/our-data/)) (accessed June 22, 2020).

<sup>15</sup> *Twelve Million Phones, One Dataset, Zero Privacy*, New York Times (Dec. 19, 2019) (online at [www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html](http://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html)).

<sup>16</sup> *A Location-Sharing Disaster Shows How Exposed You Really Are*, Wired (May 19, 2018) (online at [www.wired.com/story/locationsmart-securus-location-data-privacy/](http://www.wired.com/story/locationsmart-securus-location-data-privacy/)); *Hundreds of Apps Can Empower Stalkers to Track Their Victims*, New York Times (May 19, 2018) (online at [www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html](http://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html)); *Catholics in Iowa Went to Church. Steve Bannon Tracked Their Phones*, ThinkProgress (July 19, 2019) (online at <https://thinkprogress.org/exclusive-steve-bannon-geofencing-data-collection-catholic-church-4aaeacd5c182/>); Senate Committee on Commerce, Science, and Transportation, Ranking Member Maria Cantwell, *The State of Online Privacy and Data Security* (Nov. 2019) (online at [www.cantwell.senate.gov/imo/media/doc/The%20State%20of%20Online%20Privacy%20and%20Data%20Security.pdf](http://www.cantwell.senate.gov/imo/media/doc/The%20State%20of%20Online%20Privacy%20and%20Data%20Security.pdf)).

<sup>17</sup> *Firm Settles Massachusetts Probe over Anti-abortion Ads Sent to Phones*, Reuters (Apr. 4, 2017) (online at [www.reuters.com/article/us-massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSKBN1761PX](http://www.reuters.com/article/us-massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSKBN1761PX)).

<sup>18</sup> *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, New York Times (Dec. 10, 2018) (online at [www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html](http://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html)).

<sup>19</sup> *Political Campaigns Know Where You've Been. They're Tracking Your Phone*, Wall Street Journal (Oct. 10, 2019) (online at [www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889](http://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889)).

2019, the Los Angeles City Attorney brought a lawsuit against the Weather Channel and its parent company, IBM, which sell data collected from the Weather Channel app's 45 million users. The City Attorney alleged the companies deceptively collected, shared, and profited from the location information of millions of American consumers.<sup>20</sup>

In February 2020, the Federal Communications Commission (FCC) fined the four major wireless carriers, Verizon, AT&T, T-Mobile, and Sprint, for selling location data without the knowledge or consent of their subscribers. In issuing the fines, the FCC described the sensitivity of location data and its potential for abuse:

The precise physical location of a wireless device is an effective proxy for the precise physical location of the person to whom that phone belongs at that moment in time. Exposure of this kind of deeply personal information puts those individuals at significant risk of harm—physical, economic, or psychological. For consumers who have job responsibilities in our country's military, government, or intelligence services, exposure of this kind of information can have serious national security implications.<sup>21</sup>

For all of these reasons, please provide the following information and documents by July 8, 2020, for the period from January 1, 2016, to the present:

1. For each provision of goods or services to a federal agency by your company:
  - a. documents sufficient to show the nature and purpose of the product or service provided and any use case or justification provided by the purchasing agency;
  - b. documents sufficient to show any actions that Venntel or its suppliers take to obtain the consent of the individuals whose location and other data is provided to or accessed by the agency;
  - c. all documents relating to any restrictions on how the agency may use the product or service, including whether the agency may share information with other federal or state government agencies and whether Venntel and the agency entered into a nondisclosure agreement regarding the agency's use of Venntel's services;
  - d. documents sufficient to show Venntel's revenue from the sale or provision of the goods or services;
  - e. copies of all contracts or agreements relating to the sale or provision of the goods or services;
2. All correspondence between Venntel and any employee, official, or representative of any federal department, federal agency, or executive branch office;

---

<sup>20</sup> *Los Angeles Accuses Weather Channel App of Covertly Mining User Data*, New York Times (Jan. 3, 2019) (online at [www.nytimes.com/2019/01/03/technology/weather-channel-app-lawsuit.html](http://www.nytimes.com/2019/01/03/technology/weather-channel-app-lawsuit.html)).

<sup>21</sup> *See, e.g.*, Federal Communications Commission, *Notice of Apparent Liability for Forfeiture and Admonishment*, T-Mobile (Feb. 28, 2020) (online at <https://docs.fcc.gov/public/attachments/FCC-20-27A1.pdf>).

3. A list of all customers who purchase, license, or access location data from Venntel or any Venntel subsidiary. For each customer, please provide the following:
  - a. documents sufficient to show the nature and purpose of the product or service provided;
  - b. documents sufficient to show any actions that Venntel or its suppliers take to obtain the consent of the individuals whose location and other data is provided to or accessed by the customer;
  - c. all documents relating to any restrictions on how the customer may use the product or service;
  - d. copies of all contracts or agreements relating to the sale or provision of the goods or services;
  - e. for any foreign entity, detail the steps Venntel has taken to seek and obtain export licenses for these sales;
4. A description of any COVID-19 related efforts that Venntel is involved in, including:
  - a. any COVID-19-related apps from which Venntel collects or has collected data;
  - b. any documents related to the provision of goods or services to federal agencies, state governments, local law enforcement, and foreign entities, related to monitoring or mitigating the COVID-19 pandemic; and
5. Documents sufficient to show the specific location data that Venntel collects, other information it collects (*e.g.*, Advertising ID, wireless information, web search history, phone or demographic information), and how is it paired or combined with location data;
6. Documents sufficient to show the number of individuals from whom Venntel collects location data;
7. Information indicating how long Venntel keeps user data, regardless of whether it is anonymized;
8. Documents sufficient to identify all sources from which Venntel and its upstream suppliers have received consumer location and other data which it provides to any government agency, and the specific type of data collected from each source. For each source, please provide documents sufficient to show the following:
  - a. the amount paid by Venntel to receive location data from that source;
  - b. copies of all contracts or written agreements with that source;
9. Documents sufficient to show all measures Venntel or its upstream suppliers take, if any, to ensure the anonymity of users whose data is collected by Venntel;

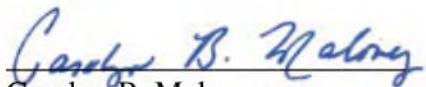
10. Documents sufficient to show all steps Venntel takes, contractually or otherwise, to ensure that its customers do not attempt to re-identify anonymized data provided to them;
11. A description of how Venntel ensures that all data it buys and sells, licenses, or provides access to was obtained from individuals who consented to the collection of, use of, sale of, or sale of access to their data, including to federal agencies and law enforcement agencies;
12. A description of any data security practices and policies Venntel uses to ensure that location data is not accessed without authorization;
13. A description of each instance in which Venntel's location data has been breached or accessed without authorization; and
14. Copies of all policies and procedures related to the collection, use, license, or sale of location data, including with respect to data security, data privacy, user consent, and anonymization.

The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

An attachment to this letter provides additional instructions for responding to this request. If you have any questions regarding this request, please contact Committee staff at (202) 225-5051, Senator Warren's staff at (202) 224-4543, or Senator Wyden's staff at (202) 224-5244.

Thank you for your attention to this important matter.

Sincerely,



Carolyn B. Maloney  
Chairwoman  
House Committee on Oversight and Reform



Elizabeth Warren  
United States Senator



Ron Wyden  
United States Senator



Mark DeSaulnier  
Member of Congress

Enclosure

cc: The Honorable Jim Jordan, Ranking Member,

Mr. Chris Gildea  
Page 7

House Committee on Oversight and Reform

## Responding to Oversight Committee Document Requests

1. In complying with this request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. Produce all documents that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party.
2. Requested documents, and all documents reasonably related to the requested documents, should not be destroyed, altered, removed, transferred, or otherwise made inaccessible to the Committee.
3. In the event that any entity, organization, or individual denoted in this request is or has been known by any name other than that herein denoted, the request shall be read also to include that alternative identification.
4. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, thumb drive, or secure file transfer) in lieu of paper productions.
5. Documents produced in electronic format should be organized, identified, and indexed electronically.
6. Electronic document productions should be prepared according to the following standards:
  - a. The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
  - b. Document numbers in the load file should match document Bates numbers and TIF file names.
  - c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
  - d. All electronic documents produced to the Committee should include the following fields of metadata specific to each document, and no modifications should be made to the original metadata:  
  
BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,

INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,  
BEGATTACH.

7. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, zip file, box, or folder is produced, each should contain an index describing its contents.
8. Documents produced in response to this request shall be produced together with copies of file labels, dividers, or identifying markers with which they were associated when the request was served.
9. When you produce documents, you should identify the paragraph(s) or request(s) in the Committee's letter to which the documents respond.
10. The fact that any other person or entity also possesses non-identical or identical copies of the same documents shall not be a basis to withhold any information.
11. The pendency of or potential for litigation shall not be a basis to withhold any information.
12. In accordance with 5 U.S.C. § 552(d), the Freedom of Information Act (FOIA) and any statutory exemptions to FOIA shall not be a basis for withholding any information.
13. Pursuant to 5 U.S.C. § 552a(b)(9), the Privacy Act shall not be a basis for withholding information.
14. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
15. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) every privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, addressee, and any other recipient(s); (e) the relationship of the author and addressee to each other; and (f) the basis for the privilege(s) asserted.
16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (by date, author, subject, and recipients), and explain the circumstances under which the document ceased to be in your possession, custody, or control.
17. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents that would be responsive as if the date or other descriptive detail were correct.

18. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data, or information not produced because it has not been located or discovered by the return date shall be produced immediately upon subsequent location or discovery.
19. All documents shall be Bates-stamped sequentially and produced sequentially.
20. Two sets of each production shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2105 of the Rayburn House Office Building.
21. Upon completion of the production, submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control that reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

### **Definitions**

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, data, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, communications, electronic mail (email), contracts, cables, notations of any type of conversation, telephone call, meeting or other inter-office or intra-office communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, mail, releases, electronic



message including email (desktop or mobile device), text message, instant message, MMS or SMS message, message application, or otherwise.

3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information that might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neutral genders.
4. The term “including” shall be construed broadly to mean “including, but not limited to.”
5. The term “Company” means the named legal entity as well as any units, firms, partnerships, associations, corporations, limited liability companies, trusts, subsidiaries, affiliates, divisions, departments, branches, joint ventures, proprietorships, syndicates, or other legal, business or government entities over which the named legal entity exercises control or in which the named entity has any ownership whatsoever.
6. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual’s complete name and title; (b) the individual’s business or personal address and phone number; and (c) any and all known aliases.
7. The term “related to” or “referring or relating to,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with, or is pertinent to that subject in any manner whatsoever.
8. The term “employee” means any past or present agent, borrowed employee, casual employee, consultant, contractor, de facto employee, detailee, fellow, independent contractor, intern, joint adventurer, loaned employee, officer, part-time employee, permanent employee, provisional employee, special government employee, subcontractor, or any other type of service provider.
9. The term “individual” means all natural persons and all persons or entities acting on their behalf.

OPOAM 3016.505-90(a)(2)(iv)  
 Justification for Brand Name Exception to Fair Opportunity  
 Exceeding the SAT pursuant to FAR 16.505(a)(4)

JEFO No.:

Date: March 2018

PR Number:

1. Agency and Contracting Activity. Identification of the agency and the contracting activity, and specific identification of the document as a “Justification for an Exception to Fair Opportunity.”

The Department of Homeland Security, Office of Procurement Operations, Science and Technology Acquisition Division (STAD) on behalf of the Science and Technology Directorate (S&T), Homeland Security Advanced Research Projects Agency (HSARPA) Data Analytics Engine (DA-E) prepared this justification for an exception to fair opportunity.

2. Nature and/or description of the **action** being approved.

DHS/OPO/S&T intends to award a delivery order without considering other brand names pursuant to FAR 16.505(b)(2)(i)(B) for the procurement of the Venntel Marketing Data. DHS/OPO/S&T intends to solicit the Venntel Marketing Data from authorized First Source II vendors to ensure a fair and reasonable price.

3. A description of the supplies or services required to meet the agency’s need (including the estimated value).

S&T Homeland Security Advanced Research Agency (HSARPA) Data Analytics Engine (DA-E) has a need for Venntel Marketing Data for research and development. The Venntel marketing data HSARPA DA-E is seeking is as follows:

SKU	Product Description	Qty
	Venntel Geographic Marketing Data	1
	Venntel Geographoc Marketing Data Service Support	1

The estimated value of this action is \$392,000.

The IGCE for this effort is \$380,000. The period of performance is for twelve months from date of award.

<u>Period</u>		<u>Unit Price</u>	<u>Total</u>
Data	12 mo.	(b)(4)	(b)(4)
Support	12 mo.		

JEFO No. FY17-2712

Rev. 2/5/2016

OPOAM 3016.505-90(a)(2)(iv)  
Justification for Brand Name Exception to Fair Opportunity  
Exceeding the SAT pursuant to FAR 16.505(a)(4)

Total        \$392,000

4. Identify the exception to fair opportunity and supporting rationale.

OPO intends to procure a brand name specification for the Venntel Marketing Data in accordance with FAR 16.505(a)(4)(i). The exception is based on FAR 16.505(b)(2)(i)(B), only one source is capable of providing the Venntel Marketing Data because the Venntel Marketing Data is unique and highly specialized.

Market research has indicated that the for data transformation that are ideal to the developing requirements within HSARPA. Venntel offers broad and uncontrolled access to the underlying data set, making it possible for HSARPA to investigate the utility of this data across a broad set of use cases and potential applications. HSARPA researched software tools similar to the Venntel Portal, including Babel Street's Locate X, Google Mobile Analytics and Apple Application Analytics. Babel Street basically re-hosts Venntel's data set at a greater cost and with significant constraints on data access. Google and Apple offer access to some of the same data but unlike Venntel, do not provide access to cleaned and deduped data sets and have resisted government use cases. Therefore, HSARPA has determined to test and evaluate Venntel Marketing Data at this time in order to determine if this data provides value to DHS mission sets, and to determine compatibility with laboratory infrastructure, to evaluate its performance, and to determine the value of this tool in the formulation of future DHS enterprise analytic requirements.

Procuring the Venntel Marketing Data is essential to the Government's requirements under the Data Analytics Engine program because Venntel Marketing Data is unique and highly specialized for Government mission spaces. Procuring the Venntel Portal as described herein allows HSARPA to properly evaluate a rapidly emerging technology that has demonstrated significant promise for the government's counter-terrorism mission. In the future, other software may also be tested.

5. Determination by the contracting officer that the anticipated cost to the Government will be fair and reasonable.

The Contracting Officer has determined that issuing the proposed order for brand name Venntel Marketing Data represents the best value and will result in the lowest overall cost, considering price and administrative costs, to meet the Government's needs. DHS will solicit this requirement through the FirstSource II IDIQ and anticipates receiving more than one offer, which will ensure a competitive award is made at a fair and reasonable price.

6. Any other facts supporting the justification.

OPOAM 3016.505-90(a)(2)(iv)  
Justification for Brand Name Exception to Fair Opportunity  
Exceeding the SAT pursuant to FAR 16.505(a)(4)

No other facts are provided.

7. A statement of the actions, if any, the agency may take to remove or overcome any barriers that led to the exception to fair opportunity before any subsequent acquisition for the supplies or services is made.

Approval to purchase the Venntel Marketing Data is for the purposes of product testing only and is not to be used as a de facto evaluation and/or market research. Once testing is completed, the program office will define its functional requirements and competitively solicit those requirements as they will no longer need to support a brand name action based on the test findings

8. DHS intends to include the JEFO with the solicitation for this requirement to all vendors in the HUBZone track of the FirstSource II Vehicle.

9. Technical/Requirements Personnel Certification.

Pursuant to FAR 16.505(b)(2)(ii)(B)(9), I certify that this requirement meets the Government's minimum need and that the supporting data, which form a basis for the justification, are accurate and complete.

\_\_\_\_\_  
(b)(6)

Technical Representative/COR

\_\_\_\_\_  
Date

10. Contracting Officer Certification and/or Approval \*

Pursuant to FAR 16.505(b)(2)(ii)(B)(8), I certify that this justification is accurate and complete to the best of my knowledge and belief and hereby determine that the circumstances for an exception to fair opportunity exist:

\_\_\_\_\_  
Not exceeding \$700,000

(b)(6)

Contracting Officer

\_\_\_\_\_  
Date

OPOAM 3016.505-90(a)(2)(iv)  
Justification for Brand Name Exception to Fair Opportunity  
Exceeding the SAT pursuant to FAR 16.505(a)(4)

JEFO No.: FY18-0223

Date: April 30, 2018

PR Number: RSAR-18-00056

1. Agency and Contracting Activity. Identification of the agency and the contracting activity, and specific identification of the document as a “Justification for an Exception to Fair Opportunity.”

The Department of Homeland Security, Office of Procurement Operations, Science and Technology Acquisition Division (STAD) on behalf of the Science and Technology Directorate (S&T), Homeland Security Advanced Research Projects Agency (HSARPA) Data Analytics Engine (DA-E) prepared this justification for an exception to fair opportunity.

2. Nature and/or description of the **action** being approved.

DHS/OPO/S&T intends to award a delivery order without considering other brand names pursuant to FAR 16.505(b)(2)(i)(B) for the procurement of the Venntel Marketing Data. DHS/OPO/S&T intends to solicit the Venntel Marketing Data from authorized First Source II vendors to ensure a fair and reasonable price. Approval for brand name justification was granted by the competition advocate (STAD Division Director) on April 30, 2018.

3. A description of the supplies or services required to meet the agency’s need (including the estimated value).

S&T Homeland Security Advanced Research Agency (HSARPA) Data Analytics Engine (DA-E) has a need for Venntel Marketing Data for research and development. The Venntel marketing data HSARPA DA-E is seeking is as follows:

SKU	Product Description	Qty
	Venntel Geographic Marketing Data	1
	Venntel Geographoc Marketing Data Service Support	1

The Venntel software marketing data tool offers broad and uncontrolled access to the underlying data set, making it possible for HSARPA to investigate the utility of this data across a broad set of use cases and potential applications. The Venntel Portal is a unique and highly specialized tool that brings together 80,000 mobile applications into a single source for analytics through a web based portal that provides geo-fencing capabilities.

The estimated value of this action is \$392,000. The period of performance is for twelve months from date of award.

JEFO No. FY18-0223

Rev. 2/5/2016

OPOAM 3016.505-90(a)(2)(iv)  
 Justification for Brand Name Exception to Fair Opportunity  
 Exceeding the SAT pursuant to FAR 16.505(a)(4)

<u>Period</u>		<u>Unit Price</u>	<u>Total</u>
Data	12 mo.	(b)(4)	(b)(4)
Support	12 mo.		
		Total	\$392,000

4. Identify the exception to fair opportunity and supporting rationale.

OPO intends to procure a brand name specification for the Venntel Marketing Data in accordance with FAR 16.505(a)(4)(i). The exception is based on FAR 16.505(b)(2)(i)(B), only one source is capable of providing the Venntel Marketing Data because the Venntel Marketing Data is unique and highly specialized.

Market research has indicated that the for data transformation that are ideal to the developing requirements within HSARPA. Venntel offers broad and uncontrolled access to the underlying data set, making it possible for HSARPA to investigate the utility of this data across a broad set of use cases and potential applications. HSARPA researched software tools similar to the Venntel Portal, including Babel Street’s Locate X, Google Mobile Analytics and Apple Application Analytics. Babel Street basically re-hosts Venntel’s data set at a greater cost and with significant constraints on data access. Google and Apple offer access to some of the same data but unlike Venntel, do not provide access to cleaned and deduped data sets and have resisted government use cases. Therefore, HSARPA has determined to test and evaluate Venntel Marketing Data at this time in order to determine if this data provides value to DHS mission sets, and to determine compatibility with laboratory infrastructure, to evaluate its performance, and to determine the value of this tool in the formulation of future DHS enterprise analytic requirements.

Procuring the Venntel Marketing Data is essential to the Government’s requirements under the Data Analytics Engine program because Venntel Marketing Data is unique and highly specialized for Government mission spaces. Procuring the Venntel Portal as described herein allows HSARPA to properly evaluate a rapidly emerging technology that has demonstrated significant promise for the Government’s counter-terrorism mission and is essential for HSARPA to investigate the utility of this data across a broad set of use cases and potential applications. The use of other similar software products at the present time could result in interoperability, compatibility, interface issues that would preclude HSARPA from providing efficient and effective customer support. In the future, other software may also be tested.

5. Determination by the Contracting Officer that the anticipated cost to the Government will be fair and reasonable.

The Contracting Officer has determined that issuing the proposed action for brand name Venntel Marketing Data against the First DSource II IDIQ contract vehicle represents the best value and will result in the lowest overall cost, considering price and administrative costs, to meet the Government’s needs. The Contracting Officer anticipates receiving more than one quotation, which will ensure a competitive award is made at a fair and reasonable price.

OPOAM 3016.505-90(a)(2)(iv)  
Justification for Brand Name Exception to Fair Opportunity  
Exceeding the SAT pursuant to FAR 16.505(a)(4)

6. Any other facts supporting the justification.

No other facts are provided.

7. A statement of the actions, if any, the agency may take to remove or overcome any barriers that led to the exception to fair opportunity before any subsequent acquisition for the supplies or services is made.

Approval to purchase the Venntel Marketing Data is for the purposes of product testing only and is not to be used as a de facto evaluation and/or market research. Once testing is completed, the program office will define its functional requirements and competitively solicit those requirements as they will no longer need to support a brand name action based on the test findings

8. DHS intends to include the JEFO with the solicitation for this requirement to all vendors in the HUBZone track of the FirstSource II Vehicle.

9. Technical/Requirements Personnel Certification.

Pursuant to FAR 16.505(b)(2)(ii)(B)(9), I certify that this requirement meets the Government's minimum need and that the supporting data, which form a basis for the justification, are accurate and complete.

(b)(6)

(b)(6)

Technical Representative/COR

Date

10. Contracting Officer Certification and/or Approval \*

Pursuant to FAR 16.505(b)(2)(ii)(B)(8), I certify that this justification is accurate and complete to the best of my knowledge and belief and hereby determine that the circumstances for an exception to fair opportunity exist:

Not exceeding \$700,000

(b)(6)

Contracting Officer

Date

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:**  
**Subject:** FW: OIG Request Venntel  
**Date:** Friday, February 5, 2021 10:36:53 AM  
**Attachments:** [RE Geolocation Data Project.msg](#)  
[Mobile Marketing DataVenntel Follow-up .msg](#)  
[RE Venntel Follow up.msg](#)  
[Venntel Follow up.msg](#)  
[RE Connection - Minal to TomKristinRachel.msg](#)  
[RE POC for Ad ID Date and Carpenter Case.msg](#)  
[FW List of Technologies .msg](#)  
[RE Quick White List Experiment.msg](#)  
[FW VenntelProject Alexander.msg](#)

---

Hello,  
Attached are e-mails that we were able to locate about the Venntel project, including e-mail discussion with ICE OPLA. Sending along in case this is helpful for our 2:30 pm internal call today.  
Thanks, (b)(6)

(b)(6)  
Deputy Associate General Counsel  
(Technology Programs)  
Office of the General Counsel  
Department of Homeland Security  
(b)(6) (Office)  
(b)(6) (Mobile)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

---

**From:** (b)(6)  
**Sent:** Thursday, February 4, 2021 9:44 AM  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** OIG Request Venntel

(b)(6) –  
Attached are emails/discussions relating to Venntel that may have pre-dated (b)(6) These do not contain TPLD’s legal analysis but rather identify the issue and capture the discussions that need to occur.

Best,



(b)(6)

---

(b)(6)

Attorney - Technology Programs Law Division  
Office of the General Counsel  
Department of Homeland Security

(b)(6) Office)  
(b)(6) Cell)

(b)(6)

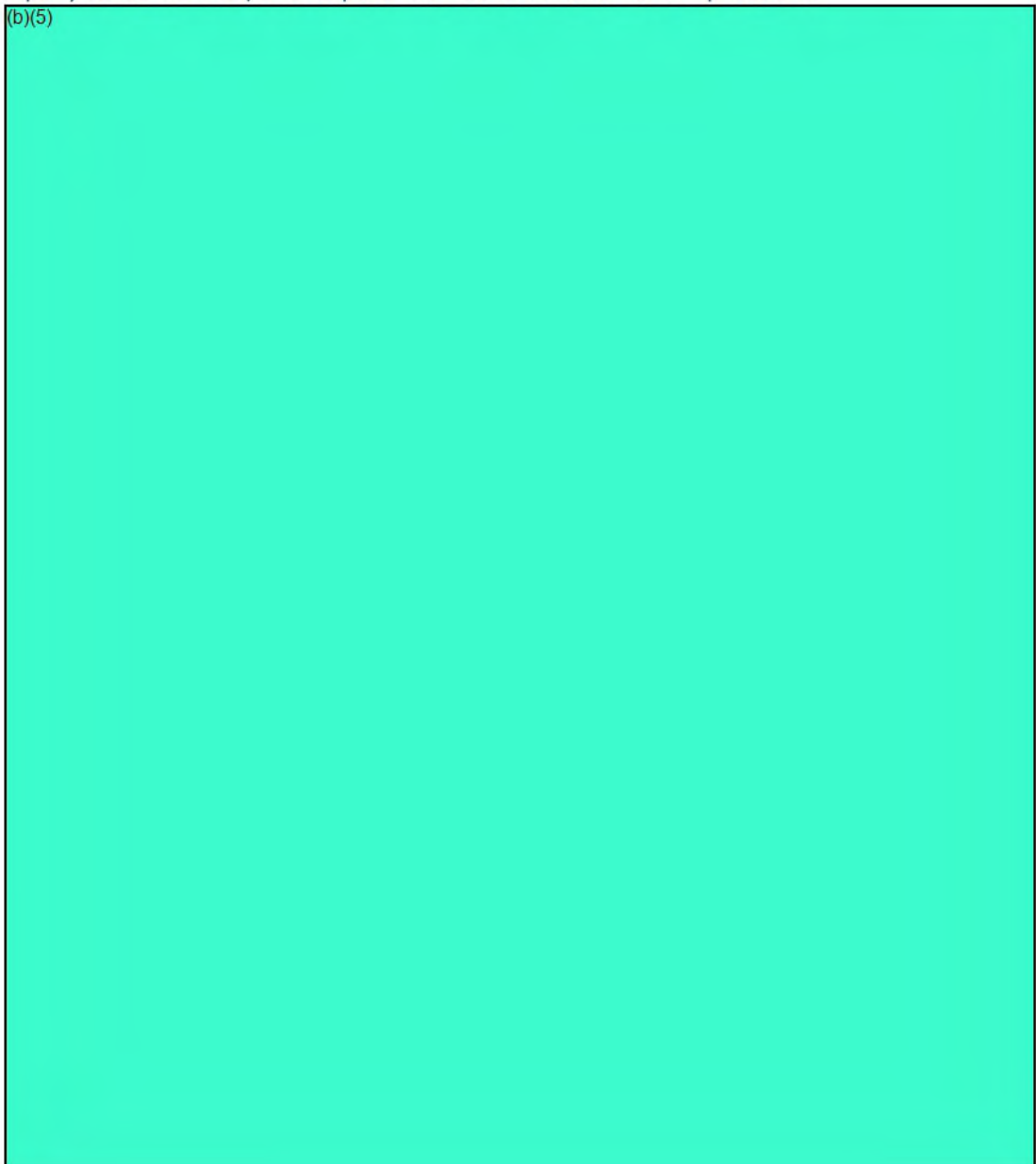
This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

**From:** (b)(6)  
**Sent:** 8 Nov 2019 20:50:08 +0000  
**To:** (b)(6)  
(b)(6)  
**Cc:** (b)(6)  
(b)(6)  
**Subject:** RE: Geolocation Data Project

Good afternoon,  
2:30pm on Tuesday works for CBP OCC. I'm adding a few of my colleagues who may participate in the call.

As you may already be aware, CBP OCC, in consultation with ICE OPLA and S&T counsel, develop the following high-level analysis relating to the use of advertising identification information (in this case, as offered by a company called Venntel) and its potential Fourth Amendment implications:

(b)(5)



(b)(5)

(b)(6)

Senior Attorney  
Office of Chief Counsel  
U.S. Customs and Border Protection  
Desk: (b)(6)

This document, and any attachment(s), may contain information which is law enforcement sensitive, attorney-client privileged, attorney work product, or U.S. Government information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this message or any attachment(s).

**From:** (b)(6)

**Sent:** Friday, November 8, 2019 2:02 PM

(b)(6)

(b)(6)

**Subject:** RE: Geolocation Data Project

I may be out of the office Tuesday due to Jury Duty; I'll know tonight and confirm the appointment on Tuesday.

(b)(6)  
Attorney, Technology Programs  
Office of the General Counsel  
Department of Homeland Security  
(b)(6) (Cell) - Preferred  
(Office)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

**From:** (b)(6)

**Sent:** Friday, November 8, 2019 12:37 PM

(b)(6)

(b)(6)

**Subject:** Geolocation Data Project

All,

First of all, as the newest member of the OGC front office I want to say hello! I know I haven't met some of you yet (digitally or in person), but I look forward to meeting with all of you at some point.

I have included each of you on this email because I am currently working on a project that is looking at the use of geolocation data gathered by third parties, and your names came up as relevant, interested and/or knowledgeable. My hope is to leverage your thinking and perspectives to contribute legal analysis for a guide/framework for the Department.

At this time, I am in the information gathering phase. Specifically, I'm looking into the legal authorities for collecting, storing and using geolocation data by the components and HQ divisions, as well as the potential legal restrictions and requirements, *e.g.*, the Fourth Amendment. Depending on what we already have, the first thing I may ask you to help me with is some more digging on these topics.

I was hoping we could have telecon meeting either Tuesday or Wednesday of next week to discuss the project. Please reply to me, (b)(6) (cc'ed) with your availability on those days.

In the meantime, if you have any written materials/cases/law review articles that you think are relevant, please send them to the group. I can't promise I'll get through all of it before we meet for the first time, but I wouldn't mind some weekend reading.

If you have any questions for me or if you think I've missed someone important in OGC or in legal at one of the components, please let me know. Otherwise, enjoy your Veteran's Day weekend!

Thank you,

(b)(6)

Deputy General Counsel  
Office of the General Counsel  
U.S. Department of Homeland Security

(b)(6)

(Office)  
(Cell)

**From:** (b)(6)  
**Sent:** 26 Aug 2019 20:02:54 +0000  
**To:** (b)(6)  
**Cc:** (b)(6)  
(b)(6)  
**Subject:** Mobile Marketing Data/Venntel Follow-up

DELIBERATIVE  
ATTORNEY WORK PRODUCT

(b)(6)

I've spoken with you or reached out to you in varying degrees about the issue involving DHS' use of Mobile Marketing Data, which includes location data. S&T along with the components, particularly CBP and ICE are exploring how this data may be utilized to support specific DHS mission responsibilities. Earlier this year, S&T and CBP jointly submitted a PTA to HQ Privacy relating to the use of the Mobile Marketing Data. At that time, HQ Privacy flagged the PTA and asked if there were any legal guidance, advice or opinions on file on the implications of the 2018 Supreme Court decision in *Carpenter* and DHS' intended use for the Mobile Marketing Data. There were none.

Since then, CBP OCC (b)(6) and ICE OPLA (b)(6)

(b)(6) have provided a written starting point for the advice that they informally provided to their respective clients. That written analysis is provided below. Thanks to CBP OCC and ICE OPLA, there is a starting place for us to begin having a broader discussion within OGC on the nuances of this matter.

**After you have had a chance to review the information contained herein, I'd like to set up a call for us to provide any additional background information you may need and to lay out the next steps. Are you available for such a call this week?**

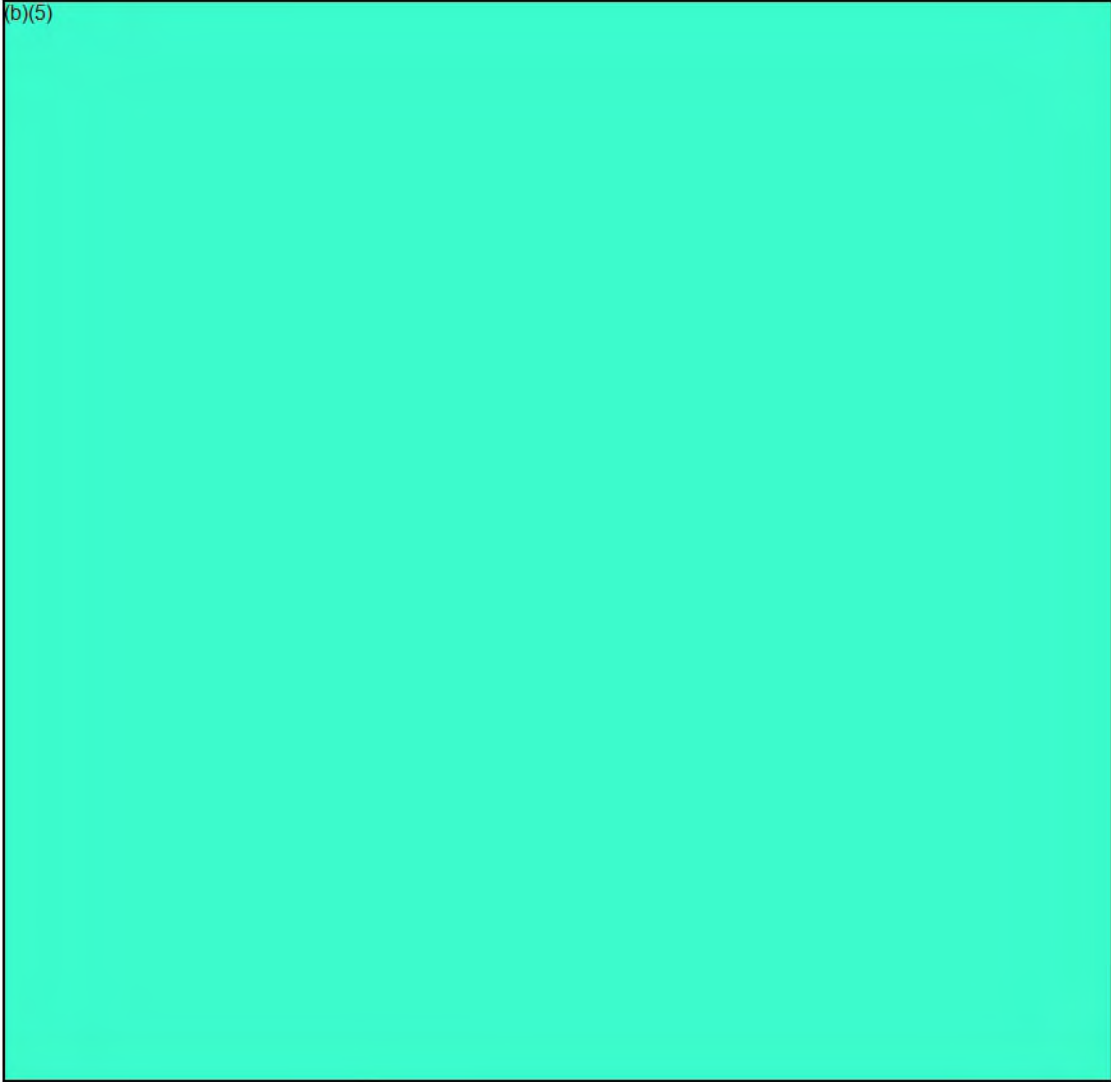
In addition to setting up a time for us to have a preliminary discussion, I'd like to find a time for all of us attorneys to receive a briefing on what Mobile Marketing Data is and how DHS envisions using the data – which can be arranged through ICE and/or CBP with support from the S&T. I will start identifying available times for such a briefing to take place next week or the week after.

Here is the written analysis CBP OCC and ICE OPLA developed:

(b)(5)



(b)(5)



Best,

(b)(6)

---

(b)(6)

Attorney - Technology Programs Law Division

Office of the General Counsel

Department of Homeland Security

(b)(6) (Office)

(b)(6) (Cell)

(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or

copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

*Id.* at 2220. The Court also made clear this does not disturb the third party doctrine under *Smith* and *Miller. Id.* Under longstanding Supreme Court precedent, an individual has no reasonable expectation of privacy under the Fourth Amendment in information voluntarily disclosed to third parties.

We believe *Carpenter* increases the litigation risk associated with use of AdID information, as the reasoning in *Carpenter* could potentially be extended to this type of information in the future. However, we also believe that the commercial acquisition of AdID information is distinguishable from the compelled disclosure of CSLI at issue in *Carpenter*. As we understand it, the AdID information offered by Venntel is generated by applications for which the user has the ability to disable location services or to delete (and, in most cases, the user affirmatively chose to install the application on the phone). Also, AdID is commercially acquired and is generally available for commercial purposes. Furthermore, it's our understanding that this information is generally collected under circumstances where the user has provided express consent for the collection and sharing of information generated by the application. Finally, there is arguably no government intrusion on which to base a search because the information is collected, used, and sold by private parties in the first instance.

Given the differences between CSLI and AdID, we don't think that *Carpenter* is binding on the government's acquisition of commercially available location data and that there is a strong argument that such information continues to be governed by the third-party doctrine. If so, the acquisition of AdID information would not constitute a "search," and thus no warrant would be required.

**PRIVILEGED ATTORNEY-CLIENT COMMUNICATION; FOR OFFICIAL USE ONLY (FOUO)**

Thomas McIntosh

Senior Attorney

Office of Chief Counsel

U.S. Customs and Border Protection

Desk: (304) 724-5827

This document, and any attachment(s), may contain information which is law enforcement sensitive, attorney-client privileged, attorney work product, or U.S. Government information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this message or any attachment(s).

---

**From:** (b)(6)  
**Sent:** Friday, August 9, 2019 2:00 PM  
**To:** WEINSTEIN, RACHEL (OCC) <[rachel.weinstein@cbp.dhs.gov](mailto:rachel.weinstein@cbp.dhs.gov)>; Giles, Margaret M <[Margaret.M.Giles@ice.dhs.gov](mailto:Margaret.M.Giles@ice.dhs.gov)>; MCINTOSH, THOMAS (OCC) <[thomas.j.mcintosh@cbp.dhs.gov](mailto:thomas.j.mcintosh@cbp.dhs.gov)>  
**Cc:** Marcson, Nicole <[Nicole.Marcson@HQ.DHS.GOV](mailto:Nicole.Marcson@HQ.DHS.GOV)>  
**Subject:** Venntel Follow up

(b)(6)  
Thank you for the call earlier this week. As we discussed during the call, attached is the Venntel Briefing (please note the proprietary marking on the briefing) that I received through our S&T programs. Tom, your Venntel briefing document may be slightly different and geared to CBP mission needs.

As we discussed during our call, the next steps at this time (subject to change as we move forward) are:

1. Written preliminary legal guidance: (b)(6) will share the preliminary guidance he provided to CBP with (b)(6) and me. (b)(6) will review and provide input from OPLA's perspective. I will do the same from S&T perspective.
2. Share preliminary legal guidance with DHS HQ OGC Priv (b)(6) Once we have written preliminary guidance that all of us agree on, we can reach out to (b)(6) and share with him our preliminary thinking. We may also loop in other DHS OGC HQ offices (i.e. Operations and Enforcement Law Division), as necessary. (b)(6) may want to have an initial conversation after he has an opportunity to review the preliminary written guidance or he may first want to receive a 101 on this technology and how ICE and CBP envision using this technology.



3. 101 type introduction to Mobile Advertising Data: The components will conduct the initial 101 introduction. If we collectively feel we still have questions, we can potentially get additional information from Venntel, as well.
4. Legal Discussion: CBP OCC, ICE OPLA, S&T OGC, and PRIV OGC meet to discuss the preliminary legal guidance provided and determine if there is concurrence or disagreement amongst all of the DHS legal offices.

I will be on leave beginning mid-week next week into the following week. In my absence, if you need anything, please reach out to (b)(6) Deputy Associate General Counsel for Tech Programs (cc'ed herein).

Best,

(b)(6)

---

(b)(6)

Attorney - Technology Programs Law Division

Office of the General Counsel

Department of Homeland Security

(b)(6) (Office)

(Cell)

(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

Page 034

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

**From:** (b)(6)  
**Sent:** 9 Aug 2019 17:59:47 +0000  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** Venntel Follow up  
**Attachments:** Venntel Briefing June 2018.pdf

(b)(6)

Thank you for the call earlier this week. As we discussed during the call, attached is the Venntel Briefing (please note the proprietary marking on the briefing) that I received through our S&T programs. Tom, your Venntel briefing document may be slightly different and geared to CBP mission needs.

As we discussed during our call, the next steps at this time (subject to change as we move forward) are:

1. Written preliminary legal guidance: (b)(6) will share the preliminary guidance he provided to CBP with (b)(6) and me. (b)(6) will review and provide input from OPLA's perspective. I will do the same from S&T perspective.
2. (b)(6) legal guidance with DHS HQ OGC Priv (b)(6): Once we have written preliminary guidance that all of us agree on, we can reach out to (b)(6) and share with him our preliminary thinking. We may also loop in other DHS OGC HQ offices (i.e. Operations and Enforcement Law Division), as necessary. (b)(6) may want to have an initial conversation after he has an opportunity to review the preliminary written guidance or he may first want to receive a 101 on this technology and how ICE and CBP envision using this technology.
3. 101 type introduction to Mobile Advertising Data: The components will conduct the initial 101 introduction. If we collectively feel we still have questions, we can potentially get additional information from Venntel, as well.
4. Legal Discussion: CBP OCC, ICE OPLA, S&T OGC, and PRIV OGC meet to discuss the preliminary legal guidance provided and determine if there is concurrence or disagreement amongst all of the DHS legal offices.

I will be on leave beginning mid-week next week into the following week. In my absence, if you need anything, please reach out to Nicole Marcson, Deputy Associate General Counsel for Tech Programs (cc'ed herein).

Best,

(b)(6)

---

(b)(6)

Attorney - Technology Programs Law Division  
Office of the General Counsel  
Department of Homeland Security

(b)(6) (Office)  
(b)(6) (Cell)

(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or

copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

**From:** (b)(6)  
**Sent:** 19 Jun 2019 16:24:20 +0000  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** FW: Venntel/Project Alexander  
**Attachments:** RE\_ Alexander Data.pdf, RE\_ Supreme Court case to weigh in on location data privacy.pdf  
**Importance:** High

(b)(6)

I hope this finds you well. Please take a look at the below email from HQ Privacy. I wanted to ping you as this legal analysis would have occurred before my time. Can you please confirm DATC legally acquired the Venntel data they have. I have attached the previous emails that Chris had sent to DATC on the risks of acquiring Venntel data.

They are asking if OGC conducted an analysis under the Carpenter case to ensure that we were able to legally acquire this data.

[https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf)

DATC is under heightened scrutiny as part of the Privacy Audit and HQ Privacy is digging deeper into what DATC is doing to ensure everything is being done properly.

Please advise if these issues were addressed and signed off on by OGC. Thank you for your time and review.

(b)(6)

(b)(6)

Privacy Officer (Acting)  
Science and Technology Directorate  
Department of Homeland Security

(b)(6)

---

**From:** (b)(6)  
**Sent:** Wednesday, June 19, 2019 11:26 AM  
**To:** (b)(6)  
**Subject:** Venntel/Project Alexander

Hi (b)(6)

I understand that S&T has purchased information from Venntel as part of Project Alexander. The PTA was never approved because we had and continue to have significant concerns with this technology. Prior to receiving the information, did OGC conduct an analysis under the Carpenter case to ensure that we are able to legally acquire it?

Thanks,

(b)(6)

(b)(6)

Senior Director, Privacy Compliance

DHS Privacy Office

Desk (b)(6)

Cell: (b)(6)

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** RE: Alexander Data  
**Date:** Monday, June 25, 2018 4:09:05 PM  
**Attachments:** [PTA ST - DHS ST Alexander \(ICE IGP 05 11 2018\) - CSL responses 15 JUN 2....docx](#)  
[PTA ST - DHS ST Alexander CBP 6 14 18 - Border Patrol Incident PTA updat....docx](#)  
[image002.png](#)

---

Hi (b)(6)

I'm checking in to see what questions/comments you have on the PTA.

Is CBP legal drafting new guidance on location privacy in light of the *Carpenter* Supreme Court ruling last week? [https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf)

(b)(6)

(b)(6)

**Directorate Privacy Officer | Science & Technology Directorate | Department of Homeland Security**

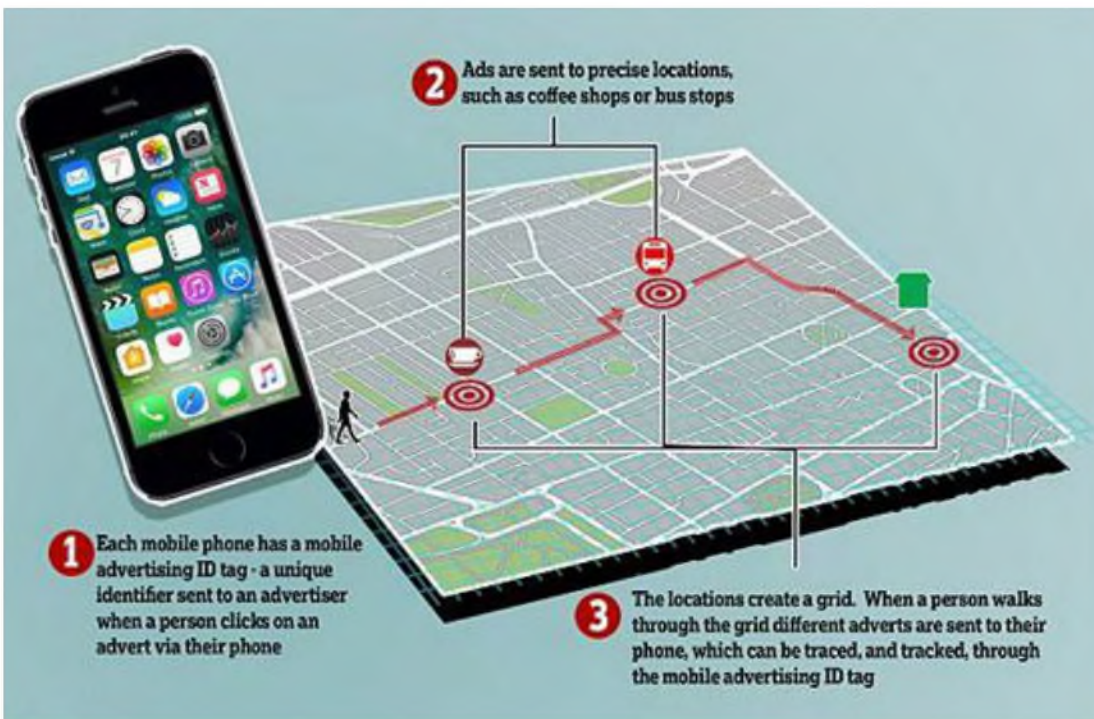
(b)(6) Office | (b)(6) Cell | (b)(6)

---

**From:** (b)(6)  
**Sent:** Friday, June 15, 2018 3:02 PM  
**To:** (b)(6)  
**Cc:** (b)(6)  
(b)(6)  
**Subject:** RE: Alexander Data

Hi (b)(6)

Here's a diagram that briefly describes how commercial app tracking works (borrowed from a British news site).



3<sup>rd</sup> party companies obtain the app advertiser data (made freely available by Apple and Google), “hash” the unique id, and then sell the data to anyone with a credit card.

See attached responses for additional details.

On related matters, Border Patrol reached out to S&T for assistance after the Border Patrol agent in Arizona was shot. Border Patrol wanted to know what other cell phones were in the vicinity of the shooting, using the VennTel tools described in the PTA.

To keep on top of this issue, I had the S&T team add to the Project Alexander PTA for this case. See other attachment. I also made it clear that Border Patrol had to obtain CBP legal and privacy guidance before using any of the data provided. To limit improper disclosure of ongoing investigative activities, the discussion added to the PTA has been kept at a very general level.

Summarizing the initial findings:

- 1) Most of the signals identified appear to be from other Border Patrol Agents – as the signals track back to CBP offices.
- 2) Some phones appear to be using “scramblers”, free apps that make your phone appear to be in 20 different locations the same time.
- 3) About 2-3 phones were identified near the vicinity of the shooting that didn’t track back to CBP offices or have scramblers.

S&T drafted a briefing on this 48 hour study that describes the scope and findings in detail. I believe a meeting to present the briefing is being scheduled for next week. I’ll make sure you get on the invite list.



Page 041

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 042

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 043

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 044

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 045

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 046

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 047

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 048

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 049

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 050

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 051

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 052

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 053

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 054

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 055

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 056

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 057

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 058

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

**From:** (b)(5)  
**To:** (b)(5)  
**Subject:** RE: Supreme Court case to weigh in on location data privacy  
**Date:** Friday, June 22, 2018 1:20:57 PM

---

Here are some interesting excerpts from the *Carpenter* case:

[https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf?mc\\_cid=6c060aef3d&mc\\_eid=96610f9b8a](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf?mc_cid=6c060aef3d&mc_eid=96610f9b8a)

- “Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.”
- “A majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which “hold for many Americans the ‘privacies of life,’ ” *Riley v. California*, contravenes that expectation. In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in *Jones*: They give the Government near perfect surveillance and allow it to travel back in time to retrace a person’s whereabouts...”

The *Carpenter* case focuses on cell-site records, which may end up influencing the legal opinion regarding Project GLASSDOOR.

The decision also cites cell location data dozens of times, which may influence the legal opinion on Project Alexander activities.

Paraphrasing an ACLU attorney, “I may have granted Starbucks and Apple permission to use my location data to get drink coupons. But I never authorized and Apple/Starbucks never told me that my location data would end up being used by 300 other third-parties and part of warrantless government searches.”

Add that to the public opinion on parent-child separations, triggering the doxxing of 9,000 current and former ICE employees ([The Person Doxxing ICE Employees Is A Professor At NYU](#)) and protestors outside of S1’s private residence ([Protesters blast sounds of crying children outside home of DHS chief](#)) – and you’ve got clear warning signs that DHS projects will be put under a lot more scrutiny going forward. What the public was willing to tolerate last year may not be true this year.

---

**From:** Lewis, Charles J. <cjlewis@mitre.org>  
**Sent:** Friday, June 22, 2018 11:42 AM  
**To:** Lee, Christopher <Christopher.Lee@HQ.DHS.GOV>; Dennis, Stephen

(b)(6)

**Subject:** Re: Supreme Court case to weigh in on location data privacy

Is there a difference between “cell tower location data” and app data that you “opt in too”?

(b)(6)

*Senior Principal Systems Engineer / Analytics & Big Data Outcome Leader*

*The MITRE Corporation*

*Homeland Security Systems Engineering & Development Institute (HS SEDI) FFRDC*

cell: (b)(6) | ph: (b)(6)

(b)(6)

---

**From:** (b)(6)

**Date:** Thursday, June 21, 2018 at 10:58 PM

(b)(6)

**Subject:** Supreme Court case to weigh in on location data privacy

### Supreme Court case to weigh in on location data privacy

A Fourth Amendment case, Carpenter vs. United States, currently being decided upon by the U.S. Supreme Court focuses on key digital privacy questions, and its decision has the potential to influence future location-tracking practices, Forbes reports. The case questions whether law enforcement’s warrantless access to seven months of cell tower location data, which was then used to study a defendant’s movements as part of a robbery investigation, is unconstitutional. While the government states the defendant had “no legitimate expectation of privacy,” the defense argues, that “cell phone location data does not necessarily involve any voluntary act on the part of users.” Privacy advocates have raised concern that if the decision rules in favor of government access to location data, citizens could be placed at greater risk for future surveillance by law enforcement.

[Full Story](#)

Page 061

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 062

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 063

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 064

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 065

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 066

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 067

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 068

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 069

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 070

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 071

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 072

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 073

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 074

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 075

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 076

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 077

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 078

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 079

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 080

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 081

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 082

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 083

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 084

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 085

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 086

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 087

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 088

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 089

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 090

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 091

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 092

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 093

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 094

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 095

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 096

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



**From:** (b)(6)  
**Sent:** 3 Jul 2019 15:22:47 +0000  
**To:** (b)(6)  
**Subject:** RE: POC for Ad ID Date and Carpenter Case  
**Attachments:** FW: Venntel/Project Alexander

Hi (b)(6)

S&T, CBP and ICE have been exploring the use of Advertising data for Homeland Security mission space. The data contains location information. DHS Privacy raised a question about whether the use of this data was ever analyzed against the Supreme Court *Carpenter* case that was issued in June 2018.

At this time, I am not aware of any analysis that exists within the Department.

Considering the number of components involved and the questions raised, I am working closely with S&T Privacy to determine what the components have in place, what analysis may have occurred, and what type of work is occurring at the component levels. S&T Privacy and I are also pulling together component privacy and legal POCs who would be involved in future discussions. We are planning to begin with an introduction of what this data is, how it is acquired and additional technical information that will provide a common foundation for an analysis on the legality of the Department utilizing this data.

Attached is an email that may provide more context.

If you still think you are the correct POCs for this matter, please let me know and I will add you to the list. The S&T Privacy office is already having discussions with ICE Privacy – (b)(6)

Have a wonderful Fourth!

Best,

(b)(6)

---

(b)(6)

Attorney - Technology Programs Law Division  
Office of the General Counsel  
Department of Homeland Security

(b)(6) (Office)  
(b)(6) (Cell)

(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged

**From:** (b)(6)  
**Sent:** 19 Jun 2019 16:24:20 +0000  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** FW: Venntel/Project Alexander  
**Attachments:** RE\_ Alexander Data.pdf, RE\_ Supreme Court case to weigh in on location data privacy.pdf  
**Importance:** High

(b)(6)

I hope this finds you well. Please take a look at the below email from HQ Privacy. I wanted to ping you as this legal analysis would have occurred before my time. Can you please confirm DATC legally acquired the Venntel data they have. I have attached the previous emails that Chris had sent to DATC on the risks of acquiring Venntel data.

They are asking if OGC conducted an analysis under the Carpenter case to ensure that we were able to legally acquire this data.

[https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf)

DATC is under heightened scrutiny as part of the Privacy Audit and HQ Privacy is digging deeper into what DATC is doing to ensure everything is being done properly.

Please advise if these issues were addressed and signed off on by OGC. Thank you for your time and review.

(b)(6)

---

(b)(6)  
Privacy Officer (Acting)  
Science and Technology Directorate  
Department of Homeland Security

(b)(6)

---

**From:** (b)(6)  
**Sent:** Wednesday, June 19, 2019 11:26 AM  
**To:** (b)(6)  
**Subject:** Venntel/Project Alexander

H (b)(6)

I understand that S&T has purchased information from Venntel as part of Project Alexander. The PTA was never approved because we had and continue to have significant concerns with this technology. Prior to receiving the information, did OGC conduct an analysis under the Carpenter case to ensure that we are able to legally acquire it?

Thanks,

(b)(6)

(b)(6)

Senior Director, Privacy Compliance

DHS Privacy Office

Desk (b)(6)

Cell:

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** RE: Alexander Data  
**Date:** Monday, June 25, 2018 4:09:05 PM  
**Attachments:** [PTA ST - DHS ST Alexander \(ICE IGP 05 11 2018\) - CSL responses 15 JUN 2....docx](#)  
[PTA ST - DHS ST Alexander CBP 6 14 18 - Border Patrol Incident PTA updat....docx](#)  
[image002.png](#)

---

Hi (b)(6)

I'm checking in to see what questions/comments you have on the PTA.

Is CBP legal drafting new guidance on location privacy in light of the *Carpenter* Supreme Court ruling last week? [https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf)

(b)(6)

(b)(6)

**Directorate Privacy Officer | Science & Technology Directorate | Department of Homeland Security**

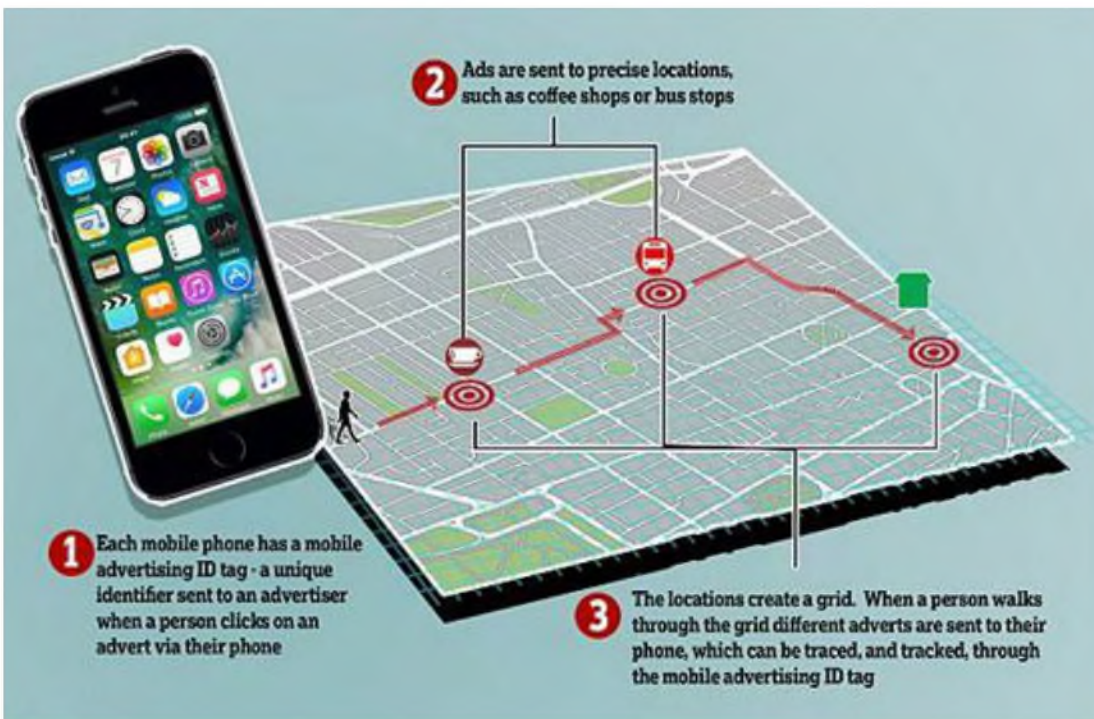
(b)(6) Office (b)(6) Cell (b)(6)

---

**From:** (b)(6)  
**Sent:** Friday, June 15, 2018 3:02 PM  
**To:** (b)(6)  
**Cc:** (b)(6)  
(b)(6)  
**Subject:** RE: Alexander Data

Hi (b)(6)

Here's a diagram that briefly describes how commercial app tracking works (borrowed from a British news site).



3<sup>rd</sup> party companies obtain the app advertiser data (made freely available by Apple and Google), “hash” the unique id, and then sell the data to anyone with a credit card.

See attached responses for additional details.

On related matters, Border Patrol reached out to S&T for assistance after the Border Patrol agent in Arizona was shot. Border Patrol wanted to know what other cell phones were in the vicinity of the shooting, using the VennTel tools described in the PTA.

To keep on top of this issue, I had the S&T team add to the Project Alexander PTA for this case. See other attachment. I also made it clear that Border Patrol had to obtain CBP legal and privacy guidance before using any of the data provided. To limit improper disclosure of ongoing investigative activities, the discussion added to the PTA has been kept at a very general level.

Summarizing the initial findings:

- 1) Most of the signals identified appear to be from other Border Patrol Agents – as the signals track back to CBP offices.
- 2) Some phones appear to be using “scramblers”, free apps that make your phone appear to be in 20 different locations the same time.
- 3) About 2-3 phones were identified near the vicinity of the shooting that didn’t track back to CBP offices or have scramblers.

S&T drafted a briefing on this 48 hour study that describes the scope and findings in detail. I believe a meeting to present the briefing is being scheduled for next week. I’ll make sure you get on the invite list.

Page 102

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 103

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 104

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 105

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 106

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 107

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 108

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 109

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 110

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 111

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 112

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 113

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 114

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 115

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 116

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 117

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 118

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 119

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

**From:** (b)(6)  
**To:** [Redacted]  
**Subject:** RE: Supreme Court case to weigh in on location data privacy  
**Date:** Friday, June 22, 2018 1:20:57 PM

---

Here are some interesting excerpts from the *Carpenter* case:  
[https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf?mc\\_cid=6c060aef3d&mc\\_eid=96610f9b8a](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf?mc_cid=6c060aef3d&mc_eid=96610f9b8a)

- “Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.”
- “A majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which “hold for many Americans the ‘privacies of life,’ ” *Riley v. California*, contravenes that expectation. In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in *Jones*: They give the Government near perfect surveillance and allow it to travel back in time to retrace a person’s whereabouts...”

The *Carpenter* case focuses on cell-site records, (b)(5) [Redacted]  
(b)(5) [Redacted]

The decision also cites cell location data dozens of times, (b)(5) [Redacted]  
(b)(5) [Redacted]

Paraphrasing an ACLU attorney, “I may have granted Starbucks and Apple permission to use my location data to get drink coupons. But I never authorized and Apple/Starbucks never told me that my location data would end up being used by 300 other third-parties and part of warrantless government searches.”

(b)(5) [Redacted]

---

**From:** (b)(6) [Redacted]  
**Sent:** Friday, June 22, 2018 11:42 AM  
**To:** (b)(6) [Redacted]



(b)(6)

**Subject:** Re: Supreme Court case to weigh in on location data privacy

Is there a difference between “cell tower location data” and app data that you “opt in too”?

(b)(6)

*Senior Principal Systems Engineer / Analytics & Big Data Outcome Leader*

*The MITRE Corporation*

*Homeland Security Systems Engineering & Development Institute (HS SEDI) FFRDC*

cell: (b)(6) | ph: (b)(6)

(b)(6)

---

**From:** (b)(6)

**Date:** Thursday, June 21, 2018 at 10:58 PM

(b)(6)

**Subject:** Supreme Court case to weigh in on location data privacy

### Supreme Court case to weigh in on location data privacy

A Fourth Amendment case, Carpenter vs. United States, currently being decided upon by the U.S. Supreme Court focuses on key digital privacy questions, and its decision has the potential to influence future location-tracking practices, Forbes reports. The case questions whether law enforcement’s warrantless access to seven months of cell tower location data, which was then used to study a defendant’s movements as part of a robbery investigation, is unconstitutional. While the government states the defendant had “no legitimate expectation of privacy,” the defense argues, that “cell phone location data does not necessarily involve any voluntary act on the part of users.” Privacy advocates have raised concern that if the decision rules in favor of government access to location data, citizens could be placed at greater risk for future surveillance by law enforcement.

[Full Story](#)

Page 122

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 123

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 124

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 125

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 126

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 127

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 128

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 129

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 130

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 131

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 132

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 133

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 134

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 135

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 136

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 137

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 138

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 139

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 140

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 141

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 142

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 143

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 144

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 145

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 146

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 147

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 148

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 149

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 150

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 151

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 152

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 153

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 154

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 155

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 156

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 157

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

**From:** (b)(6)  
**Sent:** 27 Dec 2017 20:35:04 +0000  
**To:** (b)(6)  
**Subject:** FW: List of Technologies

(b)(6) - (b)(6) and I are working together to evaluate the types of technologies he wants to work with in calendar year 2018. In the email below he provided the first tranche of technologies that he is looking into to conduct T&E. I'm not sure what type of legal product I will provide (b)(6) but I'm working on evaluating (b)(5). Each of the technologies is connected with a DHS component/private sector operational partner. I've already given (b)(6) a heads up that I want to talk through some of the issues I may identify for OELD input.

When you are back in the office, I'll provide an update on where I am with this project.

Best,

(b)(6)

---

(b)(6)  
Attorney - Technology Programs Law Division  
Office of the General Counsel  
Department of Homeland Security  
(b)(6) (Office)  
(b)(6) (Cell)  
(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

---

**From:** (b)(6)  
**Sent:** Friday, December 22, 2017 3:35 PM  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** RE: List of Technologies

~~FOR OFFICIAL USE ONLY//LAW ENFORCEMENT SENSITIVE~~  
Pre-decisional information

(b)(6)

I greatly appreciate your expertise and help with legal analysis around these technologies. We are looking forward to examining the technical capabilities that DHS might bring to bear to improve

Homeland Security, either directly, and/or with our partners in the Homeland Security Enterprise. Let me know if you have any questions regarding these technologies and associated use cases.

Best regards,

(b)(6)

(b)(5)

[Redacted content]

---

**From:** (b)(6)

**Sent:** Wednesday, December 13, 2017 5:43 PM

**To:** (b)(6)

**Cc:** (b)(6)

**Subject:** List of Technologies

Hi (b)(6)

Is there something that you guys have internally regarding the technologies that you are working with?

I'm mostly interested in the cell site simulator, cell phone history technologies, commercial cell/app data services, and social media tools that the group is working with. I am also interested in the technologies that you all may be scoping for the NBA All-Stars.

(b)(5)

A list of those technologies, some brief discussion about what they do and some conceptual use cases would be helpful.

Best,

(b)(6)

(b)(6)

Attorney - Technology Programs Law Division  
Office of the General Counsel  
Department of Homeland Security

(b)(6)

(Office)

(Cell)

(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.



**From:** (b)(6)  
**Sent:** 12 Apr 2018 16:09:28 +0000  
**To:** (b)(6)  
**Subject:** RE: Quick White List Experiment

(b)(5)

---

(b)(6)  
Attorney - Technology Programs Law Division  
Office of the General Counsel  
Department of Homeland Security  
(b)(6) (Office)  
(b)(6) (Cell)  
(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

---

**From:** (b)(6)  
**Sent:** Thursday, April 12, 2018 11:56 AM  
**To:** Patel, Minal <Minal.Patel@HQ.DHS.GOV>; Lee, Christopher <Christopher.Lee@HQ.DHS.GOV>  
**Subject:** Quick White List Experiment

(b)(6)  
We would like to send one of our program burner phones, that will use a wireless satellite connection, on a ship with (b)(6) a witting S&T federal employee, during an exercise being run by JIATF-S. We would like to look for this device later in Venntel. Any issues with this?

(b)(6)

**From:** (b)(6)  
**Sent:** 20 Jun 2019 14:18:42 +0000  
**To:** (b)(6)  
**Subject:** FW: Venntel/Project Alexander  
**Attachments:** RE\_ Alexander Data.pdf, RE\_ Supreme Court case to weigh in on location data privacy.pdf  
**Importance:** High

Good Morning (b)(6)  
I work under (b)(6) and support the Science and Technology Directorate (S&T).

(b)(5)

I'm trying to pull together appropriate HQ attorneys and component attorneys (CBP/ICE). (b)(6) (b)(6) in our S&T Privacy office is similarly pulling together the appropriate Privacy folks to provide formal guidance on if DHS can use such data legally, and if so, how that data can be used by the Department.

(b)(6) recommended that I start with you to discuss this matter. Do you have some time today to discuss? If not today, are you available on Monday to set aside a half hour to discuss?

Best,  
(b)(6)

(b)(6)  
\_\_\_\_\_  
Attorney - Technology Programs Law Division  
Office of the General Counsel  
Department of Homeland Security  
(b)(6) (Office)  
(b)(6) (Cell)

(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message.

Thank you.

---

**From:** (b)(6)  
**Sent:** Wednesday, June 19, 2019 12:24 PM  
**To:** (b)(6)

**Cc:** (b)(6)

(b)(6)

**Subject:** FW: Venntel/Project Alexander

**Importance:** High

(b)(6)

I hope this finds you well. Please take a look at the below email from HQ Privacy. I wanted to ping you as this legal analysis would have occurred before my time. Can you please confirm DATC legally acquired the Venntel data they have. I have attached the previous emails that (b)(6) had sent to DATC on the risks of acquiring Venntel data.

They are asking if OGC conducted an analysis under the Carpenter case to ensure that we were able to legally acquire this data.

[https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf)

DATC is under heightened scrutiny as part of the Privacy Audit and HQ Privacy is digging deeper into what DATC is doing to ensure everything is being done properly.

Please advise if these issues were addressed and signed off on by OGC. Thank you for your time and review.

(b)(6)

---

(b)(6)

Privacy Officer (Acting)  
Science and Technology Directorate  
Department of Homeland Security

(b)(6)

---

**From:** (b)(6)

**Sent:** Wednesday, June 19, 2019 11:26 AM

**To:** (b)(6)

**Subject:** Venntel/Project Alexander

Hi (b)(6)

I understand that S&T has purchased information from Venntel as part of Project Alexander. The PTA was never approved because we had and continue to have significant concerns with this technology. Prior to receiving the information, did OGC conduct an analysis under the Carpenter case to ensure that we are able to legally acquire it?

Thanks.

(b)(6)

Senior Director, Privacy Compliance  
DHS Privacy Office

Desk: (b)(6)

Cell: (b)(6)

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** RE: Alexander Data  
**Date:** Monday, June 25, 2018 4:09:05 PM  
**Attachments:** [PTA ST - DHS ST Alexander \(ICE IGP 05 11 2018\) - CSL responses 15 JUN 2....docx](#)  
[PTA ST - DHS ST Alexander CBP 6 14 18 - Border Patrol Incident PTA updat....docx](#)  
[image002.png](#)

---

Hi (b)(6)

I'm checking in to see what questions/comments you have on the PTA.

Is CBP legal drafting new guidance on location privacy in light of the *Carpenter* Supreme Court ruling last week? [https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf)

(b)(6)

(b)(6)

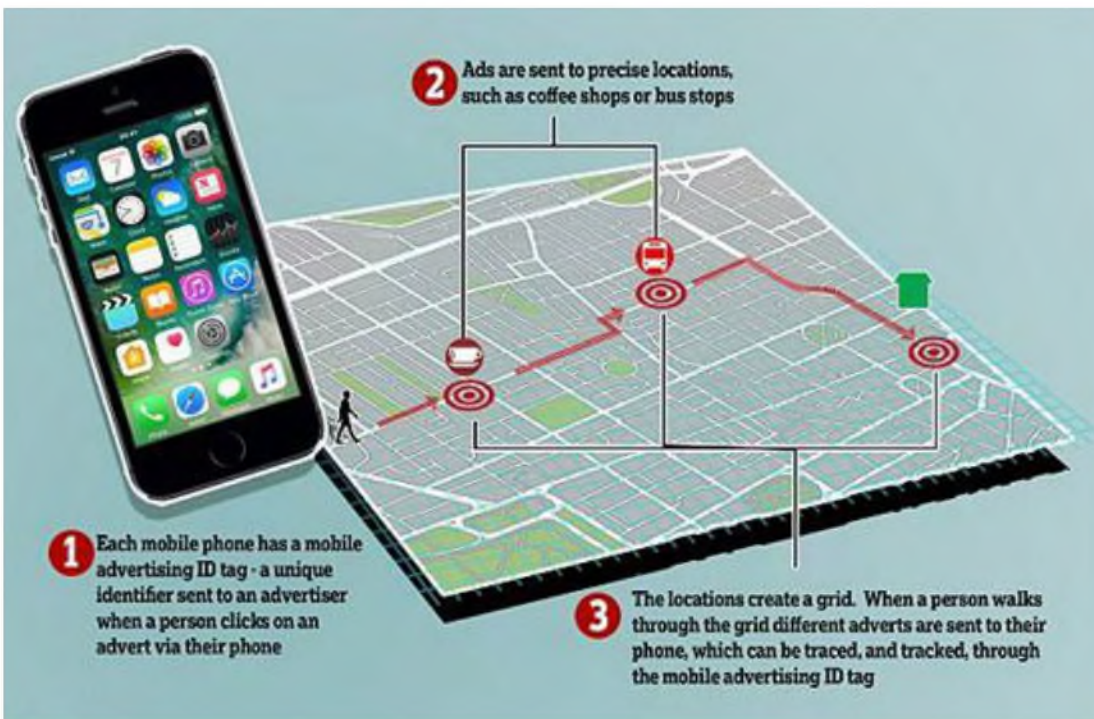
**Directorate Privacy Officer | Science & Technology Directorate | Department of Homeland Security**  
(b)(6) Office (b)(6) Cell (b)(6)

---

**From:** (b)(6)  
**Sent:** Friday, June 15, 2018 3:02 PM  
**To:** (b)(6)  
**Cc:** (b)(6)  
(b)(6)  
**Subject:** RE: Alexander Data

Hi (b)(6)

Here's a diagram that briefly describes how commercial app tracking works (borrowed from a British news site).



3<sup>rd</sup> party companies obtain the app advertiser data (made freely available by Apple and Google), “hash” the unique id, and then sell the data to anyone with a credit card.

See attached responses for additional details.

On related matters, Border Patrol reached out to S&T for assistance after the Border Patrol agent in Arizona was shot. Border Patrol wanted to know what other cell phones were in the vicinity of the shooting, using the VennTel tools described in the PTA.

To keep on top of this issue, I had the S&T team add to the Project Alexander PTA for this case. See other attachment. I also made it clear that Border Patrol had to obtain CBP legal and privacy guidance before using any of the data provided. To limit improper disclosure of ongoing investigative activities, the discussion added to the PTA has been kept at a very general level.

Summarizing the initial findings:

- 1) Most of the signals identified appear to be from other Border Patrol Agents – as the signals track back to CBP offices.
- 2) Some phones appear to be using “scramblers”, free apps that make your phone appear to be in 20 different locations the same time.
- 3) About 2-3 phones were identified near the vicinity of the shooting that didn’t track back to CBP offices or have scramblers.

S&T drafted a briefing on this 48 hour study that describes the scope and findings in detail. I believe a meeting to present the briefing is being scheduled for next week. I’ll make sure you get on the invite list.

Page 166

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 167

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 168

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 169

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 170

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 171

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 172

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 173

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 174

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 175

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 176

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 177

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 178

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 179

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 180

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 181

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 182

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 183

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

**From:** (b)(6)  
**To:** (b)(6)  
**Subject:** RE: Supreme Court case to weigh in on location data privacy  
**Date:** Friday, June 22, 2018 1:20:57 PM

---

Here are some interesting excerpts from the *Carpenter* case:  
[https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf?mc\\_cid=6c060aef3d&mc\\_eid=96610f9b8a](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf?mc_cid=6c060aef3d&mc_eid=96610f9b8a)

- “Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.”
- “A majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which “hold for many Americans the ‘privacies of life,’ ” *Riley v. California*, contravenes that expectation. In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in *Jones*: They give the Government near perfect surveillance and allow it to travel back in time to retrace a person’s whereabouts...”

The *Carpenter* case focuses on cell-site records, (b)(5)  
(b)(5)

The decision also cites cell location data dozens of times, (b)(5)  
(b)(5)

Paraphrasing an ACLU attorney, “I may have granted Starbucks and Apple permission to use my location data to get drink coupons. But I never authorized and Apple/Starbucks never told me that my location data would end up being used by 300 other third-parties and part of warrantless government searches.”

Add that to the public opinion on parent-child separations, triggering the doxxing of 9,000 current and former ICE employees ([The Person Doxxing ICE Employees Is A Professor At NYU](#)) and protestors outside of S1’s private residence ([Protesters blast sounds of crying children outside home of DHS chief](#)) – and you’ve got clear warning signs that DHS projects will be put under a lot more scrutiny going forward. What the public was willing to tolerate last year may not be true this year.

---

**From:** (b)(6)  
**Sent:** Friday, June 22, 2018 11:42 AM  
**To:** (b)(6)



(b)(6)

**Subject:** Re: Supreme Court case to weigh in on location data privacy

Is there a difference between “cell tower location data” and app data that you “opt in too”?

(b)(6)

*Senior Principal Systems Engineer / Analytics & Big Data Outcome Leader  
The MITRE Corporation  
Homeland Security Systems Engineering & Development Institute (HS SEDI) FFRDC*

cell: (b)(6) ph: (b)(6)

(b)(6)

---

**From:** (b)(6)

**Date:** Thursday, June 21, 2018 at 10:58 PM

**To:** (b)(6)

(b)(6)

(b)(6)

(b)(6)

(b)(6)

**Subject:** Supreme Court case to weigh in on location data privacy

### Supreme Court case to weigh in on location data privacy

A Fourth Amendment case, Carpenter vs. United States, currently being decided upon by the U.S. Supreme Court focuses on key digital privacy questions, and its decision has the potential to influence future location-tracking practices, Forbes reports. The case questions whether law enforcement’s warrantless access to seven months of cell tower location data, which was then used to study a defendant’s movements as part of a robbery investigation, is unconstitutional. While the government states the defendant had “no legitimate expectation of privacy,” the defense argues, that “cell phone location data does not necessarily involve any voluntary act on the part of users.” Privacy advocates have raised concern that if the decision rules in favor of government access to location data, citizens could be placed at greater risk for future surveillance by law enforcement.

[Full Story](#)

Page 186

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 187

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 188

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 189

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 190

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 191

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 192

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 193

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 194

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 195

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 196

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 197

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 198

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 199

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 200

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 201

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 202

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 203

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 204

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 205

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 206

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 207

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:** (b)(6)  
**Subject:** FOR DHS CLEARANCE: Contract Awards to Venntel  
**Date:** Thursday, September 10, 2020 10:50:00 AM  
**Attachments:** [CBP OPO Contracts with Venntel Response 9.9.2020.docx](#)  
[RE Requests to vendors for information on use of DHS tools.msg](#)  
[Requests to vendors for information on use of DHS tools.msg](#)

---

Good Morning,

Attached for clearance is the DHS OCPO response to the HAC-HS inquiry asking the Department to identify any contracts awarded to Venntel, who is believed to collect location data from smart phones and sell it to clients. Congress has been looking into this on the basis of privacy concerns. .

Also, for your awareness, the SAC-HS Majority Clerk reached out to (b)(6), Budget Director, informing her that Senator Wyden (D-OR) sent a letter directly to Venntel for information instead of working through the Department. Please see the attached emails.

Clearance is requested from PLCY, OLA, and OGC Oversight. Please provide comments or edits **NLT 10:00 AM tomorrow, September 11, 2020.**

If you have any questions, please let me know.

V/r,

(b)(6)

(b)(6)

Deputy Assistant Director, Budget Division  
Office of the Chief Financial Officer  
U.S. Department of Homeland Security

Office: (b)(6)

Cell: (b)(6)

(b)(6)



**From:** Babb, Peter (Appropriations)  
**Sent:** 25 Aug 2020 20:08:18 +0000  
**To:** (b)(6)  
**Cc:** Harper, Justin (Appropriations); White, Kamela (Appropriations)  
**Subject:** RE: Requests to vendors for information on use of DHS tools

Were Policy and other relevant folks aware of this? There was some press on this today related to a CBP contract:

<https://www.businessinsider.com/cbp-venntel-contract-phone-location-data-2020-8>

---

**From:** Babb, Peter (Appropriations)  
**Sent:** Friday, July 31, 2020 1:01 PM  
**To:** (b)(6)  
**Cc:** Harper, Justin (Appropriations); (b)(6); White, Kamela (Appropriations); (b)(6)  
**Subject:** Requests to vendors for information on use of DHS tools

Good day,

I just wanted you to be aware that Senator Wyden's staff has requested all correspondence from CBP/ICE from a couple vendors (Venntel, Babel Street) on some products/services DHS purchases, and wanted you to be aware of the potential sharing of this information. I would guess that Senator Wyden is requesting information from vendors, rather than from DHS for reasons of expedience.

I have known of one of the product's uses for years, and know that DHS uses some of the described data to help keep the homeland safe. Senator Wyden's staff indicated to others in industry that are some more "big articles" coming out soon and they are calling more companies for information and will possibly send letters. Attached is a letter from the House Oversight Committee and below are two related articles. There's a lot going on with civil liberties (in line with the email from Scott/me earlier today). I don't have a real ask here, other than making sure that folks in Policy and elsewhere are aware of these requests, as if these tools are critical for legitimate law enforcement purposes, it probably makes sense for DHS to present a united front in responding to these inquiries and justifying the use of these tools.

Thanks,  
Peter

[Academic Project Used Marketing Data to Monitor Russian Military Sites](#)

And

[House Investigating Company Selling Phone Location Data to Government Agencies](#)

**From:** Babb, Peter (Appropriations)  
**Sent:** 31 Jul 2020 17:01:04 +0000  
**To:** Mehringer, Holly  
**Cc:** Harper, Justin (Appropriations); White, Kamela (Appropriations)  
**Subject:** Requests to vendors for information on use of DHS tools  
**Attachments:** House Oversight, Wyden, Venntel letter.pdf

Good day,

I just wanted you to be aware that Senator Wyden's staff has requested all correspondence from CBP/ICE from a couple vendors (Venntel, Babel Street) on some products/services DHS purchases, and wanted you to be aware of the potential sharing of this information. I would guess that Senator Wyden is requesting information from vendors, rather than from DHS for reasons of expedience.

I have known of one of the product's uses for years, and know that DHS uses some of the described data to help keep the homeland safe. Senator Wyden's staff indicated to others in industry that are some more "big articles" coming out soon and they are calling more companies for information and will possibly send letters. Attached is a letter from the House Oversight Committee and below are two related articles. There's a lot going on with civil liberties (in line with the email from Scott/me earlier today). I don't have a real ask here, other than making sure that folks in Policy and elsewhere are aware of these requests, as if these tools are critical for legitimate law enforcement purposes, it probably makes sense for DHS to present a united front in responding to these inquiries and justifying the use of these tools.

Thanks,  
Peter

[Academic Project Used Marketing Data to Monitor Russian Military Sites](#)

And

[House Investigating Company Selling Phone Location Data to Government Agencies](#)

**Congress of the United States**  
**Washington, DC 20515**

June 24, 2020

Mr. Chris Gildea  
President  
Venntel, Inc.  
2201 Cooperative Way, Suite 600  
Herndon, VA 20171

Dear Mr. Gildea:

We are investigating the collection and sale of sensitive mobile phone location data that reveals the precise movements of millions of American adults, teens, and even children. We seek information about your company's provision of consumer location data to federal government agencies for law enforcement purposes without a warrant and for any other purposes, including in connection with the response to the coronavirus crisis.

The vast majority of Americans carry cell phones with apps capable of collecting precise location information 24 hours a day, 7 days a week. This location-tracking raises serious privacy and security concerns. As Chief Judge Roberts wrote in the *Carpenter* opinion, "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."<sup>1</sup> This location data can reveal where we go and with whom we associate, tracking us in our homes, at the doctor, or at church.<sup>2</sup>

With Americans installing contact-tracing apps as part of the effort to limit the spread of COVID-19, it has become increasingly important to make sure that the American public has a full understanding of who is collecting their location data, how it may be provided to the government, and what the government is doing with it.

It was recently reported that a contact-tracing app recommended to residents by the governors of North Dakota and South Dakota was sending location data to a third party—in violation of promises made to users.<sup>3</sup> According to that third party, the data was not used; nevertheless, this example shows that Americans may increasingly be unwittingly handing over their location data to unknown third party data brokers such as Venntel. There are limited restrictions on how this data may be sold to and used by the federal government.

---

<sup>1</sup> *Carpenter v. United States*, 138 S.Ct. 2206 (2018).

<sup>2</sup> *The Government Uses 'Near Perfect Surveillance' Data on Americans*, New York Times (Feb. 7, 2020) (online at [www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html](http://www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html)).

<sup>3</sup> *One of the First Contact-Tracing Apps Violates Its Own Privacy Policy*, Washington Post (May 21, 2020) (online at [www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/](http://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/)).

In February, the Wall Street Journal reported that Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) purchased consumers' location data from Venntel and used it without a warrant to identify, locate, and arrest migrants.<sup>4</sup> According to the report:

The Trump administration 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. ... The location data is drawn from ordinary cellphone apps, including those for games, weather and e-commerce, for which the user has granted permission to log the phone's location.<sup>5</sup>

Federal spending records indicate that the Drug Enforcement Agency (DEA), Federal Bureau of Investigation (FBI), and Internal Revenue Service (IRS) also may have obtained data or data services from your company.<sup>6</sup> Furthermore, federal, state, and local governments reportedly are using or considering the use of cell phone location data to track the spread of the coronavirus.<sup>7</sup>

The Supreme Court has held that the government must obtain a warrant before agencies can obtain location data from wireless phone companies and technology companies like Facebook and Google. By acting as an intermediary in the sale of this data, your company may be selling data to the government that it otherwise would need a warrant to compel, impacting the privacy of millions of people, including vulnerable populations like children.<sup>8</sup>

Consumers often do not understand that popular apps for weather, travel, shopping, and other purposes—which may have legitimate needs for location data—may be selling this data to brokers.<sup>9</sup> An investigation in 2018 by the New York Times uncovered 75 companies that were

---

<sup>4</sup> *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall Street Journal (Feb. 7, 2020) (online at [www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600](http://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600)).

<sup>5</sup> *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall Street Journal (Feb. 7, 2020) (online at [www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600](http://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600)).

<sup>6</sup> *USASpending.gov* (accessed June 22, 2020).

<sup>7</sup> *U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus*, Washington Post (Mar. 17, 2020) (online at [www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/](http://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/)); *Government Tracking How People Move Around in Coronavirus Pandemic*, Wall Street Journal (Mar. 28, 2020) (online at [www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202](http://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202));

<sup>8</sup> See 18 U.S.C. § 2702.

<sup>9</sup> *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, New York Times (June 12, 2019) (online at [www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html](http://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html)); Federal Trade Commission, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers* (Dec. 5, 2013) (online at [www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived](http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived)).

buying and selling mobile app-derived location data.<sup>10</sup> Location-targeted advertising sales are predicted to reach an estimated \$27 billion this year.<sup>11</sup>

The scale of this data collection is staggering. For example, Venntel's reported parent company, Gravy Analytics,<sup>12</sup> has revealed that it collects location data from software "embedded within tens of thousands of apps."<sup>13</sup> According to its website, Gravy Analytics "processes billions of pseudonymous mobile location signals every day from millions of mobile devices."<sup>14</sup> Despite claims that anonymization protects privacy, computer scientists and journalists repeatedly have demonstrated the ease with which individuals in purportedly anonymized data sets may be identified.<sup>15</sup>

Reports also indicate that location data is vulnerable to hacking and that this data could lead to individuals being targeted for commercial or political purposes, stalking, or discrimination.<sup>16</sup> In 2017, the Massachusetts Attorney General reached a settlement with a company that targeted advertisements to "abortion-minded women" entering reproductive health facilities and methadone clinics in multiple states.<sup>17</sup> Media reports have also identified companies targeting advertisements to people in emergency rooms<sup>18</sup> and dialysis centers.<sup>19</sup> In

---

<sup>10</sup> *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, New York Times (Dec. 10, 2018) (online at [www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html](http://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html)).

<sup>11</sup> *Location Targeted Mobile Advertising Spending in the United States from 2016 to 2023*, Statista (Nov. 8, 2019) (online at [www.statista.com/statistics/274837/local-and-national-mobile-us-ad-spending-since-2009/](http://www.statista.com/statistics/274837/local-and-national-mobile-us-ad-spending-since-2009/)).

<sup>12</sup> *Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones*, Protocol (Mar. 5, 2020) (online at [www.protocol.com/government-buying-location-data](http://www.protocol.com/government-buying-location-data)).

<sup>13</sup> Gravy Analytics, *Location Data & COVID-19* (online at [gravyanalytics.com/covid-19/](http://gravyanalytics.com/covid-19/)) (accessed June 22, 2020).

<sup>14</sup> Gravy Analytics, *Our Data* (online at [gravyanalytics.com/our-data/](http://gravyanalytics.com/our-data/)) (accessed June 22, 2020).

<sup>15</sup> *Twelve Million Phones, One Dataset, Zero Privacy*, New York Times (Dec. 19, 2019) (online at [www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html](http://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html)).

<sup>16</sup> *A Location-Sharing Disaster Shows How Exposed You Really Are*, Wired (May 19, 2018) (online at [www.wired.com/story/locationsmart-securus-location-data-privacy/](http://www.wired.com/story/locationsmart-securus-location-data-privacy/)); *Hundreds of Apps Can Empower Stalkers to Track Their Victims*, New York Times (May 19, 2018) (online at [www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html](http://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html)); *Catholics in Iowa Went to Church. Steve Bannon Tracked Their Phones*, ThinkProgress (July 19, 2019) (online at <https://thinkprogress.org/exclusive-steve-bannon-geofencing-data-collection-catholic-church-4aaeacd5c182/>); Senate Committee on Commerce, Science, and Transportation, Ranking Member Maria Cantwell, *The State of Online Privacy and Data Security* (Nov. 2019) (online at [www.cantwell.senate.gov/imo/media/doc/The%20State%20of%20Online%20Privacy%20and%20Data%20Security.pdf](http://www.cantwell.senate.gov/imo/media/doc/The%20State%20of%20Online%20Privacy%20and%20Data%20Security.pdf)).

<sup>17</sup> *Firm Settles Massachusetts Probe over Anti-abortion Ads Sent to Phones*, Reuters (Apr. 4, 2017) (online at [www.reuters.com/article/us-massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSKBN1761PX](http://www.reuters.com/article/us-massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSKBN1761PX)).

<sup>18</sup> *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, New York Times (Dec. 10, 2018) (online at [www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html](http://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html)).

<sup>19</sup> *Political Campaigns Know Where You've Been. They're Tracking Your Phone*, Wall Street Journal (Oct. 10, 2019) (online at [www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889](http://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889)).

2019, the Los Angeles City Attorney brought a lawsuit against the Weather Channel and its parent company, IBM, which sell data collected from the Weather Channel app's 45 million users. The City Attorney alleged the companies deceptively collected, shared, and profited from the location information of millions of American consumers.<sup>20</sup>

In February 2020, the Federal Communications Commission (FCC) fined the four major wireless carriers, Verizon, AT&T, T-Mobile, and Sprint, for selling location data without the knowledge or consent of their subscribers. In issuing the fines, the FCC described the sensitivity of location data and its potential for abuse:

The precise physical location of a wireless device is an effective proxy for the precise physical location of the person to whom that phone belongs at that moment in time. Exposure of this kind of deeply personal information puts those individuals at significant risk of harm—physical, economic, or psychological. For consumers who have job responsibilities in our country's military, government, or intelligence services, exposure of this kind of information can have serious national security implications.<sup>21</sup>

For all of these reasons, please provide the following information and documents by July 8, 2020, for the period from January 1, 2016, to the present:

1. For each provision of goods or services to a federal agency by your company:
  - a. documents sufficient to show the nature and purpose of the product or service provided and any use case or justification provided by the purchasing agency;
  - b. documents sufficient to show any actions that Venntel or its suppliers take to obtain the consent of the individuals whose location and other data is provided to or accessed by the agency;
  - c. all documents relating to any restrictions on how the agency may use the product or service, including whether the agency may share information with other federal or state government agencies and whether Venntel and the agency entered into a nondisclosure agreement regarding the agency's use of Venntel's services;
  - d. documents sufficient to show Venntel's revenue from the sale or provision of the goods or services;
  - e. copies of all contracts or agreements relating to the sale or provision of the goods or services;
2. All correspondence between Venntel and any employee, official, or representative of any federal department, federal agency, or executive branch office;

---

<sup>20</sup> *Los Angeles Accuses Weather Channel App of Covertly Mining User Data*, New York Times (Jan. 3, 2019) (online at [www.nytimes.com/2019/01/03/technology/weather-channel-app-lawsuit.html](http://www.nytimes.com/2019/01/03/technology/weather-channel-app-lawsuit.html)).

<sup>21</sup> *See, e.g.*, Federal Communications Commission, *Notice of Apparent Liability for Forfeiture and Admonishment*, T-Mobile (Feb. 28, 2020) (online at <https://docs.fcc.gov/public/attachments/FCC-20-27A1.pdf>).

3. A list of all customers who purchase, license, or access location data from Venntel or any Venntel subsidiary. For each customer, please provide the following:
  - a. documents sufficient to show the nature and purpose of the product or service provided;
  - b. documents sufficient to show any actions that Venntel or its suppliers take to obtain the consent of the individuals whose location and other data is provided to or accessed by the customer;
  - c. all documents relating to any restrictions on how the customer may use the product or service;
  - d. copies of all contracts or agreements relating to the sale or provision of the goods or services;
  - e. for any foreign entity, detail the steps Venntel has taken to seek and obtain export licenses for these sales;
4. A description of any COVID-19 related efforts that Venntel is involved in, including:
  - a. any COVID-19-related apps from which Venntel collects or has collected data;
  - b. any documents related to the provision of goods or services to federal agencies, state governments, local law enforcement, and foreign entities, related to monitoring or mitigating the COVID-19 pandemic; and
5. Documents sufficient to show the specific location data that Venntel collects, other information it collects (*e.g.*, Advertising ID, wireless information, web search history, phone or demographic information), and how is it paired or combined with location data;
6. Documents sufficient to show the number of individuals from whom Venntel collects location data;
7. Information indicating how long Venntel keeps user data, regardless of whether it is anonymized;
8. Documents sufficient to identify all sources from which Venntel and its upstream suppliers have received consumer location and other data which it provides to any government agency, and the specific type of data collected from each source. For each source, please provide documents sufficient to show the following:
  - a. the amount paid by Venntel to receive location data from that source;
  - b. copies of all contracts or written agreements with that source;
9. Documents sufficient to show all measures Venntel or its upstream suppliers take, if any, to ensure the anonymity of users whose data is collected by Venntel;

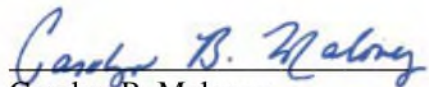
10. Documents sufficient to show all steps Venntel takes, contractually or otherwise, to ensure that its customers do not attempt to re-identify anonymized data provided to them;
11. A description of how Venntel ensures that all data it buys and sells, licenses, or provides access to was obtained from individuals who consented to the collection of, use of, sale of, or sale of access to their data, including to federal agencies and law enforcement agencies;
12. A description of any data security practices and policies Venntel uses to ensure that location data is not accessed without authorization;
13. A description of each instance in which Venntel's location data has been breached or accessed without authorization; and
14. Copies of all policies and procedures related to the collection, use, license, or sale of location data, including with respect to data security, data privacy, user consent, and anonymization.

The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

An attachment to this letter provides additional instructions for responding to this request. If you have any questions regarding this request, please contact Committee staff at (202) 225-5051, Senator Warren's staff at (202) 224-4543, or Senator Wyden's staff at (202) 224-5244.

Thank you for your attention to this important matter.

Sincerely,



Carolyn B. Maloney  
Chairwoman  
House Committee on Oversight and Reform



Elizabeth Warren  
United States Senator



Ron Wyden  
United States Senator



Mark DeSaulnier  
Member of Congress

Enclosure

cc: The Honorable Jim Jordan, Ranking Member,



Mr. Chris Gildea  
Page 7

House Committee on Oversight and Reform

## Responding to Oversight Committee Document Requests

1. In complying with this request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. Produce all documents that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party.
2. Requested documents, and all documents reasonably related to the requested documents, should not be destroyed, altered, removed, transferred, or otherwise made inaccessible to the Committee.
3. In the event that any entity, organization, or individual denoted in this request is or has been known by any name other than that herein denoted, the request shall be read also to include that alternative identification.
4. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, thumb drive, or secure file transfer) in lieu of paper productions.
5. Documents produced in electronic format should be organized, identified, and indexed electronically.
6. Electronic document productions should be prepared according to the following standards:
  - a. The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
  - b. Document numbers in the load file should match document Bates numbers and TIF file names.
  - c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
  - d. All electronic documents produced to the Committee should include the following fields of metadata specific to each document, and no modifications should be made to the original metadata:  
  
BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,

INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,  
BEGATTACH.

7. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, zip file, box, or folder is produced, each should contain an index describing its contents.
8. Documents produced in response to this request shall be produced together with copies of file labels, dividers, or identifying markers with which they were associated when the request was served.
9. When you produce documents, you should identify the paragraph(s) or request(s) in the Committee's letter to which the documents respond.
10. The fact that any other person or entity also possesses non-identical or identical copies of the same documents shall not be a basis to withhold any information.
11. The pendency of or potential for litigation shall not be a basis to withhold any information.
12. In accordance with 5 U.S.C. § 552(d), the Freedom of Information Act (FOIA) and any statutory exemptions to FOIA shall not be a basis for withholding any information.
13. Pursuant to 5 U.S.C. § 552a(b)(9), the Privacy Act shall not be a basis for withholding information.
14. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
15. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) every privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, addressee, and any other recipient(s); (e) the relationship of the author and addressee to each other; and (f) the basis for the privilege(s) asserted.
16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (by date, author, subject, and recipients), and explain the circumstances under which the document ceased to be in your possession, custody, or control.
17. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents that would be responsive as if the date or other descriptive detail were correct.

18. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data, or information not produced because it has not been located or discovered by the return date shall be produced immediately upon subsequent location or discovery.
19. All documents shall be Bates-stamped sequentially and produced sequentially.
20. Two sets of each production shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2105 of the Rayburn House Office Building.
21. Upon completion of the production, submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control that reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

### **Definitions**

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, data, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, communications, electronic mail (email), contracts, cables, notations of any type of conversation, telephone call, meeting or other inter-office or intra-office communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, mail, releases, electronic

message including email (desktop or mobile device), text message, instant message, MMS or SMS message, message application, or otherwise.

3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information that might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neutral genders.
4. The term “including” shall be construed broadly to mean “including, but not limited to.”
5. The term “Company” means the named legal entity as well as any units, firms, partnerships, associations, corporations, limited liability companies, trusts, subsidiaries, affiliates, divisions, departments, branches, joint ventures, proprietorships, syndicates, or other legal, business or government entities over which the named legal entity exercises control or in which the named entity has any ownership whatsoever.
6. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual’s complete name and title; (b) the individual’s business or personal address and phone number; and (c) any and all known aliases.
7. The term “related to” or “referring or relating to,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with, or is pertinent to that subject in any manner whatsoever.
8. The term “employee” means any past or present agent, borrowed employee, casual employee, consultant, contractor, de facto employee, detailee, fellow, independent contractor, intern, joint adventurer, loaned employee, officer, part-time employee, permanent employee, provisional employee, special government employee, subcontractor, or any other type of service provider.
9. The term “individual” means all natural persons and all persons or entities acting on their behalf.

Page 222

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 223

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 224

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 225

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 226

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 227

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 228

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 229

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 230

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 231

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 232

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 233

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 234

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 235

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 236

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 237

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 238

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

**From:** (b)(6)  
**To:** (b)(6)  
**Cc:**  
**Subject:** RE: Geolocation Data Project  
**Date:** Friday, November 22, 2019 12:02:00 PM  
**Attachments:** [HawkEye360 Memo 2019.11.22.pdf](#)  
[HawkEye360 TandE Narrative 2019.11.22.pdf](#)  
[venntel\\_signal-record-format\\_daily121.pdf](#)

---

Hi (b)(6)

OGC/S&T provides the following input in response to your request for information below:

**LEGAL AUTHORITIES FOR THE SCIENCE AND TECHNOLOGY DIRECTORATE**

(b)(5)

S&T is considered a support component within DHS and is responsible for research, development, test and evaluation activities (RDT&E activities) on behalf of DHS components and offices. **S&T does not have operational, law enforcement or intelligence authorities.**

Pursuant to 6 U.S.C. § 182, the Under Secretary for Science and Technology is responsible for, in relevant part:

1. conducting research, development, demonstration, testing and evaluation activities that are relevant to any or all elements of the Department, except human health-related research and development activities (Section 182(4))
2. supporting the Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection, by assessing and testing homeland security vulnerabilities and possible threats (Section 182(3))
3. establishing and administering the primary research and development activities of the Department, including the long-term research, development, demonstration, testing and evaluation activities of the Department (Section 182(11))
4. coordinating and integrating all research, development, demonstration, testing and evaluation activities of the Department (Section 182(12))

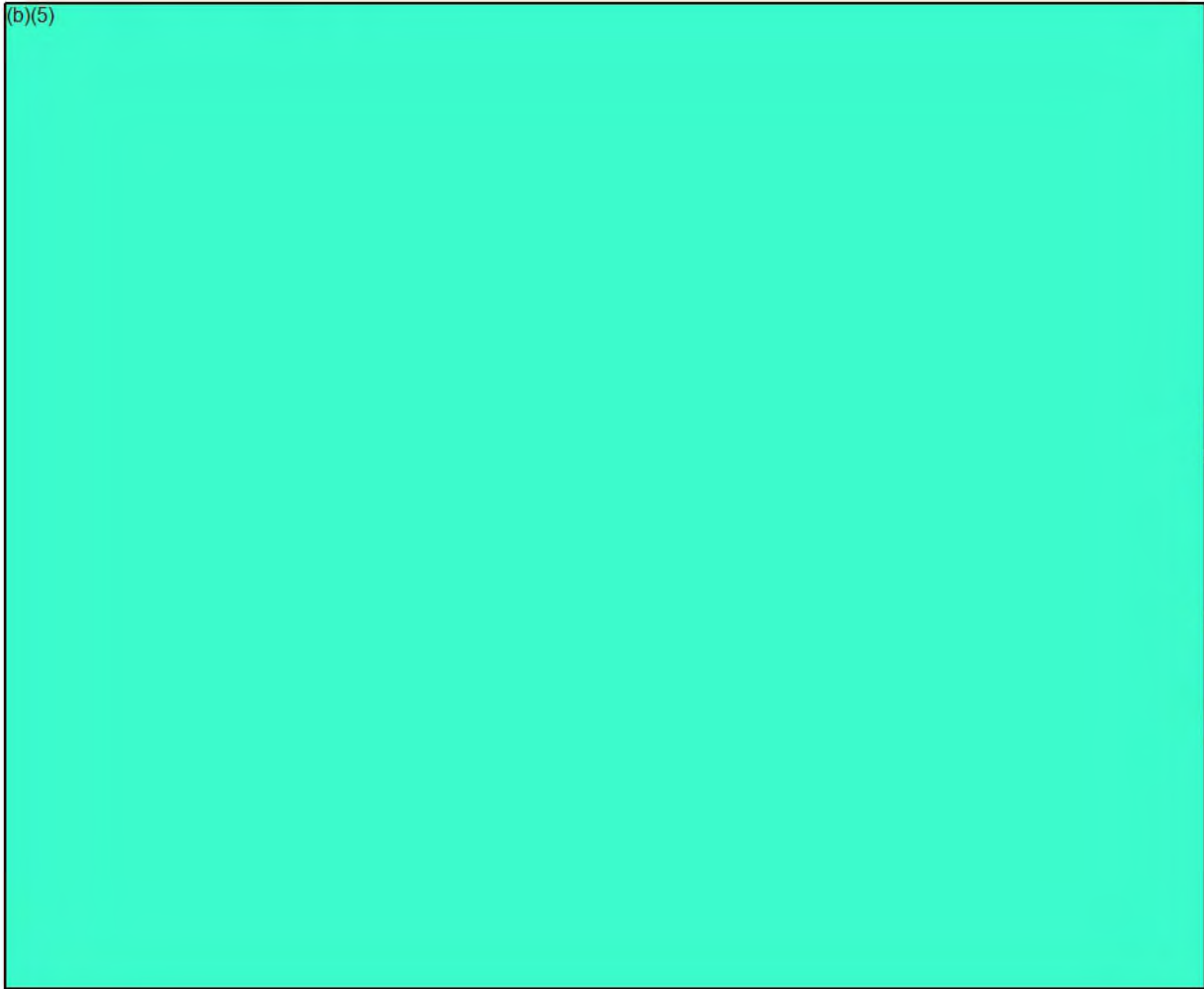
S&T conducts RDT&E activities for the Department by working closely with operational components to leverage the operational component's authorities to acquire, use, transfer, share and store information/data. (b)(5)

(b)(5)

(b)(5) This same model would apply to any S&T's RDT&E activities relating to geolocation data projects.

**POTENTIAL DATA SOURCES**

(b)(5)

A large rectangular area of the page is completely redacted with a solid black fill. The text "(b)(5)" is written in the top-left corner of this redacted area. On the right edge of the redacted area, there are two small yellow sticky tabs. The top tab has the letters "t." and "s" visible, and the bottom tab has the letter "y" visible.

(b)(5)

A smaller rectangular area of the page is redacted with a solid black fill. The text "(b)(5)" is written in the top-left corner of this redacted area.

**DHS USE CASES**

(b)(5)

A large rectangular area at the bottom of the page is redacted with a solid black fill. The text "(b)(5)" is written in the top-left corner of this redacted area.



(b)(5)



**OTHER INFORMATION**

While you did not ask for this information specifically, I think it may be useful for you as we continue to work on this issue.

(b)(5)



If you would like to discuss any of the input above, please let us know. Have a great weekend.

Best,

(b)(6)

---

Minal Patel  
Attorney - Technology Programs Law Division  
Office of the General Counsel  
Department of Homeland Security

(b)(6) (Office)  
(b)(6) (Cell)

(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

---

**From:** (b)(6)

**Sent:** Tuesday, November 19, 2019 2:07 PM

(b)(6)



**Subject:** Geolocation Data Project

Team,

My apologies for the delay on following up after our first call. I wanted to circle back with a status update, as well as some requests for each component represented on this email.

(b)(5)



last week.

(b)(5)



Thank you,

(b)(6)

(b)(6)

Deputy General Counsel  
Office of the General Counsel  
U.S. Department of Homeland Security

(b)(6)

(Office)  
(Cell)

Page 244

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 245

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 246

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 247

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 248

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 249

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 250

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 251

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 252

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 253

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act