

EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:

ENVIRONMENT AND PUBLIC WORKS

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON SECURITY

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

February 12, 2020

SUITE SD-255
DIRKSEN BUILDING
WASHINGTON, DC 20510-2107
202-224-2742

975 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-677-0523

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

The Honorable Chad F. Wolf
Acting Secretary
U.S. Department of Homeland Security
245 Murray Lane, SW
Washington, DC 20528

Dear Acting Secretary Wolf:

I write regarding recent reports that the Department of Homeland Security (DHS) has purchased data and software that tracks the physical location of millions of individuals and is using this information for immigration enforcement purposes.¹ The government's access to and use of this information poses serious privacy and civil liberty risks, and is an egregious escalation of the Trump administration's practice of employing invasive and draconian immigration enforcement tactics.

New findings published in the *Wall Street Journal* show that, dating back to 2017, DHS has paid a private company, Venntel Inc., for access to information about the physical location of individuals and their mobile devices.² Venntel Inc. itself reportedly purchases this information from private marketing companies that source the data from cellphone apps. Although it appears that the data in question is not explicitly attached to specific individuals, it is clear that even anonymized mobile location data can easily be used to identify unique persons.³ DHS's apparent leveraging of a large data set of sensitive information is particularly concerning following the revelation that a "malicious cyberattack" last year compromised troves of data held on behalf of U.S. Customs and Border Protection (CBP).⁴

¹ Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, *Wall Street Journal* (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600?reflink=share_mobilewebshare.

² *Id.*

³ Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, *N.Y. Times* (Dec. 19 2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>.

⁴ Drew Harwell & Geoffrey A. Fowler, *U.S. Customs and Border Protection says photos of travelers were taken in a data breach*, *Wash. Post* (June 10, 2019), https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/?utm_term=.29d4023b211d.

Moreover, in the Supreme Court's 2018 decision in *Carpenter v. United States*, the Court acknowledged that cell-site location information (CSLI) is a highly sensitive and revealing class of information, deserving of "special solicitude."⁵ In *Carpenter*, writing for the majority, Chief Justice Roberts described government tracking of CSLI as "near perfect surveillance."⁶ Further, the Court explained that the third-party doctrine — under which a person forgoes his or her legitimate expectation of privacy when voluntarily exposing information to a third party — does not hold up when it comes to CSLI:

Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements.⁷

For these reasons, the Court held that the government will generally need a search warrant supported by probable cause in order to access CSLI.⁸

DHS's purchase of location data gleaned from cellphone apps thus appears to contravene the spirit, if not the letter, of *Carpenter*. Circumventing *Carpenter*'s warrant requirement in this manner is particularly alarming because DHS has been using this location data for law enforcement purposes. According to the *Wall Street Journal*, DHS has used this data to generate investigative leads about possible illegal border crossings, as well as to track human- and drug-smuggling investigations.⁹ Worse still, sources cited in the *Wall Street Journal* report also allege that Immigration and Customs Enforcement (ICE) has since shared this revealing data with ICE's Enforcement and Removal Operations (ERO) directorate — the division tasked with deportations. In effect, DHS seems to thumb its nose at the Supreme Court by engaging in warrantless cellphone location tracking of individuals in order to expand the reach of its merciless deportation force.

Tracking like this is completely inconsistent with — and has disturbing and chilling effects on — the privacy protections our Constitution guarantees. Therefore, I request written answers to the following questions by Tuesday, March 3, 2020:

1. Please identify all contracts or other agreements between DHS and any non-government entities under which DHS is purchasing or otherwise accessing individuals'

⁵ *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018).

⁶ *Id.* at 2218.

⁷ *Id.* at 2220 (internal quotation marks, brackets, and citation omitted).

⁸ *Id.* at 2221.

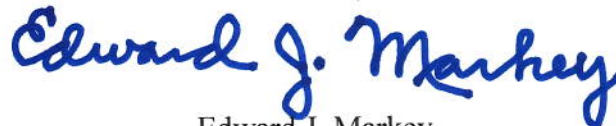
⁹ Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, *Wall Street Journal* (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600?reflink=share_mobilewebshare.

location data, including all substantive terms (*e.g.*, the parties, scope, duration, and compensation). Please provide copies of the contracts.

2. Does the ERO directorate under ICE have access to location data DHS obtains under these contracts or other agreements? If so, when and how did ERO obtain access to this data?
3. What reasons, if any, did DHS give to Ventell Inc. or any other non-government entities as to why DHS was purchasing location data from them?
4. How specifically is DHS using purchased location data? If uses differ between CBP and ICE, please describe those differences.
 - a. Has ICE ever used this location data for routine deportation operations? If yes, in how many instances? If not, does ICE have any plans to use the data for those purposes?
5. What legal standard, if any, does DHS believe applies to the access and use of location information from Ventell Inc. or other commercial sources of this type of data? Does DHS believe a search warrant or other court order is ever required?
6. What privacy protections and limits, if any, does DHS have on how it uses location data? If protections and limits differ between CBP and ICE or any other entities within DHS, please describe those differences.
7. How long does DHS retain the location data it purchases from private entities?
8. Is the data in question stored by DHS itself or a private contractor?
9. Please detail the data security practices DHS employs to ensure that individuals' location data is not breached or left vulnerable to malicious actors.
10. Has location information that DHS has purchased ever been breached or inappropriately accessed? If so, please describe when and how that occurred.

Thank you in advance for your attention to these requests.

Sincerely,



Edward J. Markey
United States Senator