GlobalResearch
Center for Research on Globalization

HART: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' "Non-Obvious Relationships"

By Jennifer Lynch
Global Research, January 20, 2021
Electronic Frontier Foundation 7 June 2018

Region: USA
Theme: Intelligence

This article was originally published on EFF in June 2018.

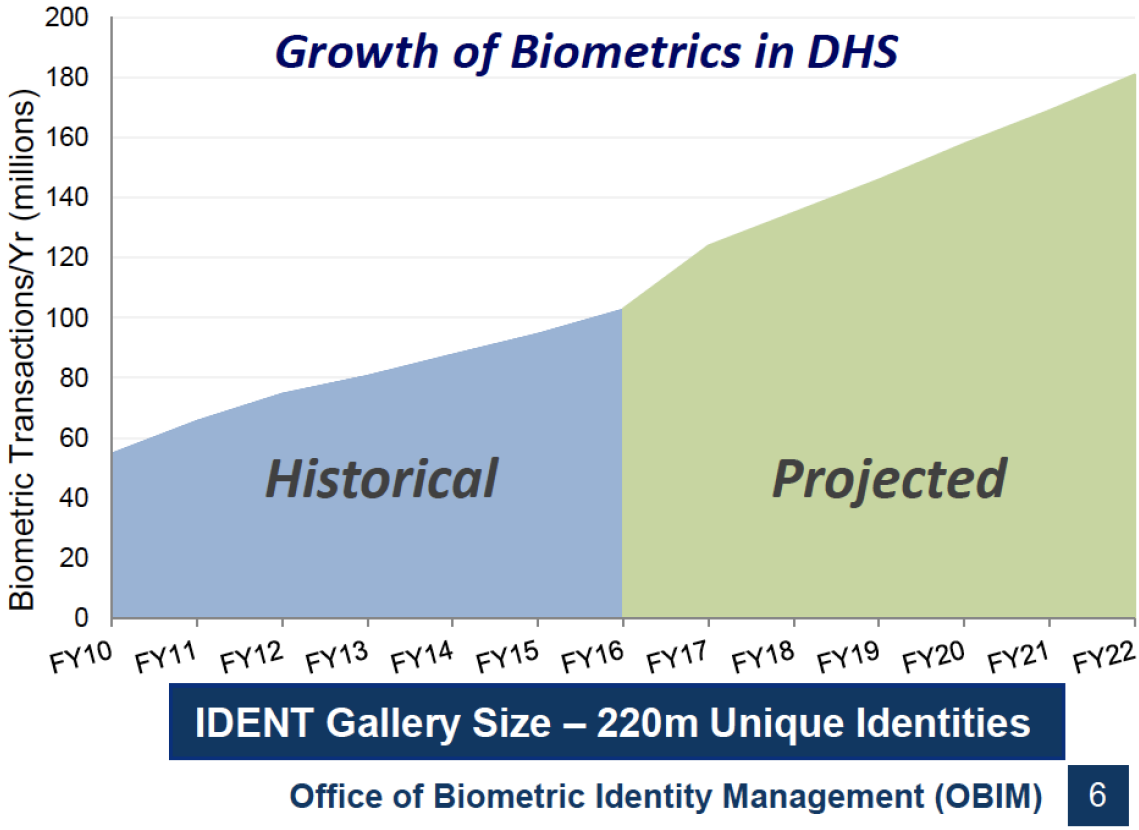
So why do we know so little about it?

The U.S. Department of Homeland Security (DHS) is quietly building what will likely become the largest database of biometric and biographic data on citizens and foreigners in the United States. The agency's new Homeland Advanced Recognition Technology (HART) database will include multiple forms of biometrics—from face recognition to DNA, data from questionable sources, and highly personal data on innocent people. It will be shared with federal agencies outside of DHS as well as state and local law enforcement and foreign governments. And yet, we still know very little about it.

The records DHS plans to include in HART will chill and deter people from exercising their First Amendment protected rights to speak, assemble, and associate. Data like face recognition makes it possible to identify and track people in real time, including at lawful political protests and other gatherings. Other data DHS is planning to collect—including information about people's "relationship patterns" and from officer "encounters" with the public—can be used to identify political affiliations, religious activities, and familial and friendly relationships. These data points are also frequently colored by conjecture and bias.

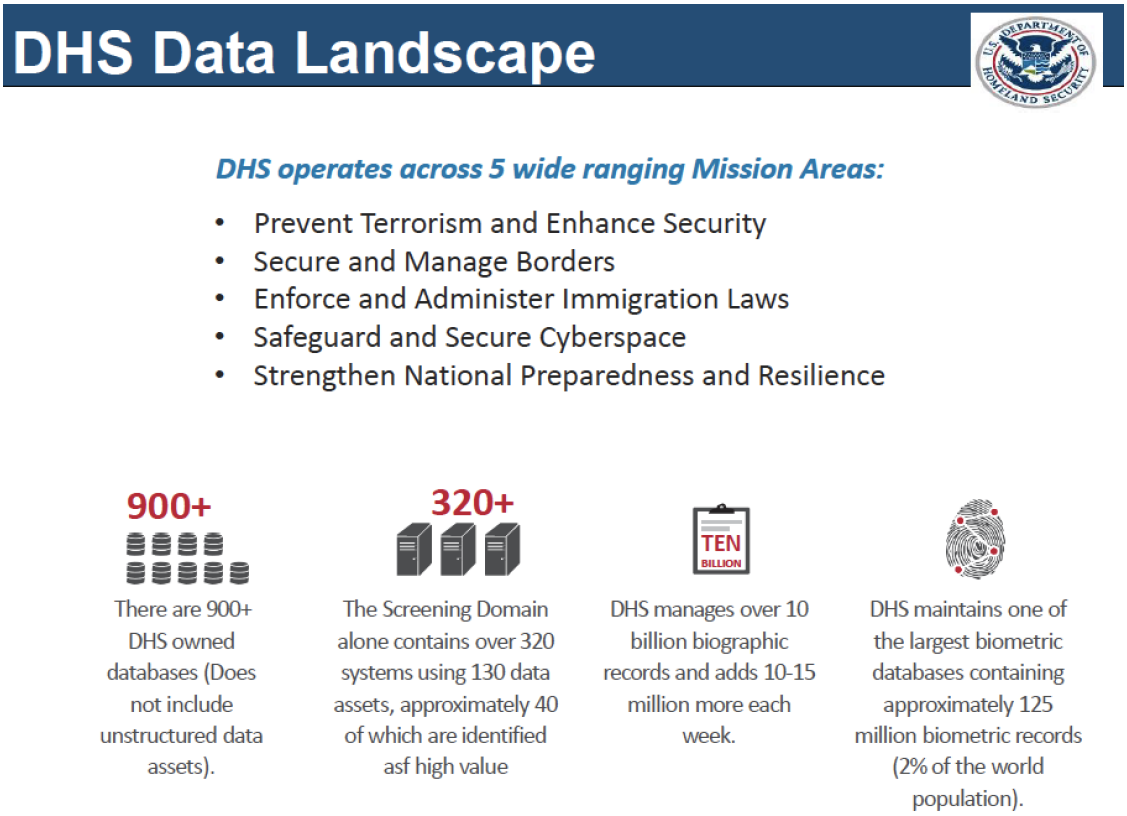
In late May, EFF filed comments criticizing DHS's plans to collect, store, and share biometric and biographic records it receives from external agencies and to exempt this information from the federal Privacy Act. These newly-designated "External Biometric Records" (EBRs) will be integral to DHS's bigger plans to build out HART. As we told the agency in our comments, DHS must do more to minimize the threats to privacy and civil liberties posed by this vast new trove of highly sensitive personal data.

DHS Biometrics Systems—From IDENT to HART



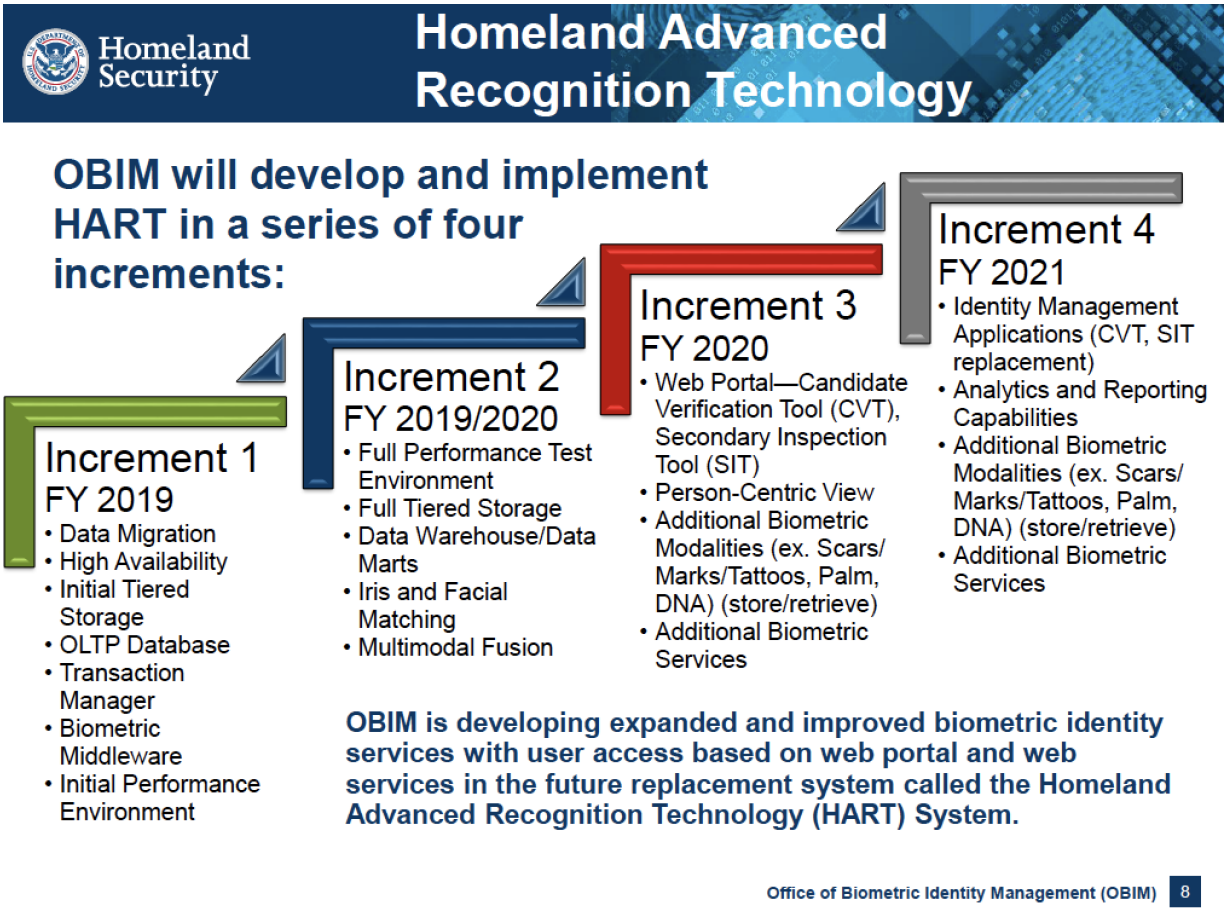
DHS slide showing growth of its legacy IDENT biometric database

DHS currently collects a lot of data. Its legacy IDENT fingerprint database contains information on 220-million unique individuals and processes 350,000 fingerprint transactions every day. This is an exponential increase from 20 years ago when IDENT only contained information on 1.8-million people. Between IDENT and other DHS-managed databases, the agency manages over 10-billion biographic records and adds 10-15 million more each week.



DHS slide showing breadth of DHS biometric and biographic data

DHS's new HART database will allow the agency to vastly expand the types of records it can collect and store. HART will support at least seven types of biometric identifiers, including face and voice data, DNA, scars and tattoos, and a blanket category for "other modalities." It will also include biographic information, like name, date of birth, physical descriptors, country of origin, and government ID numbers. And it will include data we know to by highly subjective, including information collected from officer "encounters" with the public and information about people's "relationship patterns."



DHS slide showing expansion of its new HART biometric and biographic database

HART will Impinge on First Amendment Rights

DHS plans to include records in HART that will chill speech and deter people from associating with others.

DHS's face recognition roll-out is especially concerning. The agency uses mobile biometric devices that can identify faces and capture face data in the field, allowing its ICE (immigration) and CBP (customs) officers to scan everyone with whom they come into contact, whether or not those people are suspected of any criminal activity or an immigration violation. DHS is also partnering with airlines and other third parties to collect face images from travelers entering and leaving the U.S. When combined with data from other government agencies, these troubling collection practices will allow DHS to build a database large enough to identify and track all people in public places, without their knowledge—not just in places the agency oversees, like airports, but anywhere there are cameras.

Police abuse of facial recognition technology is not a theoretical issue: it's happening today. Law enforcement has already used face recognition on public streets and at political protests. During the protests surrounding the death of Freddie Gray in 2015, Baltimore Police ran social media photos against a face recognition database to identify protesters and arrest them. Recent Amazon promotional videos encourage police agencies to acquire that company's face "Rekognition" capabilities and use them with body cameras and smart cameras to track people throughout cities. At least two U.S. cities are already using Rekognition.

DHS compounds face recognition's threat to anonymity and free speech by planning to include "records related to the analysis of relationship patternsamong individuals." We don't know where DHS or its external partners will be getting these "relationship pattern" records, but they could come from social media profiles and posts, which the government plans to track by collecting social media user names from all foreign travelers entering the country.

Social media records, even if they are publicly available, can include highly personal and private information, and the fear that the government may be collecting and searching through this information may cause people to self-censor what they say online. The data collected also won't be limited to information about foreign travelers—travelers' social media records may include information on family members and friends who are U.S. citizens or lawful permanent residents, two groups protected explicitly by the Privacy Act. As the recent, repeated Facebook scandals are showing us, even when you think you have done everything you can to protect your own data, it could easily be disclosed without your control through the actions of your friends and contacts or Facebook itself.

DHS's "relationship pattern" records will likely be misleading or inaccurate. DHS acknowledges that these records will include "non-obvious relationships." However, if the relationships are "non-obvious," one has to question whether they truly exist. Instead, DHS could be seeing connections among people that are based on nothing more than "liking" the same news article, using the same foreign words, or following the same organization on social media. This is highly problematic because records like these frequently inform officer decisions to stop, search, and arrest people.

DHS plans to include additional records in HART that could be based on or impact First Amendment protected speech and activity. Records will include "miscellaneous officer comment information" and "encounter data." These types of information come from police interactions with civilians, and are often collected under extremely questionable legal circumstances. For example, ICE officers use mobile devices to collect biometric and biographic data from people they "encounter" in the field, including via unauthorized entry into people's homes and Bible study groups, and in public places where people congregate with other members of their community, such as on soccer fields, in community centers, and on buses. "Encounters" like these, whether they are conducted by ICE or by state or local police, are frequently not based on individualized suspicion that a civilian has done anything wrong, but that doesn't prevent the officer from stockpiling any information obtained from the civilian during the encounter.

Finally, DHS relies on data from gang databases (its own and those from states), which often contain unsubstantiated data concerning people's status and associations and are notoriously inaccurate. DHS has even fabricated gang status as an excuse to deport people.

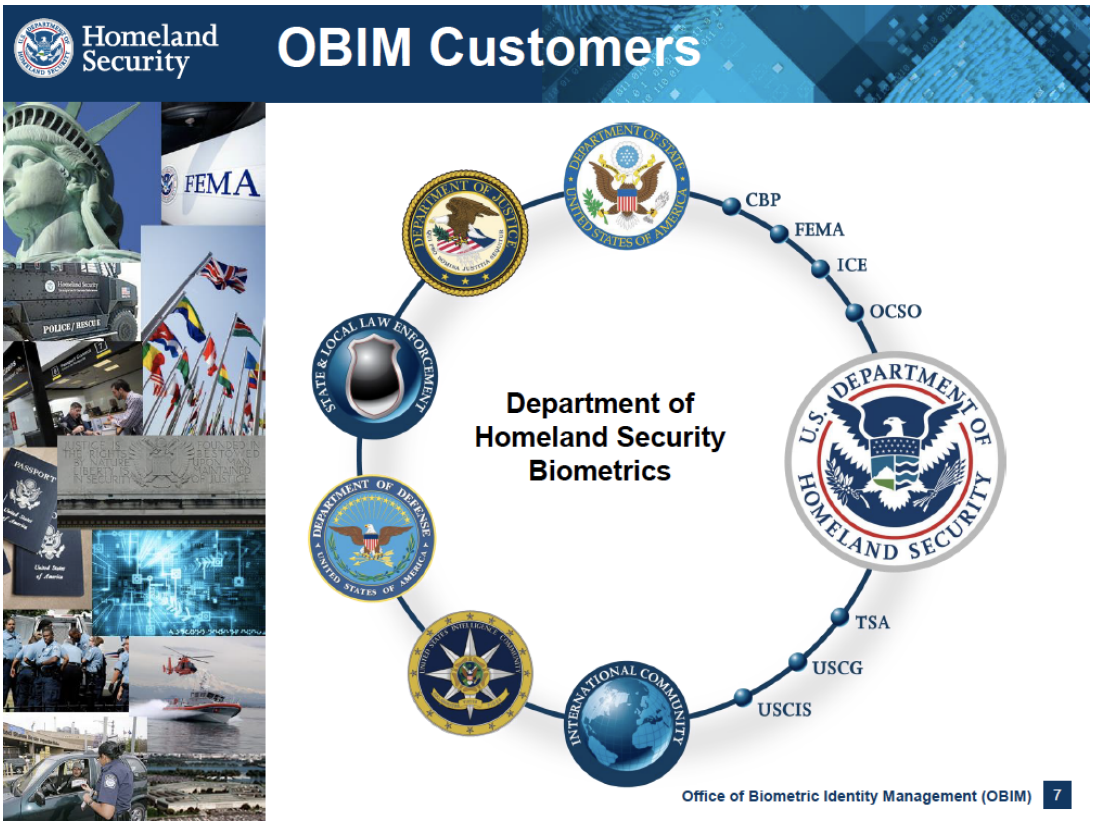
HART Will Include Inaccurate Data and Will Share that Data with Other Agencies

DHS is not taking necessary steps with its new HART database to determine whether its own data and the data collected from its external partners are sufficiently accurate to prevent innocent people from being identified as criminal suspects, immigration law violators, or terrorists.

DHS has stated that it intends to rely on face recognition to identify data subjects across a variety of its mission areas, and "face matching" is one of the first components of the HART database to be built out. However, face recognition frequently is an inaccurate and

unreliable biometric identifier. DHS's tests of its own systems found significantly high levels of inaccuracy—the systems falsely rejected as many as 1 in 25 travelers. As a Georgetown report recently noted, "DHS' error-prone face scanning system could cause 1,632 passengers to be wrongfully delayed or denied boarding every day at New York's John F. Kennedy (JFK) International Airport alone."

DHS's external partners are also employing face recognition systems with high rates of inaccuracy. For example, FBI has admitted that its Next Generation Identification database "may not be sufficiently reliable to accurately locate other photos of the same identity, resulting in an increased percentage of misidentifications." Potential foreign partners such as police departments in the United Kingdom use face recognition systems with false positive rates as high as a 98%—meaning that for every 100 people identified as suspects, 98 in fact were not suspects.



DHS Slide Showing Partner Agencies

People of color and immigrants will shoulder much more of the burden of these misidentifications. For example, people of color are disproportionately represented in criminal and immigration databases, due to the unfair legacy of discrimination in our criminal justice and immigration systems. Moreover, FBI and MIT research has shown that current face recognition systems misidentify people of color and women at higher rates than whites and men, and the number of mistaken IDs increases for people with darker skin tones. False positives represent real people who may erroneously become suspects in a law enforcement or immigration investigation. This is true even if a face recognition system offers several results for a search instead of one; each of the people identified could be detained or brought in for questioning, even if there is nothing else linking them to a crime or violation.

In addition to accuracy problems inherent in face recognition, DHS's own immigration data

has also been shown to be unacceptably inaccurate. A 2005 Migration Policy Institute study analyzing records obtained through FOIA found "42% of NCIC immigration hits in response to police queries were 'false positives' where DHS was unable to confirm that the individual was an actual immigration violator." A 2011 study of DHS's Secure Communities program found approximately 3,600 United States citizens were improperly caught up in the program due to incorrect immigration records. As these inaccurate records are propagated throughout DHS's partner agencies' systems, it will become impossible to determine the source of the inaccuracy and correct the data.

HART Is Fatally Flawed and Must Be Stopped

DHS's plans for future data collection and use should make us all very worried. For example, despite pushback from EFF, Georgetown, ACLU, and others, DHS believes it's legally authorized to collect and retain face data from millions of U.S. citizens traveling internationally. However, as Georgetown's Center on Privacy and Technology notes, Congress has never authorized face scans of American citizens.

Despite this, DHS plans to roll out its face recognition program to every international flight in the country within the next four years. DHS has stated "the only way for an individual to ensure he or she is not subject to collection of biometric information when traveling internationally is to refrain from traveling."

This is just the tip of the iceberg. CBP Commissioner Kevin McAleenan has stated CBP wants to be able to use biometrics to "confirm the identity of travelers at any point in their travel," not just at entry to or exit from the United States. This includes creating a "biometric pathway" to track all travelers through airports, from check-in, through security, into airport lounges and shops, and onto flights. Given CBP's recent partnerships with airlines and plans to collect social media credentials, this could also mean CBP plans to track travelers from the moment they begin their internet travel research. Several Congress members have introduced legislation to legitimize some of these plans.

Congress has expressed concerns with DHS's biometric programs. Senators Edward Markey and Mike Lee, in a recent letter addressed to the agency, stated, "[w]e are concerned that the use of the program on U.S. citizens remains facially unauthorized[.] . . . We request that DHS stop the expansion of this program and provide Congress with its explicit statutory authority to use and expand a biometric exit program on U.S. citizens." The senators have urged DHS to propose a rulemaking to clarify its plans for biometric exit. Congress also withheld funds last year from DHS's Office of Biometric Identity Management.

DHS's Inspector General criticized the agency last year for failure to properly train its personnel on how biometric systems worked and noted that the agency's reliance on third parties to verify travelers leaving the country "occasionally provided false departure or arrival status on visitors." The OIG is again investigating the biometric exit program this year and plans to "assess whether biometric data collected at pilot locations has improved DHS's ability to verify departures." The Government Accountability Office has also looked into the agency's programs, criticizing the reliability of DHS's data and the agency's failure to evaluate whether a program that collects biometrics from all travelers leaving the country was even feasible.

However, these actions are not enough. DHS needs to end its plans to use its HART database to collect even more biometric and biographic information about U.S. citizens and

foreigners. This system poses a very real threat to First Amendment-protected activities. Further, DHS has a well-documented history of poor data management, and face recognition has a high rate of misidentifications. Congress must step in with more oversight and act now to put the brakes on DHS's broad expansion of data collection.

*

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.

Featured image is from EFF

Articles by: Jennifer Lynch