Chief FOIA Officer
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Ave SE
Washington, DC 20528-0655

Via Email

June 13, 2020

Re: Records related to COVID-19 surveillance and data analysis

Dear FOIA Officer:

Pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and the implementing regulations of your agency, Just Futures Law, Mijente Support Committee, Media Justice, and the Immigrant Defense Project seek records from U.S. Department of Homeland Security (DHS) (herein "agency") that shed light on how federal and local governments are using technologies and companies to expand data surveillance during the COVID-19 pandemic, and to what extent governments and companies are collecting and sharing this data for possible uses beyond addressing the immediate health crisis.

Background

Federal and local governments have been developing technologies to track the physical location, biometrics data, and online data of residents long before the COVID-19 pandemic. Many tech corporations, such as Palantir, Google, and Amazon, already sell massive data collection or analytics services to government agencies, including police departments and Immigration and Customs Enforcement (ICE).

Now, amid a global health crisis, governments and tech corporations are using the moment to dramatically accelerate mass surveillance.[1] For example, the Trump Administration has tapped Palantir Technologies to build a health surveillance system for U.S. healthcare agencies using the

[1] *See, e.g.* Adam Cancryn, *Kushner's team seeks national coronavirus surveillance system*, Politico, (Apr. 8, 2020), https://www.politico.com/news/2020/04/07/kushner-coronavirus-surveillance-174165 (A national coronavirus surveillance system represents "a significant expansion of government use of individual patient data, forcing a new reckoning over privacy limits amid a national crisis").

same software sold to ICE to track down immigrants for deportation.[2] In the coming months and years, Health and Human Services (HHS) is set to spend $500 million from Congress's stimulus package on health surveillance and data technologies. From GPS trackers to thermal scanners to private health data collection, everything seems to be on the table.

However, while some of this data may have a public health purpose, there is little to no information on the duration of this surveillance, limits on data use, or the effectiveness of these invasive technologies at addressing the immediate crisis. For example, neither mobile location data nor contact-tracing apps have been shown to mitigate disease spread.[3] Moreover, concerns over privacy can actually deter people from seeking care and other essential health services.[4]

Meanwhile, the privacy impact of this data surveillance is deeply alarming. At least one government surveillance platform, HHS Protect Now, has been built by contractor Palantir to store personal health information.[5] Moreover, though tech companies claim that they only share anonymous data with governments, multiple studies have shown that industry standards for de-identified data (e.g. sharing so-called "aggregated" mobile location data) fail to preserve anonymity and can still lead to privacy breaches.[6]

The expansion of the government surveillance under COVID-19 and the close collaboration of tech corporations has drawn global scrutiny.[7] For example, in the United Kingdom, there are growing concerns over a similar health surveillance system that Palantir, Amazon, and Google are building for the National Health Service (NHS).[8] UK transparency groups have called the surveillance project "the largest handover of NHS patient data to corporations in history."[9]

---

[2] Thomas Brewster, *Palantir, The $20 Billion, Peter Thiel-Backed Big Data Giant, Is Providing Coronavirus Monitoring To The CDC,* Forbes (Mar. 31, 2020), https://www.forbes.com/sites/thomasbrewster/2020/03/31/palantir-the-20-billion-peter-thiel-backed-big-data-giant-is-providing-a-coronavirus-monitoring-tool-to-the-cdc/#7000a1411595.

[3] *U.S. Senate Republicans' COVID-19 data protection bill misses the mark*, Access Now (May 8, 2020), https://www.accessnow.org/u-s-senate-republicans-covid-19-data-protection-bill-misses-the-mark/; Adam Schwartz & Andrew Crocker, *Governments Haven't Shown Location Surveillance Would Help Contain COVID-19*, Electronic Frontier Foundation (Mar. 23, 2020), https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance-would-help-contain-covid-19.

[4] Miriam Jordan, *'We're Petrified': Immigrants Afraid to Seek Medical Care for Coronavirus*, N.Y. Times (Mar. 18, 2020) (updated May 12, 2020), https://www.nytimes.com/2020/03/18/us/coronavirus-immigrants.html.

[5] Blake Dodge, *The US teamed up with Palantir on a secretive project to analyze coronavirus data. Now, they want to gather personal health information, too*, Business Insider (May 7, 2020), https://www.businessinsider.com/hhs-protect-palantir-healthcare-data-coronavirus-trump-2020-5.

[6] Kelsey Campbell-Dollaghan, *Sorry, your data can still be identified even if it's anonymized*, Fast Company (Dec. 10, 2018), https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized.

[7] Nemo Kim, *'More Scary Than Coronavirus': South Korea's Health Alerts Expose Private Lives*, The Guardian (Mar. 5, 2020), https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives; David Gilbert, *Iran Launched an App That Claimed to Diagnose Coronavirus. Instead, It Collected Location Data on Millions of People*, Vice (Mar. 14, 2020), https://www.vice.com/en_us/article/epgkmz/iran- launched-an-app-that-claimed-to-diagnose-coronavirus-instead-it-collected-location-data-on-millions-of- people.

[8] Matthew Gould, Dr. Indra Josh, & Ming Tang, *The power of data in a pandemic*, Technology in the NHS (Mar. 28, 2020), https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/.

[9] Sources have reportedly described the amounts of health data funneled into the data project as "unprecedented." Paul Lewis, David Conn, & David Pegg, *UK government using confidential patient data in coronavirus response*, The Guardian (Apr. 12, 2020),

Requesters seek information on what types of data governments and technology companies are collecting as part of COVID-19 health surveillance and how they store, share, and sell the data. For ease of review, this request breaks down into the below sections:

- Data Sources and Collection Methods
- Technology and Intelligence Companies
- Data-Anonymization
- Data-Sharing and Use Limitations
- Data-Retention.

Please refer this search request for records to sub-agencies that are involved in COVID-19 health surveillance or/and data analytics. This should include but may not be limited to the Office of the Secretary; Office of the Deputy Secretary; Office of the Chief Procurement Officer including but not limited to its COVID-19 Procurement & Acquisition Innovation Response (PAIR) Team and Office of Acquisition; Office of the Chief Information Officer (CIO) including but not limited to its Office of the Chief Technology Officer and Information Sharing and Services Office; DHS Privacy Office; and Office of Partnership and Engagement.

Records Requested

I. Data Sources and Collection Methods

1. Records on the sources of data collected or used by the agency[10] relating to COVID-19[11] health surveillance or data analytics[12] such as to monitor disease spread, conduct contact-tracing or track social distancing. Examples of data sources may include but are not limited to:
    a. Mobile location data or mobility data[13] e.g. data from mobile advertisers or telecom operators such as Cuebiq, SafeGraph, X-Mode, Unacast, Foursquare, Tutela;[14]

---

https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response; Mary Fitzgerald & Cori Crider, *We need urgent answers about the massive NHS COVID data deal*, Open Democracy (May 7, 2020), https://www.opendemocracy.net/en/opendemocracyuk/we-need-urgent-answers-about-massive-nhs-covid-data-deal/.

[10] For the purposes of this request, we mean the term "agency" to include the agency, its contractors, vendors or agents.

[11] For the purposes of this request, we mean the term "COVID-19" to include and be interchangeable with "coronavirus", "SARS-CoV-2", "Wuhan flu", "Wuhan virus" or "severe acute respiratory syndrome."

[12] For the purposes of this request, "COVID-19 health surveillance and/or data analytics" includes any data source, data platform, data product, or data analytics systems collected or used by the agency in responding to COVID-19.

[13] *E.g.*, Arielle Lasry et al., *Timing of Community Mitigation and Changes in Reported COVID-19 and Community Mobility -- Four U.S. Metropolitan Areas, February 26-April 1, 2020*, Centers for Disease Control and Prevention (Apr. 13, 2020), https://www.cdc.gov/mmwr/volumes/69/wr/mm6915e2.htm (confirming that the CDC uses data from SafeGraph); *COVID-19 Daily Data Summary*, COVID-19: Keeping Los Angeles Safe (Apr. 29. 2020), https://corona-virus.la/sites/default/files/inline-files/Release_Daily%20Data%20Report%20Wednesday%204_29_F.pdf (reporting the City of Los Angeles use of mobile location data from Unacast, SafeGraph, Facebook, and Apple).

[14] A more comprehensive list of mobile advertisers and mobile intelligence companies can be found at Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 12, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

b. Data analytics or platform companies e.g. Google, Amazon Web Services, Microsoft, Facebook, Palantir Technologies, MITRE, Bluedot;
c. Contact-tracing mobile applications;
d. Health monitoring applications or wearables e.g. Fitbit, Apple apps;
e. Social media data or monitoring programs;
f. Street cameras;
g. Thermal scanners, cameras or other temperature monitoring devices e.g. Kinsa, Flir Systems, DaHua;
h. Stingrays or cell-site simulators;
i. Drones or unmanned aerial systems;
j. Facial recognition devices;
k. State or city phone hotlines related to COVID-19;
l. 911 call data tracking platforms e.g. Carbyne Ltd[15], or reports to 911 or 311 related to COVID-19 or social distancing violations;
m. COVID-19 testing, diagnostic or lab data;
n. Patient medical records or data from medical-records companies;
o. Hospital or healthcare facilities data;
p. State, county or city public health agencies;
q. Colleges, universities, and/or research institutions.

2. For each of the sources of data collected or used by the agency for COVID-19 health surveillance or data analytics, records reflecting the method that the agency or/and contractors use to obtain the source of data including but not limited to:
    a. Any procurement order, purchasing order, contract, license agreement, use agreement, data-sharing agreement or memorandum of understanding (MOU);
    b. Any criminal warrant, probable cause, or reasonable suspicion justifying data collection or use;
    c. Any policy, procedure, release, or/and form relating to obtaining the consent of individuals to collect or use their data;
    d. Any policy, procedure, or/and form relating to providing notice to individuals on the collection or use of their data.

3. Records related to data sources and private companies involved in HHS Protect or Protect Now including but not limited to:
    a. Any records related to which "decision-makers and responders" have access to HHS Protect and any plans to scale the platform at DHS.[16]
    b. Any records reflecting what are the data sources or datasets. According to multiple new articles, HHS Protect includes at least 187 and up to 200 datasets

[15] Deniz Çam & Thomas Brewster, *To Fight Coronavirus, This City Is Asking 911 Callers To Agree To Self Surveillance*, Forbes (Mar. 17, 2020), https://www.forbes.com/sites/denizcam/2020/03/17/to-fight-coronavirus-new-orleans-is-using-a-911-app-backed-by-peter-thiels-founders-fund/#768cf131b065; Lucy Blumberg, *An open letter on surveillance in New Orleans*, The Lens (May 1, 2020), https://thelensnola.org/2020/05/01/an-open-letter-on-surveillance-in-new-orleans/.

[16] Dave Nyczepir, *Inside the HHS System Informing White House Coronavirus Decisions*, FEDSCOOP (Apr. 21, 2020), https://www.fedscoop.com/hhs-system-white-house-coronavirus-response-jose-arrieta/;

pulled from federal agencies, all 50 states, healthcare facilities, academia, and private industry.[17]

c. Any records related to private companies, contractors, or vendors involved in building the HHS Protect system or managing or sourcing its data.

II. Technology and Intelligence Companies

1. Records reflecting which private entities have assisted the agency in COVID-19 health surveillance or data analytics including but not limited to:
    a. Any request for proposal, solicitation, or contract awards related to COVID-19 data collection, surveillance, or data analytics including through the *DHS COVID-19 Procurement & Acquisition Innovation Response (PAIR)* Team.[18] Please include all attachments, addendums, justification for other than full and open competition, and exhibits;
    b. Any agreements, statement of work, or scope of work with contractors, vendors, or other private entities related to COVID-19 data collection, surveillance or data analytics;
    c. Any data-sharing agreements, use agreements, or licensing agreements with contractors, vendors, or other private entities related to COVID-19 data collection, surveillance or data analytics;
    d. Any policies, protocols, agreements, memoranda of understanding (MOU) governing contractors, vendors, associations of contractors and vendors, or other private entities assisting the agency in COVID-19 data collection, surveillance or data analytics.

2. All emails sent (including emails, complete email chains, email attachments, and calendar invitations) by the government officials specified below containing any of the following key terms:

    DHS Secretary Chad Wolf; Senior Official Performing the Duties of the Deputy Secretary, Ken Cucinelli; DHS Chief Procurement Officer Soraya Correa; DHS Chief Technology Officer Brian Teeple; DHS Chief Information Officer Karen Evans; DHS Information Sharing and Services Office Director Donna Roy; Office of Biometric Identity Management Director Shonnie Lyon; Senior Official Performing the Duties of the Under Secretary for Science and Technology William (Bill) Bryan; Deputy Assistant Secretary, Office of Partnership and Engagement, Private Sector Office, Andrew Teitelbaum;

    Key Terms:

---

[17] Dodge, *supra* fn 5; Frank Bajak, *Faxes and email: Old technology slows COVID-19 response*, ABC News (May 13, 2020), https://abcnews.go.com/Business/wireStory/faxes-email-technology-slows-covid-19-response-70664883; Erin Banco & Spencer Ackerman, *Team Trump Turns to Peter Thiel's Palantir to Track Virus,* Daily Beast (Apr. 21, 2020), https://www.thedailybeast.com/trump-administration-turns-to-peter-thiels-palantir-to-track-coronavirus/body.

[18] Message from DHS Chief Procurement Officer Soraya Correa to the DHS Contractor Community on Establishing the COVID-19 Procurement & Acquisition Innovation Response (PAIR) Team, DHS https://www.dhs.gov/blog/2020/04/01/covid-19-procurement-acquisition-innovation-response-pair-team

1. Protect Now
2. HHS Protect
3. Palantir
4. Google
5. Verily
6. Apple
7. Microsoft
8. Clearview
9. Facebook
10. Amazon
11. IBM
12. "mobile location data"
13. "contact tracing"
14. COVID-19 and "data analytics"

Please provide all responsive records from January 15, 2020 through present.

In an effort to accommodate the agency and reduce the number of potentially responsive records to be processed and produced, Requesters have limited its request to emails sent by the listed custodians. To be clear, however, Requesters still request that the agency produce complete email chains, displaying both sent and received messages. This means, for example, that both the custodian's response to an email and the initial received message are responsive to this request and should be produced.

III. Data-Anonymization

1. For each of the data sources collected or used for COVID-19 health surveillance or data analytics, records reflecting whether the agency and/or its contractor handles data that includes personal identifying information including but not limited to:
    a. Residential or employment address;
    b. Location data or mobile location trail[19];
    c. Name of individual, family members, and/or contacts;
    d. Date of birth;
    e. Place of birth;
    f. Citizenship or immigration status;
    g. Photo;
    h. Phone number(s); or
    i. Social Security Number.

2. For each of the data sources collected or used for COVID-19 health surveillance or data analytics, records related to how the agency or private entity sharing the data with the

[19] Mobile location data usually contains a mobile location trail that allows for identification of the phone user. *See, e.g.* Martin Kaste, *Digital Bread Crumbs: Following Your Cell Phone Trail*, NPR (Oct. 28, 2009), https://www.npr.org/templates/story/story.php?storyId=114241860.

agency de-identifies, anonymizes, or aggregates the data. Examples of responsive records include but are not limited to:

a. Any policy or procedure relating to how data is de-identified, aggregated, anonymized;
b. Any policy or procedure relating to limiting the re-identification of data;
c. Any policy or procedure relating to collection and storage of biometrics or medical data such as temperature, face photos, COVID-19 test results;
d. Any policy or procedure relating to maintaining or monitoring data privacy;
e. Any other records that allow requesters to assess the degree of de-identification or anonymization for the source of data.

IV. Data-Sharing and Use Limitations

1. Records related to what extent the agency shares data collected or used for COVID-19 health surveillance or analytics with federal, state, local agencies or task forces including but not limited to:
    a. Any data-sharing agreements, use agreements, or/and licensing agreements between the agency and/or its contractors and other government agencies or task forces;
    b. Which federal, state, local agencies or task forces can access this data or which federal, state, local agencies or task forces does the agency share this data with;
    c. What sources of data can be accessed or shared with other federal, state, local agencies or task forces;
    d. Whether and what types of personal identifying information can be accessed or shared with other government agencies or task forces.

2. Records related to whether data collected or used for COVID-19 health surveillance or data analytics is shared or can be accessed by the U.S. Department of Homeland Security, U.S. Homeland Security Investigations, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Patrol, and/or U.S. Citizenship and Immigration Services.

3. Records related to privacy impact assessments or privacy threshold assessments regarding the data collected or used for COVID-19 health surveillance or data analytics.

4. Records related to any reports, summaries, powerpoints, or presentations that use data collected or used for COVID-19 health surveillance data or analytics.

5. Records related to the proprietary ownership of the data collected or used for COVID-19 health surveillance or data analytics.

6. Records related to any limitations or restrictions placed on federal, state, or local government agencies, task forces, contractors, vendors, or private companies on the storage, duplication, use, sharing or selling of COVID-19 health surveillance data or analytics.

V. Data-Retention

1. Records related to how long the agency and/or contractors will retain, collect, or share data collected for COVID-19 health surveillance.

2. Records related to whether the agency and/or contractors have a policy, plan, or protocol to destroy, delete or return the data collected for COVID-19 health surveillance.

Requesters

Just Futures Law is a transformational immigration lawyering organization that provides legal support for grassroots organizations engaged in making critical interventions in the United States' deportation and detention systems and policies. JFL staff maintains close relationships with organizations and activists who seek to understand the scope and range of government surveillance and criminalization. JFL staff have decades of experience in providing expert legal advice, written legal resources, and training for immigration attorneys and criminal defense attorneys on the immigration consequences of the criminal legal system. JFL has a significant interest in the administration of government surveillance and data collection. JFL has already published a number of reports on government surveillance including a report around surveillance under COVID-19.

Media Justice is a nationally recognized organizing hub representing the media policy interests and building the cultural leadership of hundreds of social justice groups across the United States. MJ includes a network of nearly 100 affiliates, over 75% of which are local, regional, or statewide social justice organizations based in under-represented communities, comprising the largest racial justice network for media rights, access, and representation in the United States. Its mission is to create media and cultural conditions that strengthen movements for racial justice, economic equity, and human rights. MJ has a focus on government surveillance of communities of color, particularly the unequal and historic surveillance of Black people, Muslims, migrants, and the social movements that represent them.

Mijente Support Committee is a national organization that coordinates and organizes with its members in several states to address issues relating to immigration enforcement and Latinx political participation. Founded by community organizers, its focus is on developing and sparking social change with respect to immigration and other social justice issues in the Latinx community and beyond.

Immigrant Defense Project is a non-profit organization whose mission is to promote fundamental fairness for immigrants accused or convicted of criminal offenses. IDP works to protect and expand the rights of immigrants who have contact with the criminal legal system, including: 1) working to transform unjust deportation laws and policies; 2) minimizing the harsh and disproportionate immigration consequences of contact with the criminal legal system; and 3) educating and advising community members, criminal defenders, and other advocates.

Request for Fee Waiver

Requesters further seek a limitation or waiver of processing (search and review) fees pursuant to 5 U.S.C. § 552(a)(4)(A)(ii)(II) ("fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by ... a representative of the news media . . ."); 5 U.S.C. § 552(a)(4)(A)(iii) ("Documents shall be furnished without any charge or at a charge reduced below the fees established under clause (ii) if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester."). *See also* 6 C.F.R. §§ 5.11(d)(1), (k)(1).

In prior FOIA requests, Media Justice, Mijente Support Committee, and the Immigrant Defense Project have received record productions from federal agencies without a fee charge. *See Mijente Support Committee et al. v. ICE,* Case No. 17-cv-02448, (D.D.C. Feb. 14, 2019) (Doc. 18) (agency agreement to produce responsive records without charging a fee); *Immigrant Defense Project et al. v. ICE*, Case No. 14-cv-06117 (S.D.N.Y. Aug. 5, 2014) (same); *Ctr for Media Justice v. FBI*, Case No. 19-cv-01465 (N.D. Cal. Dec. 13, 2019) (Doc. 59) (same).

1. Release of the requested records is in the public interest.

The records requested will contribute significantly to public understanding of the government's operations or activities. Under 6 C.F.R. § 5.11(k)(2), the following factors are to be considered in determining whether a disclosure is in the public interest: (i) whether the subject of the requested records concerns "the operations or activities of the government"; (ii) whether the disclosure is "likely to contribute" to an understanding of government operations or activities; (iii) whether disclosure of the requested information will contribute to "public understanding," that is, "the understanding of a reasonably broad audience of persons interested in the subject"; and (iv) whether disclosure is likely to contribute "significantly" to public understanding of government operations or activities. *See* 6 C.F.R. § 5.11(k)(2)(i)– (iv). Each of these considerations is satisfied here.

Each of these considerations is satisfied here. First, the records requested pertain directly to "operations or activities" of the federal government: specifically, how the agency conducts health surveillance and data analytics during the COVID-19 pandemic. Second, this request is "likely to contribute" to a public understanding of government operations or activities, specifically by helping the public understand the scope, purpose, and cost of various surveillance technologies purportedly used to monitor the COVID-19 pandemic, and to what extent data collected by the government is retained, shared, sold, or repurposed.

Third, disclosure of the requested information will contribute to "understanding of a reasonably broad audience of persons interested in the subject." Requesters Just Futures Law, Media Justice, Mijente, and Immigrant Defense Project will publish responsive records and their analysis through reports, press releases, online posts, newsletters or other media to raise public awareness of the agency's use of surveillance technology during this pandemic. Moreover, requesters will use the records to inform know-your-rights presentations and trainings for the public and attorneys. Using records produced from prior FOIA requests, requesters have published multiple

reports, community resources, and legal advisories on federal and local government agency use of surveillance technologies and other troubling tactics which have reached a broad audience and garnered significant public attention.[20]

Finally, disclosure will contribute "significantly" to the public understanding of the agency's involvement in healthcare surveillance. The federal government's use of technology companies to build a COVID-19 health surveillance system has been the subject of substantial media attention, yet many questions remain unanswered about these technologies and their impact on the public.[21] *See* Attachment A (Congressional Letter). Disclosure of the requested information will help the public and lawmakers answer these pressing questions. The requested records will greatly inform the public debate over the federal government's collection of personal health data in response to the COVID-19 pandemic and its implications on data privacy, security, and civil liberties.

Requesters have thus established, "with reasonable specificity[,] that [their] request pertains to operations of the government," and "the informative value of a request depends not on there being certainty of what the documents will reveal, but rather on the requesting party having explained with reasonable specificity how those documents would increase public knowledge of the functions of the government." *Citizens for Responsibility and Ethics in Washington v. Department of Health and Human Services*, 481 F. Supp. 2d 99, 107– 109 (D.D.C. 2006).

2. Disclosure of the information requested is not in Requesters' commercial interest.

Disclosure of the information requested is not primarily in the commercial interest of requesters Just Futures Law, Media Justice, Mijente Support Committee or Immigrant Defense Project. 6 C.F.R. § 5.11. Any information obtained as a result of this FOIA request will be made available to the public at no cost.

---

[20] *See, e.g., Take Action Now: Fight for Immigrant Justice*, The Nation (May 18, 2020), https://www.thenation.com/article/activism/take-action-now-fight-for-immigrant-justice/ (referencing the Just Futures Law advisory "Surveillance During COVID-19 to learn how governments and companies arousing the health crisis to expand surveillance); Mijente and Immigrant Defense Project, *Who's Behind ICE? The Tech and Data Companies Fueling Deportations* (2018), https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations_v3-.pdf; https://mediajustice.org/resource/no-more-shackles-report/*; Our Issues,* Media Justice, https://mediajustice.org/issues/; IDP Resources, Immigrant Defense Project, httpe://wwimmigrantdefenseproject/org/resources2. Additionally, Mijente operates the website *No Tech for ICE* which distributes research and raises public awareness around tech industry collaborations with ICE. #NoTechForICE, https://notechforice.com/. Requesters already have a demonstrated record of disseminating and analyzing FOIA records that provide the public including lawmakers and the media a better understanding of troubling government activity. *See, e.g.,* Rachel Frazin, *ICE aimed to arrest at least 8,400 in 2017 planned raid: documents*, The Hill (Jul. 3, 2019), https://thehill.com/latino/451583-ice-aimed-to-arrest-at-least-8400-in-2017-planned-raid-documents; Scott Bixby, *ICE Told Agents 'Happy Hunting!' as They Prepped for Raid*, Daily Beast (Jul. 3, 2019), https://www.thedailybeast.com/ice-told-agents-happy-hunting-as-they-prepped-for-raid; Ali Breland, *ACLU wants FBI records on activists labeled 'black identity extremists'*, The Hill (Oct. 18, 2017), https://thehill.com/policy/national-security/356016-aclu-files-request-for-fbi-to-release-surveillance-documents-of; Immigrant Defense Project, Defend Against ICE Raids and Community Arrests (2017), https://www.immdefense.org/raids/toolkit/ (including documents obtained in the *Immigrant Defense Project et al. v. ICE, et al.* FOIA litigation).

[21] *See supra* fn 15-20; Background section of this request at 1-2.

For these reasons, this request for a full fee waiver should be granted. Alternatively, if the full fee waiver is not granted, Requesters seek all applicable reductions in fees. Further, if no fee waiver is granted and the anticipated costs associated with this request exceed $25.00, please notify requesters to obtain consent and provide an estimate of the additional fees.

Request for Expedited Processing

Requesters are entitled to expedited processing of this request under the FOIA statute and implementing regulations. 5 U.S.C. § 552(a)(6)(E); 6 C.F.R. § 5.5(e)(1)(ii). Specifically, this request is entitled to expedited processing because (1) there is an "urgency to inform the public about an actual or alleged federal government activity" and the request is "made by a person who is primarily engaged in disseminating information" (2) the requested records is a "matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence," and (3) failure to obtain these records on an expedited basis "could reasonably be expected to pose an imminent threat to the life or physical safety of an individual." 6 C.F.R. §§ 5.5(e)(1)(i), (ii), (iv).

1. Requesters are organizations primarily engaged in disseminating information and there is an urgency to inform the public about actual or alleged government activity.

Dissemination of information to the public about actual or alleged government activity is a critical and substantial component of the Requesters' mission and work. The records requested are urgently needed to inform the public about actual or alleged government activity, specifically, federal government's use of powerful technologies to collect vast amounts of personal information for the purported purpose of fighting the COVID-19 pandemic.

The urgency of this information is clear. Federal and state governments and countries across the world have declared the COVID-19 a pandemic and evoked emergency powers. The U.S. government is seeking to work with technology corporations to address this public health crisis. Technology companies such as Palantir Technologies, Facebook, and Google have confirmed that they have been in conversation with the government to build health surveillance systems or source location data.[22] But lawmakers as well as the general public have expressed grave privacy concerns over this health surveillance system and how the government and corporations will expand data collection and data sharing.

2. This Request seeks information on a matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence.

There is overwhelming public concern and attention on the federal government's construction of a national government health surveillance system and its implications on data privacy, security,

[22] Tony Romm, Elizabeth Dwoskin, & Craig Timberg, *U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus*, Wash. Post (Mar. 17, 2020), https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/.

and civil liberties.[23] For example, in March, U.S. Senator Ed Markey raised many of these concerns and questions on health surveillance data collection in a letter to the Whitehouse: "We need assurances that collection and processing of these types of information, even if aggregated and anonymized, do not pose safety and privacy risks to individuals…"[24] Since then, multiple members of Congress have expressed similar concerns and even introduced a bill to curtail healthcare surveillance during the COVID-19 pandemic.[25] *See* Attachment A.

3. Failure to obtain these records on an expedited basis "could reasonably be expected to pose an imminent threat to the life or physical safety of an individual."

As our privacy laws recognize, healthcare information is one of the most sensitive types of personal data.[26] Disclosure of an individual's medical information, diagnostic tests, and related personal identifying information could seriously impact a person's physical safety and deter individuals from seeking medical treatment particularly at a critical time in this public health crisis. For example, the unmasking of individuals with COVID-19 disease has led to harassment, stigma, and public shaming.[27] Moreover, there are concerns that the federal government may use data originally collected for COVID-19 health surveillance for other purposes such as arresting individuals and separating families for civil immigration enforcement.[28] DHS has already stated

---

[23] Bajak, *supra* fn 16; *supra* 21; Byron Tau, *Government Tracking How People Move Around in Coronavirus Pandemic*, Wall Street Journal (Mar. 29, 2020), https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202; *US government is tracking Americans' cell phones to see how they move and spread coronavirus during the pandemic,* Daily Mail, *(*Mar. 29, 2020), https://www.dailymail.co.uk/news/article-8164301/Government-tracking-Americans-cell-phones-spread-coronavirus.html; Tyler Sonnemaker, *Secretive big data company Palantir is reportedly providing software to help the CDC track the coronavirus pandemic, even as critics slam its work with ICE*, Business Insider (Mar. 27, 2020), https://www.businessinsider.com/palantir-providing-cdc-with-coronavirus-tracking-software-report-2020-3; Natasha Singer & Choe Sang-Hun, *As Coronavirus Surveillance Escalates*, *Personal Privacy Plummets*, N.Y. Times, (Mar 23, 2020) (updated Apr. 17, 2020), https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

[24] Press Release, Senator Ed Markey, Senator Markey Statement on Reported White House National Coronavirus Surveillance System (Apr. 8, 2020), https://www.markey.senate.gov/news/press-releases/senator-markey-statement-on-reported-white-house-national-coronavirus-surveillance-system.

[25] Letter from Congresswoman Anna G. Eshoo, Congresswoman Suzan K. DelBene, & Senator Ron Wyden to President Donald Trump & Vice President Mike Pence (Mar. 19, 2020), https://eshoo.house.gov/sites/eshoo.house.gov/files/documents/Eshoo-Wyden-DelBene%20-%20Letter%20to%20Pres%20%26%20VP%20about%20coronavirus%20privacy%20-%203.19.20.pdf.

[26] Existing HIPAA laws require that healthcare facilities limit the disclosure of personal identifying information to the minimum necessary to lessen the spread of the disease. It also requires that the use of the information be restricted to a public health purpose. U.S. Department of Health and Human Services, *COVID-19 and HIPAA: Disclosures to law enforcement, paramedics, other first responders and public health authorities*, https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf.

[27] *See* Singer & Sang-Hun, *supra* fn 26; Kim, *supra* fn 7.

[28] Mona Sloane & Albert Fox Cahn, *Today's COVID-19 Data Will be Tomorrow's Tools of Oppression*, Daily Beast (Apr. 2, 2020), https://www.thedailybeast.com/todays-covid-19-data-will-be-tomorrows-tools-of-oppression. Moreover, DHS has already confirmed that it purchases mobile location data for immigration enforcement purposes. Marty Johnson, *DHS accessing cellphone database for immigration enforcement: report*, The Hill (Feb. 7, 2020), https://thehill.com/homenews/administration/482036-homeland-security-accessing-cell-phone-database-for-immigration.

that seeking some forms of public health assistance could harm an individual's immigration status.[29] Such use and misuse of data would certainly impact a person's physical safety.

In submitting this request for expedited processing, requesters certify that this explanation is true and correct to the best of its knowledge and belief. 5 U.S.C. § 552(a)(6)(E)(vi).

Conclusion

Thank you for your consideration of this request. We look forward to your response to our request for expedited processing within ten (10) business days, as required under 5 U.S.C. § 552(a)(6)(E)(ii)(I). Notwithstanding our request for expedited processing, we alternatively look forward to your reply to this request within twenty (20) business days, as required under 5 U.S.C. § 552(a)(6)(A)(I). If the Request is denied in whole or in part, we ask that you justify all withholdings by reference to specific exemptions to the FOIA. We also ask that you release all segregable portions of otherwise exempt material.

We request that the records be made available electronically, by e-mail attachment if available or CD-ROM if not.

For questions regarding this request contact Julie Mao at foia@justfutureslaw.org, cc: julie@justfutureslaw.org. Thank you for your consideration.

Yihong "Julie" Mao
Attorney
Just Futures Law
95 Washington Street, Suite 104-149
Canton, MA 02021

Jacinta Gonzalez
Mijente Support Committee

Mizue Aizeki
Immigrant Defense Project

Myaisha Hayes
Media Justice

[29] Camilo Montoya-Galvez, *Citing coronavirus, states urge Supreme Court to reconsider order on "public charge" rule*, CBS News, (Apr. 13, 2020) https://www.cbsnews.com/news/citing-coronavirus-states-urge-supreme-court-to-reconsider-order-on-trumps-public-charge-rule/.

ATTACHMENT A

Congress of the United States
Washington, DC 20515

March 19, 2020

The Honorable Donald J. Trump,
President
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

The Honorable Mike Pence,
Vice President
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dear President Trump and Vice President Pence,

As you work with technology companies and other private sector actors in coordinating our country's responses to the COVID-19 pandemic, we urge you to protect the privacy of Americans at every step. An unprecedented crisis of this magnitude calls for an all-of-society response, including partnering with the private sector, to protect the health of Americans, but we must not lose sight of the civil liberties that serve as the foundation of our country.

Press reports indicate that members of your Administration are in active discussions with Facebook, Google, and other technology companies to use geolocation data captured by smartphones and smartphone apps for public health purposes. This data can be critical for understanding the overall spread of COVID-19 and informing individuals of potential contact with a diagnosed person, as we've seen in South Korea and other countries. However, geolocation data is also extremely sensitive and must not be used for any other purposes.

According to media reports and the President's public remarks, the Administration has partnered with Verily, a subsidiary of Alphabet, to maintain a website for identifying testing locations. While data collected from websites like this can help identify geographic trends, without appropriate controls, information about who receiving testing could be used in discriminatory ways by government agencies (e.g., denying benefits) or companies (e.g., increasing insurance rates) based on whether someone is suspected to have COVID-19.

We support bold measures to keep Americans safe and healthy during this crisis. However, prohibiting government intrusion into the private lives of Americans is, and has always been part of the DNA of our country, enshrined in the Fourth Amendment of our Constitution. Because location and health data are some of the most private types of information about any individual, we urge you to implement procedures to protect the privacy of Americans by adopting the following privacy principles:

1) **Aggregation, Minimization, and Anonymization.** The federal government should only collect data that may be directly useful in responding to the current public health crisis. If appropriate for anticipated uses, the government should limit collection to aggregated data and trends from companies. If aggregated information is insufficient, minimize data to what public health experts identify as necessary. Where practicable, anonymize datasets by removing associated data and metadata unnecessary for the specifically intended public health uses.

2) **Use Limitations**

   a. **Private Company Uses.** The Administration should require that private companies collecting data specific to the COVID-19 crisis, such as information about individuals who are searching for testing centers or information about the disease, must not be able to use such data for any other purpose. The data must not, for example, be combined with behavioral targeting data or be used to train machine learning algorithms to improve advertising.

   b. **Governmental Uses.** Prohibit any government agency or employee from disclosing, transferring, or selling information to agencies, companies or other organizations, or individuals not directly involved with the public health response to COVID-19. Under no circumstances should this data be shared with law enforcement or immigration agencies.

3) **Data Security.** Data should be transferred and stored using the highest cybersecurity protocols.

4) **Prohibiting Reidentification.** Prohibit attempts to reidentify specific individuals from aggregate or anonymized datasets.

5) **Destruction of Data After Pandemic.** Upon conclusion of the pandemic, require all government agencies, employees, and contractors to delete identifiable data. Retaining data beyond the specific crisis creates additional privacy concerns.

In addition to adopting these principles, we ask that you consult leading computer scientists, and privacy and ethics experts in government, academia, and public interest organizations to ensure policies, procedures, and technical standards for collecting, transferring, processing, and retaining data preserve and protect privacy to the greatest extent possible.

Most gratefully,

Anna G. Eshoo
Member of Congress

Ron Wyden
U.S. Senator

Suzan K. DelBene
Member of Congress

cc: The Honorable Alex Azar, Secretary of Health and Human Services