Carmen Chubb, Chief of Staff
Office of Mayor Keisha Lance Bottoms
Atlanta City Hall
55 Trinity Ave SW
Atlanta, GA 30303

*Via E-Mail*

June 11, 2020

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

Dear FOIA Officer:

Pursuant to the Georgia Open Records Act, O.C.G.A. § 50-18-70 *et seq.*, and the implementing regulations of your agency, Just Futures Law, the Georgia Latino Alliance for Human Rights, and Project South seek records from the Office of Mayor Keisha Lance Bottoms (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 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.

---

[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").

[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.

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.[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]

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:

[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), 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/.

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

## 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]
   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;

[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 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.

  l. 911 call data tracking platforms e.g. Carbyne Ltd15, 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.

## 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. 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:

---

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/.

Mayor Keisha Lance Bottoms; Office of the Chief Operating Officer Joshua Williams; Office of the Chief of Staff Carmen Chubb; Chief Health Officer Dr. Angelica Geter Fugerson, and the City's Director of Emergency Preparedness Felipe den Brok.

Key Terms:

1. Protect Now
2. HHS Protect
3. Palantir
4. Google
5. Apple
6. Microsoft
7. Clearview
8. Facebook
9. Amazon
10. IBM
11. "mobile location data"
12. "contact tracing"
13. 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 related to what extent 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[16];
   c. Name of individual, family members, and/or contacts;
   d. Date of birth;
   e. Place of birth;
   f. Citizenship or immigration status;
   g. English as a Second Language, translation or language access needs;
   h. Race or ethnicity;

---

[16] 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.

      i.   Photo;
      j.   Phone number(s); or
      k.  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 agency de-identifies, anonymizes, or aggregates the data. Examples of responsive records include but is 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 (JFL) 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 criminal conduct, including crimes of violence. 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 under COVID-19.

Georgia Latino Alliance for Human Rights (GLAHR) is a statewide, grassroots membership organization founded in 1999 that educates, organizes, and empowers Latinxs in Georgia to defend and advance their civil and human rights. GLAHR is a community-based organization that develops statewide grassroots leadership through outreach to and support for Latinx and immigrant communities by educating the community about state, local, and city government policies and practices. Other GLAHR functions include: leadership training, community organizing for immigrants' rights, know-your-rights presentations, and addressing issues affecting the lives of Georgia's immigrant communities.

Project South is a Southern-based leadership development organization that creates spaces for movement building. We work with communities pushed forward by the struggle– to strengthen leadership and to provide popular political and economic education for personal and social transformation. We build relationships with organizations and networks across the US and global South to inform our local work and to engage in bottom-up movement building for social and economic justice. The Legal & Advocacy program of Project South uses movement lawyering to protect and defend communities of color, Muslims, and immigrant communities.

## Request for Fee Waiver

Requesters further seek a limitation or waiver of processing (search and review) fees. Release of the requested records is in the public interest. Requesters have no commercial interest in the requester records, and will publish responsive records and their analysis through reports, press releases, or other media to raise public awareness of the government's use of surveillance technology during this pandemic. Requesters have published multiple reports on federal and local government agency use of surveillance technologies which have reached a broad audience and garnered significant public attention.[17] Any information obtained as a result of this FOIA request will be made available to the public at no cost.

For these reasons, this request for a full fee waiver should be granted. Should a total waiver be denied, fees should be limited to "a reasonable charge for the search, retrieval, redaction, and production or copying costs for the production of records," utilizing "the most economical means reasonably calculated to identify and produce responsive, nonexcluded documents." O.C.G.A. § 50-18-71(c)(1). If the anticipated costs associated with this Request exceed $25.00, please notify us and provide an estimate within a reasonable period of time.

## Conclusion

Thank you for your consideration of this request. Requesters anticipate your determination on its request within three (3) business days. O.C.G.A. § 50-18-71. If records are unavailable in this timeframe, requesters further expect a description of such records and a timeline for when the records will be available for inspection or copying and provide the responsive records or access thereto as soon as practicable. If the Request is denied in whole or in part, we ask that you justify all withholdings by reference to specific exemptions to the Open Records Act. 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.

/s Yihong "Julie" Mao
Yihong "Julie" Mao
Attorney
Just Futures Law

Georgia Latino Alliance for Human Rights

Project South

[17] *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); *Deportation Defense*, GLAHR, http://glahr.org/deportation-defense/; Project South, Islamophobia & U.S. Surveillance Policy (2019), https://projectsouth.org/wp-content/uploads/2019/08/Islamophobia-and-Surveillance-Fact-Sheet-update082719.pdf.