May 31, 2019

Via Electronic Mail

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

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

RE: Request Under the Freedom of Information Act U.S. Customs and Border Protection Access to Commercial Location Data

To whom it may concern:

This letter constitutes a request under the Freedom of Information Act ("FOIA") and is submitted on behalf of the Center for Democracy & Technology ("CDT")[1] to the Department of Homeland Security ("DHS") and United States Customs and Border Protection ("CBP"). CDT respectfully requests records pertaining to CBP's access to commercial location data.

I. Requested Documents

1) Any contracts, memoranda of understanding or other agreements, including all modifications, pursuant to CBP's access to commercial location data as referred to in DHS/CBP/PIA-022(a);[2]

[1] The Center for Democracy & Technology is a 501(c)(3) organization that advocates for global online civil liberties and human rights. CDT drives policy outcomes that keep the internet open, innovative, and free. The organization supports laws, corporate policies, and technology tools that protect privacy, and advocates for stronger legal controls on government surveillance. https://cdt.org/about/.

[2] U.S. Dep't of Homeland Sec., U.S. Customs and Border Protection, DHS/CBP/PIA-002(a), Privacy Impact Assessment Update for the Border Surveillance Systems (BSS), 6 (Aug. 21, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp022-bss-september2018.pdf.

2) Any policy directives, guidance documents, memoranda, training materials, or similar records guiding CBP employees on the use of the commercial location data; and
3) Any brochures, training materials, and other informational materials provided to CBP from any entity which provides this type of access to commercial location data.

II. Background

On August 21, 2018, CBP issued a Privacy Impact Assessment (PIA), "Border Surveillance Systems (BSS) DHS/CBP/PIA-022(a),"[3] providing an update on existing border surveillance technologies. Among the acquisitions prompting the update was CBP's access to commercially available location data. CBP states that the agency may acquire "commercially available location data" from "third-party providers" in order to "detect the presence of individuals in areas between Ports of Entry where such a presence is indicative of potential illicit or illegal activity."[4] CBP further states that the data they receive "is compiled by a third-party provider from multiple commercial sources and anonymized, offered for purchase, and can then be acquired by public or private entities,"[5] including government agencies like CBP.

The source of this commercially available location data is of interest to the public. In 2018 and throughout 2019, investigations revealed that telecommunications providers sold customer location information to location data aggregators who would sell the data to other third parties, allowing the data to get into the hands of bounty hunters.[6] The providers have since promised to no longer sell location data, and that the arrangements through which they sold this data are winding down.[7] These statements came after CBP's PIA was published. It is unclear if CBP was a recipient, however indirectly, of this location data, if the agency continues to be a recipient of this data despite the statements that the location data is no longer sold, or if CBP has an alternative source of location information.

DHS and CBP are no doubt aware that location information is very sensitive. This was recently highlighted by the Supreme Court in its June 22, 2018 ruling in *Carpenter v. United States*, a case about whether law enforcement collection of cell site location information constitutes a search under the Fourth Amendment.[8] In *Carpenter*, law enforcement sought 127 days of cell site location data using an 18 USC 2703(d) order. The Supreme Court issued a groundbreaking ruling in which it held that law enforcement must get a warrant based on probable cause if it seeks more than seven days' worth of historical cell site location information. The Court noted the sensitivity of the information as the data, "provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations."[9] *Carpenter* is the first time metadata has been

[3] *Id*.
[4] *Id*.
[5] *Id*.
[6] Sean Hollister, *Carriers selling your location to bounty hunters: it was worse than we thought*, The Verge (Feb. 6, 2019), https://www.theverge.com/2019/2/6/18214667/att-t-mobile-sprint-location-tracking-data-bounty-hunters.
[7] Jon Fingas, *US Carriers say they've stopped selling location data*, Engadget (May 17, 2019), https://www.engadget.com/2019/05/17/carriers-say-they-stopped-selling-location-data/.
[8] *Carpenter v. United States,* 138 S.Ct. 2206 (2018).
[9] *Id*. at 2217.

protected by the warrant standard, and the first carve out to the third party doctrine. While the Court claimed its holding was narrow, the reasoning is quite broad. The records sought on how CBP is acquiring location information will inform the public if the government is receiving data that should be protected by a heightened standard as held in *Carpenter*.

III. Application for Waiver of Fees

CDT requests a waiver of document search, review, and duplication fees on the grounds that disclosure of the requested records is in the public interest and because disclosure is "likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester." 5 U.S.C. § 552(a)(4)(A)(iii). CDT also requests a waiver of search fees on the grounds that the CDT qualifies as a "representative of the news media" and the records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

1. *Disclosure of the requested records is likely to contribute significantly to public understanding of operations or activities of the government and is not primarily in the commercial interest of CDT.*

There is significant interest in CBP surveillance and enforcement conduct at and between Ports of Entry, and numerous news accounts reflect the considerable public interest in the requested records. CBP's use of and access to technology at the border is a topic of significant public attention, particularly how the agency's use of technology impacts the privacy and civil liberties rights of those subject to the technology.[10] CBP's access to location information has garnered specific attention.[11] Likewise, information regarding the selling and receipt of location data also prompted sustained media and civil society attention.[12] It also prompted Congressional inquiries

[10] *See, e.g.,* Tanvi Misra, *The Problem With a 'Smart' Border Wall*, Citylab (Feb. 12, 2019), https://www.citylab.com/equity/2019/02/smart-wall-border-surveillance-tech-security-deal-trump-data/582589/; Emily Birnbaum, *Trump, Dem talk of 'smart wall' thrills tech companies*, The Hill (Jan. 31, 2019), https://thehill.com/policy/technology/427929-trump-dem-talk-of-smart-wall-thrills-tech-companies; Angela Chen, *How Far Has Technology Come Since The Last "Smart Border" Failed*, The Verge (Feb. 22, 2019), https://www.theverge.com/2019/2/22/18236515/smart-border-virutal-fence-surveillance-trump-borders-politics-policy; Kristina Davis, *How would a "smart wall" work at the U.S.-Mexcio border?*, L.A. Times (Mar. 24, 2019), https://www.latimes.com/local/lanow/la-me-ln-smart-border-wall-20190324-story.html; Neema Singh Guliani & Michelle Fraling, *Congress, Don't Give DHS Unrestricted Authority to Build a "Smart Wall"*, ACLU (Feb. 1, 2019), https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/congress-dont-give-dhs-unrestricted-authority; Mana Azarmi, *A "Smart Wall" That Fails to Protect Privacy and Civil Liberties is Not Smart*, Ctr. For Democracy & Tech, (Feb. 8, 2019), https://cdt.org/blog/a-smart-wall-that-fails-to-protect-privacy-and-civil-liberties-is-not-smart/; Lily Hay Newman, *A "Smart Wall" Could Spark A New Kind of Border Crisis*, Wired (Feb. 21, 2019), https://www.wired.com/story/border-smart-wall-privacy-surveillance/; Hamza Shaban, *Advocacy groups urge Democrats to oppose DNA collection and facial scanning at the border*, WaPo (Feb. 5, 2019), https://www.washingtonpost.com/technology/2019/02/05/advocacy-groups-urge-democrats-oppose-invasive-surveillance-tech-border-security-negotiations/?utm_term=.07d8a58a8cde.

[11] See, e.g., Shirin Ghaffary, *The "smarter wall": how drones, sensors, and AI are patrolling the border*, Vox (May 16, 2019), https://www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai; Bonnie Berkowitz, Shelly Tan & Kevin Uhmacher, *Beyond the wall: dogs, blimps and other things used to secure the border*, WaPo (Feb. 8, 2019), https://www.washingtonpost.com/graphics/2019/national/what-is-border-security/?noredirect=on&utm_term=.f82ee8f7a3e1.

[12] *See, e.g.*, Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You Too*, N.Y. Times (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html;

and the related pressure incentivized telecommunications companies to change their business practices.[13] Finally, there is significant interest in DHS and CBP's interpretations of its authority to conduct electronic surveillance. Modern technology provides law enforcement with new tools and sources of information to aid their investigations. What *Carpenter* means for the future of the Fourth Amendment has been the source of much discussion and debate.[14] How DHS and CBP are interpreting their obligations after *Carpenter*, as reflected in how and what location information they access, will inform Congress and the public about any gaps in protection, and provide notice to the public about the circumstances in which DHS can access their data.

CDT is not filing this FOIA to fulfill a commercial interest. This request is made in furtherance of the work CDT does for the public interest.

2. *CDT qualifies as "a representative of the news media" and the records requested are not sought for commercial use.*

CDT also requests a waiver of search fees on the grounds that CDT qualifies as a "representative of the news media" and the records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II). CDT meets the statutory and regulatory definitions of a "representative of the news media" because it is an "entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and

---

Sean Hollister, *Carriers selling your location to bounty hunters: it was worse than we thought*, The Verge (Feb. 6, 2019), https://www.theverge.com/2019/2/6/18214667/att-t-mobile-sprint-location-tracking-data-bounty-hunters; Lily Hay Newman, *Carriers Swore They'd Stop Selling Location Data. Will They Ever?*, Wired (Jan. 9, 2019), https://www.wired.com/story/carriers-sell-location-data-third-parties-privacy/; Micah Singleton, *Verizon will stop selling real-time location data to third party brokers*, The Verge (Jun 19, 2018), https://www.theverge.com/2018/6/19/17478934/verizon-selling-real-time-location-data-third-party-securus-wyden; Brian Barrett, *A Location-Sharing Disaster Shows How Exposed You Really Are*, Wired (May 18, 2018), https://www.wired.com/story/locationsmart-securus-location-data-privacy/; Zach Whittaker, US cell carriers are selling access to your real-time phone location data, ZDNet (May 14, 2018), https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/; Brian Fung, *Verizon, AT&T, T-Mobile and Sprint suspend selling of customer location data after prison officials were caught misusing it*, WaPo (Jun. 18, 2019), https://www.washingtonpost.com/news/the-switch/wp/2018/06/19/verizon-will-suspend-sales-of-customer-location-data-after-a-prison-phone-company-was-caught-misusing-it/?noredirect=on&utm_term=.e3f373ab58d3.

[13] Press Release. *Following Wyden's Investigation, Verizon Pledges to End Contracts With Companies that Sell Americans' Location* (Jun. 19, 2018), https://www.wyden.senate.gov/news/press-releases/following-wydens-investigation-verizon-pledges-to-end-contracts-with-companies-that-sell-americans-location-; Sean Lyngaas, *Wyden Calls for FCC investigation into cell-phone tracking used by law enforcement*, Cyberscoop (May 11, 2018), https://www.cyberscoop.com/wyden-calls-fcc-investigation-cell-phone-tracking-used-law-enforcement/; Press Release. *Senators Call on FCC and FTC to Investigate How Wireless Carriers Sold American's Mobile Phone Locations To Data Brokers, Bounty Hunters and Shady Middlemen* (Jan. 24, 2019), https://www.wyden.senate.gov/news/press-releases/senators-call-on-fcc-and-ftc-to-investigate-how-wireless-carriers-sold-americans-mobile-phone-locations-to-data-brokers-bounty-hunters-and-shady-middlemen.

[14] *See, e.g.,* Jake Laperruque, *The Carpenter Decision: A Huge Step Forward but Major Problems Remain*, POGO (June 28, 2018), https://www.pogo.org/analysis/2018/06/carpenter-decision-huge-step-forward-for-privacy-rights-but-major-problems-remain/; J.G. Harrington, *Carpenter v. United States: What It Means for Companies That Collect Location Data*, Cooley (June 28, 2018), https://www.cooley.com/news/insight/2018/2018-06-28-carpenter-v-united-states-what-it-means-for-companies-that-collect-location-data; Paul Ohm, *The Many Revolutions of Carpenter*, LawArXiv (Nov. 1, 2018) (https://osf.io/preprints/lawarxiv/bsedj/; *Center on Privacy & Technology Explores Implications of Carpenter v. U.S.*, Georgetown Law, (July 5, 2018), https://www.law.georgetown.edu/news/center-on-privacy-technology-explores-implications-of-carpenter-v-u-s/.

distributes that work to an audience." 5 U.S.C. § 552(a)(4)(A)(ii)(III). CDT maintains an active website and social media presence that helps it distribute its commentary and reporting on topical issues related to its mandate.[15] CDT also maintains a bi-weekly newsletter through which it disseminates new material like blog posts and insights to subscribers. CDT will release the requested documents to the public without charge.

For these reasons CDT requests that fees for this FOIA request be waived.

Please furnish materials associated with this request to:

Mana Azarmi
Center for Democracy & Technology
1401 K Street NW, Suite 200
Washington, DC 20005
mazarmi@cdt.org
(202) 407-8828

Thank you for your attention to this matter.

Respectfully,

Mana Azarmi
Policy Counsel
Center for Democracy & Technology

[15] *See, e.g.*, Natasha Duarte, *5 Takeaways from the New DHS Privacy Guidance*, Ctr. For Democracy & Tech. (May 17, 2017), https://cdt.org/blog/5-takeaways-from-the-new-dhs-privacy-guidance/; Mana Azarmi, *Location Data: The More They Know*, Ctr. For Democracy & Tech. (Nov. 27, 2017), https://cdt.org/blog/location-data-the-more-they-know/; Greg Nojeim & Mana Azarmi, *Court Steps in to Protect Constitutional Rights at the Border*, Ctr. For Democracy & Tech. (May 11, 2018), https://cdt.org/blog/courts-step-in-to-protect-constitutional-rights-at-the-border; Mana Azarmi, *CBP's Border Searches Struggle to Comply with Constitution and Agency Policy*, Ctr. For Democracy & Tech. (Dec. 18, 2018), https://cdt.org/blog/cbps-border-searches-struggle-to-comply-with-constitution-and-agency-policy/.