COVID-19 FOIA Project Reveals That DHS & HHS Used the Pandemic to Expand Tech Surveillance

During the emergence of COVID-19 as a massive threat to the health and safety of people around the world, federal agencies under the Trump Administration launched dozens of unprecedented programs, many of which used the threat of the pandemic to cover separate, more nefarious goals. In addition to **blocking asylum seekers** from reaching the United States and **fast-tracking deportations through Title 42 authority**, federal authorities seized upon the crisis of the pandemic to justify a rapid, broad expansion of surveillance programs.

Through the Covid-19 FOIA project, Just Futures Law, MediaJustice, Mijente Support Committee, Immigrant Defense Project have explored some of the most troubling new changes in "public health surveillance" including by **breaking down the HHS Protect program in a February 2021 fact sheet.** Among the most problematic aspects of HHS Protect was that its technological backbone was built through a massive contract with Palantir, a company responsible for **facilitating many abuses in immigration enforcement and perpetuating racism in policing programs.**

In addition to reporting out public information detailing efforts to expand federal surveillance dragnets, Just Futures Law, along with Mijente, MediaJustice, and the Immigrant Defense Project, filed a series of **Freedom of Information Act Requests** to the Department of Homeland Security (DHS), the Department of Health and Human Services (HHS) — **and following litigation by the Electronic Frontier Foundation** — have uncovered thousands of documents related to the

development of new surveillance technologies under the justification of COVID-19. JFL, in partnership with other state and local partners, has also received documents from municipal governments about local use of these tools through state public records requests.

JFL has **posted** select documents for public research, education and investigation around how the government has used COVID-19 to grow the surveillance dragnet. We include highlights from these documents below.

Key takeaways from the documents received so far include:

1 Contracts for the Development of New Federal Public Health Surveillance Programs Are Sweeping & Have Limited Oversight Mechanisms

The contract for HHS Protect allocates over $7 million dollars to "integrate, manage, and analyze data from the wide, complex array of information sources as identified and authorized by the Government to serve as the data infrastructure backing the national COP for the COVID-19 response. This will enable all key stakeholders from across HHS and its Operating Divisions, including CDC, Federal Government partners, including FEMA, OMB, and approved state and local government partners, and approved private sector partners to readily and proportionally access consumable, up-to-date, accurate, and complete data."[1]

This document sums up the HHS Protect platform and its dangers, including the ingestion of large amounts of personal health data from a multitude of sources without significant attention to information safeguards or use restrictions protocols. Descriptions of the program's objectives also provide for "collaboration across all agencies and teams relevant to the COVID-19 response . . . including **but not limited to** HHS, CDC, ASPR, and state and local public health departments,"[2] creating the potential for data to be shared beyond public health agencies. In

practice, this means that agencies like ICE, local police, and even private actors interested in health data may be eligible to request and receive sensitive data. For an overview of our concerns about HHS Protect misuse, see **HHS Protect: The Expansion of Dragnet Healthcare Surveillance.**

Moreover, Palantir remains central to this sweeping surveillance platform, with an initial award of over $17 million[3] for "a data sharing platform Protect cloud services, Palantir Gotham licenses, to support the HHS Protect Data Sharing Platform to create a modern, scalable, cloud-based, data infrastructure serving the needs of HHS."[4]

2 The Number of Companies Involved in Building Surveillance Technology Platforms with Access to Sensitive Data is Expanding

Documents produced by HHS also show that new **subcontracted companies** are gaining more and more access to health data through their work to build these surveillance systems. The government is contracting with lesser-known vendors like "Synapse IQ" to work on HHS Protect.[5] Other, more well-known companies such as TransUnion also rushed to be involved in pandemic response, claiming that their vast credit reporting database could be used to verify identities when combined with healthcare data.[6] These are some of the same companies which sell data aggregation and consumer information to law enforcement with harmful consequences. **See The Data Broker to Deportation Pipeline: How Thomson Reuters and LexisNexis Share Utility and Commercial Data with ICE**. Combining two sources of highly sensitive data — healthcare records with consumer behavior — creates even greater dangers.

In addition, companies that win bids to collect and analyze health data for the pandemic response escape accountability for access and potential disclosure of any government-provided data through legal exceptions created specifically for COVID-19 surveillance projects. For example, Synapse IQ's RFP Response specifies that "[t]o the extent that [Public Health information] is provided under this contract, or any modifications or extensions thereto, HHS Notification of Enforcement Discretion under HIPAA to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19, No. 4153-01-P is applicable."[7] In other words, HHS has created a potential exemption from liability for companies handling and sharing sensitive health data. Combined with already limited public knowledge or oversight of these programs, sweeping language limiting applicability of privacy protection laws such as HIPAA creates a frightening level of leeway for errors and misuse of information by private contractors.

3 Palantir is Deeply Embedded in ICE with Intimate Access to Officials

We have known for years that Palantir — in spite of its deep flaws and harmful products — has a close relationship with ICE. The FOIA documents have revealed new information about just how much contact this company has with high level officials. For example, in one email document, a Palantir Executive suggests that they should have monthly meetings with a high-ranking ICE Homeland Security Investigations official.[8] The purpose of these meetings is to demonstrate and explain the progress of several surveillance technologies — including FALCON, "ICM," and "Gaia" — Palantir is embedding into government operations.[9]

4 Technology Companies Seeking Access to Government Contracts Are Promising Expansive, Targeted Forms of Surveillance of Individuals as Features of Public Health Surveillance Programs

Technology companies are **scrambling to obtain millions of dollars in federal government funds to target, harass, and arrest immigrants**. Documents in the COVID-19 FOIA show that, even at the state and local level, companies are making frightening promises about how invasive they can be in surveilling individuals through health-oriented monitoring systems. For example, in one document, IBM offered New York authorities the chance to monitor **all Medicaid recipients**, including by using home addresses and hospital records to geolocate individuals for COVID surveillance.[10]

These documents show the ways that health surveillance is not only saturated and disturbingly granular, but it is a growing industry that is constantly presenting new threats to the privacy, autonomy, and safety of our communities.

Our organizations continue to receive new documents from government agencies. To learn more about the documents uncovered through FOIA, please visit our COVID-19 FOIA Project:

https://justfutureslaw.org/covid-19-foia-project/

Endnotes

1 HHS-OCIO Protect Data Platform, Section 1.6.3, Detailed Objectives And Target Outcomes of the Protect Platform.
https://justfutureslaw.org/wp-content/uploads/2022/04/PROTECT-project-description.pdf

2 Id.

3 HHS Contract with Palantir, Section 1.3, Commercial Items.
https://justfutureslaw.org/wp-content/uploads/2022/04/HHS-Protect-__-Palantir.pdf

4 HHS Contract with Palantir, Section 1.1, Brief Description of Services.

5 Synapse IQ, RFP Response, Section C - Statement of Work, p. 1.
https://justfutureslaw.org/wp-content/uploads/2022/04/Synapse-IQ.pdf

6 Email from James Bohnsack, Chief Revenue & Strategy Officer - Healthcare, TransUnion, to Donald Rucker, former National Coordinator for Health Information Technology, HHS (April 26, 2020, 11:24 AM).
https://justfutureslaw.org/wp-content/uploads/2022/04/Transunion-Bid.pdf

7 Synapse IQ, RFP Response, Section C - Statement of Work, p. 5.

8 Email from Executive, Palantir Technologies, to Official, Homeland Security Investigations (HSI), Immigration and Customs Enforcement (ICE) (April 17, 2020, 17:20 ET).
https://justfutureslaw.org/wp-content/uploads/2022/04/HSI-Palantir-Exchange.pdf

9 Email from Executive, Palantir Technologies, to Official, Homeland Security Investigations (HSI), Immigration and Customs Enforcement (ICE) (April 24, 2020, 05:48 ET).
https://justfutureslaw.org/wp-content/uploads/2022/04/HSI-Palantir-Exchange.pdf

10 Email from Kevin Murphy, Watson Health, IBM, to Paul Francis, former Deputy Secretary for Health and Human Services, Governor of New York (March 31, 2020, 15:31 ET),
https://justfutureslaw.org/wp-content/uploads/2022/04/IBM-FOIA-Promises.pdf