GlobalResearch
Center for Research on Globalization

Biometric Police State? DHS Plans to Start Collecting Eye Scans and DNA — With the Help of Defense Contractors

As the agency plans to collect more biometrics, including from U.S. citizens, Northrop Grumman is helping build the infrastructure.

By Felipe De La Hoz
Global Research, November 23, 2020
The Intercept 18 November 2020

Region: USA
Theme: Intelligence, Police State & Civil Rights

Through a little-discussed potential bureaucratic rule change, the Department of Homeland Security is planning to collect unprecedented levels of biometric information from immigration applicants and their sponsors — including U.S. citizens. While some types of applicants have long been required to submit photographs and fingerprints, a rule currently under consideration would require practically everyone applying for any kind of status, or detained by immigration enforcement agents, to provide iris scans, voiceprints and palmprints, and, in some cases, DNA samples. A tangled web of defense and surveillance contractors, which operate with little public oversight, have already begun to build the infrastructure that would be needed to store these records.

After proposing the rule in September, DHS is currently reviewing, and must respond to, thousands of comments it received during the 30-day period in which the public could weigh in. The agency had signaled that the proposal would be coming when it announced last year that it would be retiring its legacy Automated Biometric Identification System, or IDENT, and replacing it with the Homeland Advanced Recognition Technology framework — stating explicitly that one of its objectives was to collect more types of biometric data and make searching and matching easier. Where HART was the vessel, the new proposed rule is the means of collecting all the new data types to populate it.

Any potential contractors tasked with rolling out the new data collection infrastructure and management won't be decided until after the rule is finalized, but a look at the companies currently working on building out DHS's already vast biometrics capabilities is instructive.

The contract for the current biometrics management system used by the U.S. Citizenship and Immigration Services, or USCIS, for case processing, background checks, and identity verification was awarded in 2015 to the relatively large but low-profile federal contractor Pyramid Systems, which is based in Fairfax, Virginia. Run by a Taiwanese immigrant couple who are Democratic donors, Pyramid has been contracted by the Department of Housing and Urban Development, the Securities and Exchange Commission, the Centers for Medicare & Medicaid Services, the Census Bureau, and other agencies. In a 2016 release about the contract, which is potentially worth up to $87.5 million, the company wrote that it would "provide Agile services for enhancement and operations and maintenance (O&M) of current biometrics applications used for U.S. immigration-related efforts," using jargon for a software development methodology focused on constantly evolving to changing

circumstances and a client's needs.

Defense giant BAE Systems has a $47 million contract for USCIS biometrics support and collection, which appears to involve the mechanics of actually taking fingerprints and photographs. The technical infrastructure for the processing, searching, matching, and maintenance of the first couple of components of HART are being built by Northrop Grumman through a contract potentially worth $143 million.

These international defense conglomerates have, over the years, amassed tens of thousands of U.S. government contracts worth tens of billions of dollars, including hundreds with DHS alone, for everything from software to weapons. These partnerships between defense contractors and DHS — a sprawling agency created after 9/11 — form the backbone of a decadeslong melding of the war on terror with the war on drugs, and the expansion of an all-encompassing national security state whose reach extends inside and outside the country. BAE Systems and Pyramid Systems did not respond to requests for comment; Northrop Grumman referred questions to DHS, which responded to detailed questions by pointing back to its press release.

DHS's data collection operations are also aided by its contracts with the surveillance state. HART, like much of the federal government's data infrastructure, is hosted on Amazon Web Services; Amazon has made itself indispensable as its lobbying machine simultaneously pushes anti-labor, pro-surveillance, and pro-monopolization policy. The controversial facial recognition firm Clearview AI — which built its software by trawling social media and the web for billions of images to scrape — already has an active contract with Immigrations and Customs Enforcement, which, as a component of DHS, could easily match those images against the HART database. Palantir, the data-mining firm founded by billionaire Peter Thiel whose software uses data from various databases to form detailed relationship maps and establish connections between individuals, also has a contract with ICE.

That nongovernmental entities with commercial incentives and fewer limits on data use would have access to so much personal data is alarming to privacy watchdogs.

> "It has a private prison feel. When you start contracting out that stuff to the private sector, the private sector will never care about rights," said Paromita Shah, executive director of Just Futures Law.

In October, several Democratic senators called on the Trump administration to reverse course on its expansion of biometric data collection.

> "This proposed rule by the Department of Homeland Security should send chills down the spines of every American who doesn't want to live under big brother-style government surveillance," Oregon Sen. Jeff Merkley, one of the letter's signatories, said in a statement to The Intercept. "It's disturbing that the Trump administration is trying to inch us closer to that slippery slope and further intimidate our immigrant communities. We have to keep fighting tooth and nail to bolster biometric data privacy rights and oppose dangerous and misguided data collection policies like this one."

The Trump administration has not issued a timeline for when it will finish reviewing public comments. If that should happen before Joe Biden's inauguration in January, the new

administration would have to go through a regulatory process to roll it back. If not, Biden's DHS could decide not to move forward with implementing the rule. But it's far from certain that it would. While the president-elect has promised to roll back some unpopular Trump-era immigration policies, like the travel ban, the expansion of the surveillance state has long been a point of bipartisan consensus. The Biden transition team did not respond to a request for comment.

The proposed rule represents a significant departure from current practices, where only certain applicants for visas, residency, and naturalization must submit photographs and fingerprints. Under the new regime, practically everyone presenting an application with USCIS, and their U.S. resident or citizen sponsors, will be expected to provide iris scans, voiceprints — which can be used to identify an individual by the sound and tenor of their voice alone — palmprints, and DNA in cases where they are attempting to prove a genetic relationship. As written, it leaves the door open for adding an unlimited amount of other characteristics without further public discussion, including "behavioral characteristics" such as gait recognition.

While DHS and its component agencies have long had congressional authority to collect DNA from immigrants in their custody, it was not until this year that ICE and Customs and Border Protection began to do so. The proposed rule goes a step further, mandating additional types of detainee data collection for the first time, as well as for the first time DNA from nondetained applicants.

USCIS would be able to collect biometrics from all visitors to the U.S., as well as from all immigrants at any point up until they become a naturalized citizen, for which the shortest, widely available path — marrying a U.S. citizen — can take four or five years when factoring in processing times. Some people on work visas can reside in the country legally for decades without the option to obtain residency and subsequent citizenship. Even U.S. citizens could be forced to provide biometric data if, for example, they sponsor the application of a family member or if their prior naturalization application is reopened.

While other government entities, like the Department of Justice, also collect biometrics, DHS is known as a uniquely opaque and privacy-adverse domestic law enforcement and surveillance apparatus. Its culture disdains privacy, perhaps best exemplified by reports that former DHS Chief Privacy Officer **Mary Ellen Callahan**, whose job included overseeing the department's compliance with widely accepted standards known as Fair Information Practice Principles, or FIPPs, was called a "terrorist" by others within the department.

The Justice Department's biometrics database, for example, is strictly controlled by a number of internal privacy guidelines, including a limited number of purposes for which it can be accessed. HART has far fewer protections. DHS wants its database to be as big as the Justice Department's, said Shah, "but no one cares about who has access to it, who is it being shared with, can people have access to their own data. They're not asking those questions."

A former USCIS asylum officer who asked not to be named because she still works in the U.S. immigration sphere said, "It's sort of an open joke that it's a mystery" who has access to what kind of data. "It's like a black hole."

Access concerns are compounded by not just what the data is, but how it's organized in the system. When the FBI stores DNA in its CODIS database, the information is stored without

names or other identifying characteristics. For its part, DHS intends to use DNA for the purposes of establishing genetic relationships, meaning that the DNA would be stored with biographic information with linkages between individuals.

The proposed rule would also allow for the DNA to be used "as authorized by the immigration and naturalization laws," a vague clause that has privacy advocates worried.

> "Once you start collecting that information from people, it's pretty easy to start mapping out whole immigrant communities," said Jennifer Lynch, the surveillance litigation director at the Electronic Frontier Foundation.

While DHS currently only requests biometrics from adults, the proposed rule would eliminate age constraints, meaning minors — incapable of giving consent — will be caught in the dragnet of invasive surveillance. Pam Dixon, executive director of the World Privacy Forum, said that would be unethical and counterfactual, citing research that has shown that biometric identification is wildly inaccurate for young children.

> "It's fact-free. It's science-free. It's just, 'Here's what we want, and we're gonna get it, and we're going to explain it away by saying the words identity theft and fraud and terrorism.' That's what this is," said Dixon.

DHS's own privacy assessment of HART flags the possibility that the data could be inadvertently released, stating that as of the initial rollout, there was no security plan in place to prevent leaks and that a number of different contractors would have direct access to HART data.

Privacy advocates worry that DHS won't do enough to ensure that there will be limited access and usage for the data, for government employees and contractors alike.

> "There's just no central place where you can find information on what the regulations are for access to various databases, what the restrictions are, and how data's been shared," said EFF's Lynch.

The government is required to provide disclosures as to how the data can be used and accessed, but, much like political dark money run through webs of impenetrable LLCs, the trick is to create a tangled mess of usage permissions and exemptions that is ultimately indecipherable. So a database might have certain privacy restrictions, but can be accessed by another government agency with a different set of restrictions, which in turn is part of a larger contractor-run analytic framework, and so on and so forth.

Despite DHS's policy of adherence to the FIPPS, it is often up to its individual agencies to ensure contractors' compliance. On that front, there's already plenty of cause for concern. In a report published this September, the Government Accountability Office concluded that, since CBP had first started using facial recognition for identity verification for air and sea travel in 2017, it "had audited only one of its more than 20 commercial airline partners and did not have a plan to ensure that all partners are audited for compliance with the program's privacy requirements."

The GAO hasn't conducted an evaluation of the new rule, Rebecca Gambler, the director of

the GAO's Homeland Security and Justice division, told The Intercept. Still, Gambler said that as CBP expands its facial recognition program, "those privacy risks are just going to continue to grow." She emphasized that CBP agreed to a set of recommendations in the report and has appeared to try to implement them; yet these reforms seem to have come about as a result of direct urging.

In mid-November, Homeland Security issued another proposed biometrics rule, dealing with the CBP's long-planned rollout of a system to run facial recognition on everyone entering or leaving the country. While there have been pilot programs for the congressionally mandated scheme for some time, with the entry portion of the project almost fully implemented, the new rules would require effectively every noncitizen to be photographed both when arriving in and departing the United States. U.S. citizens would technically be allowed to opt out, but in practice they haven't always been able to do so even under the current rules. Over 180,000 of the very same images taken as part of this process have also already been leaked by the breach of a CBP contractor's system. The rule is undergoing a short public comment period slated to end on December 21.

While the stated goal of the biometrics collection is identity verification and a biometric collection, there are few constraints on the use of the data, which can be shared with a host of different law enforcement agencies and governments. The rule's ill-defined continuous vetting program could effectively mean an endless parade of invisible checkpoints for those whose information is collected, like an always-on no-fly list that could unexpectedly trigger enormous consequences, with little chance of recourse.

Privacy advocates worry that a system now focused on immigrants and their family members could eventually be expanded to the broader public. "There's no basis in history for being sanguine about the idea that once these things are trialed on foreigners, who have few legal rights anyway, and where the American public won't complain," said Edward Hasbrouck, a travel and privacy expert, "that they will then become the new normal for U.S. citizens as well."

Update: Nov. 19, 2020
This article has been updated to include information about a new CBP biometrics rule proposed by DHS after publication.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Hoz