

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.”¹ This location data can reveal where we go and with whom we associate, tracking us in our homes, at the doctor, or at church.²

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.³ 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.

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

² *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).

³ *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/).

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.⁴ 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.⁵

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.⁶ 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.⁷

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.⁸

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.⁹ An investigation in 2018 by the New York Times uncovered 75 companies that were

⁴ *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).

⁵ *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).

⁶ *USASpending.gov* (accessed June 22, 2020).

⁷ *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/); *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);

⁸ *See* 18 U.S.C. § 2702.

⁹ *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); 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).

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

The scale of this data collection is staggering. For example, Venntel's reported parent company, Gravy Analytics,¹² has revealed that it collects location data from software "embedded within tens of thousands of apps."¹³ According to its website, Gravy Analytics "processes billions of pseudonymous mobile location signals every day from millions of mobile devices."¹⁴ 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.¹⁵

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.¹⁶ 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.¹⁷ Media reports have also identified companies targeting advertisements to people in emergency rooms¹⁸ and dialysis centers.¹⁹ In

¹⁰ *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).

¹¹ *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/).

¹² *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).

¹³ Gravy Analytics, *Location Data & COVID-19* (online at gravyanalytics.com/covid-19/) (accessed June 22, 2020).

¹⁴ Gravy Analytics, *Our Data* (online at gravyanalytics.com/our-data/) (accessed June 22, 2020).

¹⁵ *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).

¹⁶ *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/); *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); *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).

¹⁷ *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).

¹⁸ *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).

¹⁹ *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).

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.²⁰

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.²¹

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;

²⁰ *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).

²¹ *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.

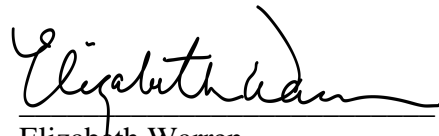
An attachment to this letter provides additional instructions for responding to this request. If you have any questions regarding this request, please contact Committee staff at (202) 225-5051, Senator Warren's staff at (202) 224-4543, or Senator Wyden's staff at (202) 224-5244.

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.