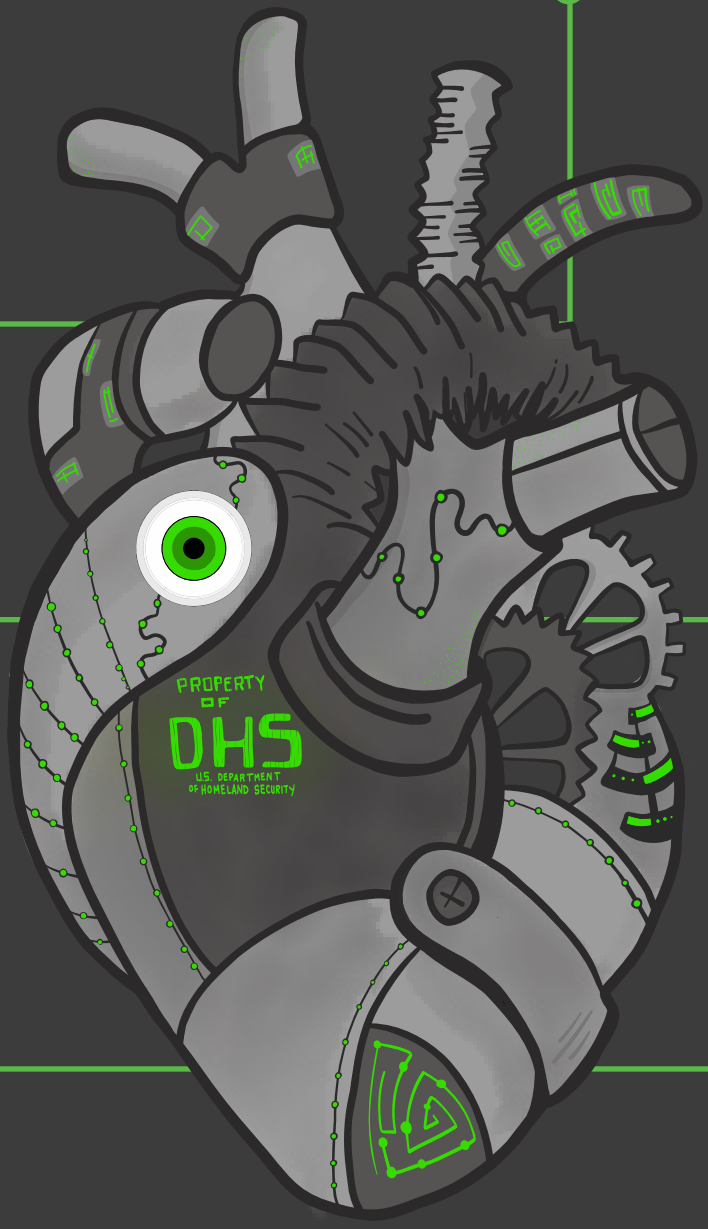


HART Attack

How DHS's massive biometrics database will supercharge surveillance and threaten rights

mijente

JUST FUTURES LAW

IDP IMMIGRANT DEFENSE PROJECT

The Immigrant Defense Project (IDP) works to secure fairness and justice for immigrants in the racially-biased US criminal and immigration systems. IDP's Surveillance, Tech & Immigration Policing project challenges the growing surveillance state, focusing on ICE policing and migrant control, as well as the rapidly expanding role of technology corporations in local governance. The project supports organizing to build the collective knowledge and political infrastructure to end state violence and to grow a just digital future.

Just Futures Law is a transformative legal organization that defends and builds the power of immigrants' rights and criminal justice activists, organizers, and base building community groups working to disrupt and dismantle our deportation and mass incarceration systems.

Mijente is a national organizing hub and political home for Latinx and Chicanx people that's pro-Black, pro-Indigenous, pro-worker, pro-woman, pro-lesbian, gay, bi, trans, and queer, and pro-migrant. It leads the #NoTechForICE campaign, organizing against the surveillance machinery supplied by Silicon Valley for immigration and border policing.

Research Support: Empower, LLC provided critical research and support for this report. Empower LLC conducts strategic corporate research in partnership with civil society organizations to advance human rights and corporate accountability, with a particular focus on technology, private capital, and grave crimes.

Our organizations would like to thank the following for their contributions to this report:

Writers: Mizue Aizeki and Paromita Shah
Editors: Alli Finn, Citlaly Mora Hernandez
Graphic Illustrators: Lucia Sandoval and Deon Eli Reed Jr
Layout: Valeria Mogilevich

May 2022

Table of Contents

1 **Executive Summary**
2 HART presents unacceptable risks and dangers

3 **Introduction**

7 **What is HART?**
10 What will go into HART?
13 What will change when HART comes online?

15 **How Much is HART Projected to Cost?**
18 Congress has raised concerns about HART expenditures

19 **Which Companies are Behind HART?**
20 The corporate players behind HART
23 What other companies could expand HART's reach?

24 **Who Will Use and Access HART?**
26 US federal agencies that will interact with HART
27 What are some of the other databases that will interact with HART?

28 **Why HART Must Be Stopped**
30 HART presents unacceptable threats

38 **Conclusion**

40 **Appendices**
41 Appendix A: HART's Development Increments
42 Appendix B: HART Services in Increment 1
45 Appendix C: Examples of Biometric Collection by DHS Components Under IDENT

Figures
9 Figure 1: OBIM Within DHS Organizational Structure
14 Figure 2: Planned Process Flow Between CBP and HART
16 Figure 3: APB Thresholds Vs. Current Estimate
17 Figure 4: Investment Spending Details
17 Figure 5: HART Schedule
25 Figure 6: DHS Biometrics Sharing Diagram

Executive Summary

The US Department of Homeland Security (DHS) is building a $6.158 billion-dollar, next-wave biometric database that will vastly expand its surveillance capabilities and supercharge the deportation system. The Homeland Advanced Recognition Technology System (HART) will collect, organize, and share invasive data on over 270 million people (including juveniles), with that number projected to grow significantly. This data will come from federal agencies including DHS and the FBI, as well as local and state police, and foreign governments.

Powered by military-grade technologies, HART will aggregate and compare biometrics data including facial recognition, DNA, iris scans, fingerprints, and voice prints—most often gathered without obtaining consent or a warrant. This will allow DHS to target immigrants for surveillance, raids, arrests, detention, and deportation. HART could be used to identify people in public spaces, creating chilling consequences for people's rights to protest, assemble, associate, and to live their daily lives. HART threatens to violate human and privacy rights at an exponential rate, particularly in Black, brown, and immigrant communities already facing discriminatory policing and surveillance.

Despite the terrifying risks, HART remains a black box—shrouded in secrecy with virtually no oversight and accountability mechanisms. Although only in phase one of its development, HART has become vastly more expensive than anticipated—generating massive revenues for first, Northrop Grumman (a military contractor), and now, Veritas Capital (a billionaire private equity firm). While troubling questions over its privacy and human rights violations remain, Congress continues to fund HART, even though it has failed to meet every milestone in its government contract.

Our report explains the dangers of HART by diving into the system's mechanics, costs, and biometric and biographic data sources. We spotlight the companies profiting from HART's development, and the agencies, private companies, and foreign governments that will contribute to and access its data. We outline the short- and long-term civil, privacy, and human rights risks. The underlying role and impact of HART will be to turbocharge DHS' unchecked power—to approve or deny immigration benefits, assemble target lists for ICE raids, expand the tech border wall, and to facilitate surveillance, arrests, immigrant detention and deportation. For such reasons, we call on DHS to dismantle HART. We also call on Congress to freeze funds dedicated to HART as an interim step.

HART presents unacceptable risks and dangers

- HART will **powerfully expand DHS' surveillance capabilities**, enabling ICE, CBP, and other domestic and foreign policing agencies to fuel discriminatory policing and violate the rights of hundreds of millions of people. HART will be especially pernicious for already heavily-surveilled and overpoliced Black and brown communities.
- HART will **harvest and exploit facets of our day-to-day lives**, jeopardizing the rights of political activists and freedom of assembly, and take away our privacy.
- HART will include **invasive personal and biometric data**, which could include unverified information about people's professional roles, religious affiliations, banking information, familial connections and friendships, romantic partnerships, personal activities, political views, travel patterns, and more.
- HART will **weaponize information that people are required to submit to access basic government services**, such as driver's licenses.
- HART's will rely on **untested, racially-biased, and unreliable biometrics**, as well as data from controversial companies like Clearview AI.
- HART will **contain data on juveniles**, including biometrics.
- HART is built on **data collection without consent.**
- DHS **"cannot ensure accuracy"[1] and quality of the data** in HART, since it says it does not own the data—but it will retain and use this data for at least 75 years nonetheless.
- HART is explicitly **designed to shield DHS from scrutiny**, accountability, and consequences for its use of data, even when it violates civil and human rights
- HART's so-called **"redress" measures are effectively non-existent**, leaving people with almost no way to challenge content in the massive database, access their information, and correct errors in their data.

Introduction

In 2016, the Department of Homeland Security (DHS) embarked on a colossal multi-year project to build a next-wave biometric repository and data platform, Homeland Advanced Recognition Technology (HART). Initially projected to cost $4.3 billion, HART's projected cost has since increased to $6.158 billion.[2] Not only does HART promise to be an incredibly powerful weapon for DHS as well as other policing agencies, it has become a lucrative investment vehicle for billionaire private equity investors. Corporate contractors have already received hundreds of millions of dollars for a project that has breached nearly all of its contract deadlines and is three years behind schedule in completing its first phase, Increment 1.[3] Despite the wide-ranging implications of a project of this scale—including significant privacy and civil rights implications for hundreds of millions of people—DHS has shrouded HART in secrecy with little oversight and few accountability mechanisms. Unfortunately, Congress continues to authorize millions of dollars in funding despite troubling questions over HART's mission, the potential for human rights violations, and privacy concerns.

Powered by military-grade technologies, HART is an unprecedented step forward in DHS' surveillance capabilities. HART is a massive surveillance tool that will aggregate, link, and compare biometrics data, including facial recognition images, DNA profiles, iris scans, digital fingerprints, and voice prints on unique profiles of more than 270 million people, including juveniles.[4] HART's purpose is to collect, organize, and share invasive personal data from federal agencies such as Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), the Federal Bureau of Investigation (FBI), and the Department of Defense, as well as from local and state law enforcement, and from dozens of foreign governments and international agencies. This includes data collected on refugees by the United Nations. HART will vastly expand the reach of DHS, and the agency has not clarified the limits of what personal and biometric information will be collected and shared. However, feeder systems into HART raise the clear possibility that it could capture people's professional roles, religious affiliations, banking information, familial connections and friendships, romantic partnerships, personal activities, political views, patterns of travel, and other sensitive information.[5] DHS could use HART to identify people in public spaces—which would severely limit people's ability to exercise their rights to protest, assemble, associate, and to live their daily lives.[6]

HART will be an incredibly powerful weapon for domestic and foreign policing agencies, but for the public and people most impacted by it, HART is designed as a "black box" that operates with few limits or mechanisms for accountability. But what we do know about HART raises multiple human rights, civil liberties, and privacy concerns.

As we detail in the report, HART raises particular concerns for Black and brown communities that are already the target of discriminatory policing. HART drastically expands the surveillance power of policing agencies, interferes with everyday lives and undermines freedom of assembly, and weaponizes information that people submit

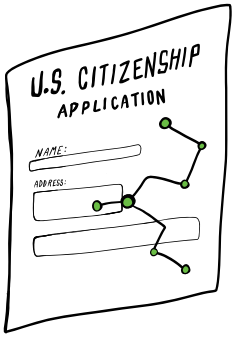
to access government services. In addition, HART relies on untested, racially-biased, and unreliable biometrics and draws on data from controversial and unreliable sources. On top of that, DHS clearly states that it will not ensure that the data is accurate or of sufficient quality, even though HART retains data for 75 years and includes juvenile biometric data.

Our report shows how HART is designed to shield DHS from scrutiny, accountability, and consequences for its use of data to violate civil and human rights. HART undermines privacy rights in multiple ways. HART will collect massive amounts of data without meaningful consent, and its redress measures for violation of privacy and civil rights are effectively non-existent.

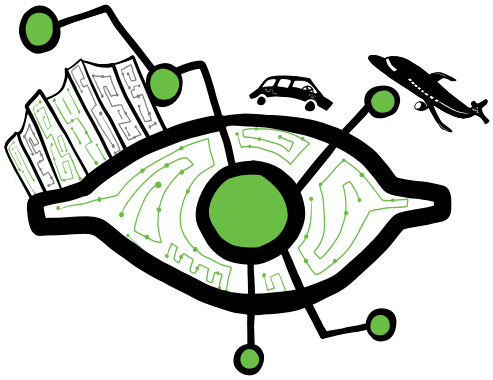
HART's dragnet effect, privacy risks, and biased margins of error in biometric identification are just the most immediate and visible threats to personal and collective freedom that HART presents. Just like Secure Communities—the automatic fingerprint sharing program between police and DHS—helped fuel unprecedented deportation, HART will vastly expand DHS' ability to target immigrants and separate families. The underlying role and impact of HART will be to turbocharge DHS' unchecked power—to approve or deny immigration benefits, assemble target lists for ICE raids, expand the tech border wall, and to facilitate surveillance, arrests, immigrant detention and deportation.

HART accelerates militarized policing against immigrants by utilizing experimental and unreliable new technologies that bring biometric collection into new corners of everyday life.

For example, HART could capture...

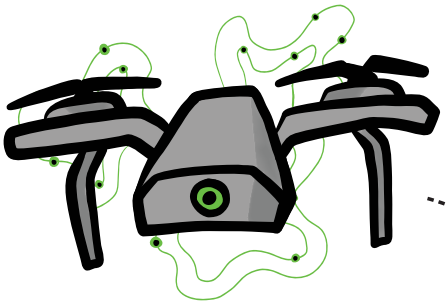


Your biometrics and other data gathered by US Citizenship and Immigration Services (USCIS) for your visa application or immigration benefits application.

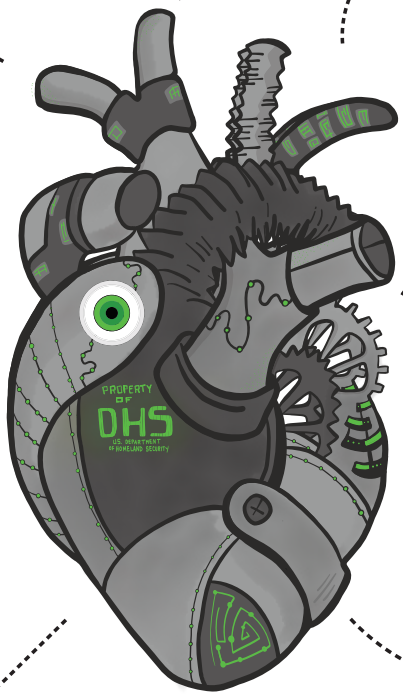


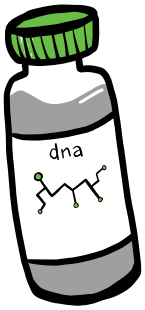
Your facial scan or a facial recognition match when you cross the border in your car or travel through an airport.

Your family, romantic, and business relationships, mapped by ICE based on your social media pictures (scraped by private companies), existing facial images, and social media monitoring.

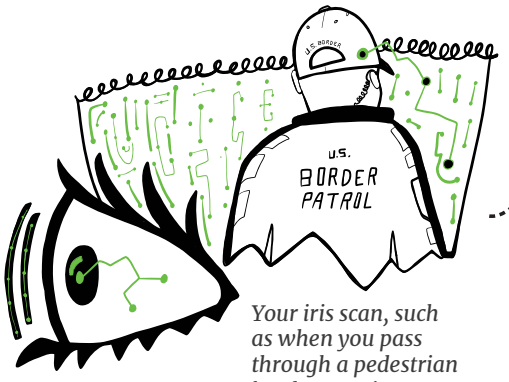


Footage of you captured by a drone in the border region or at political protest.



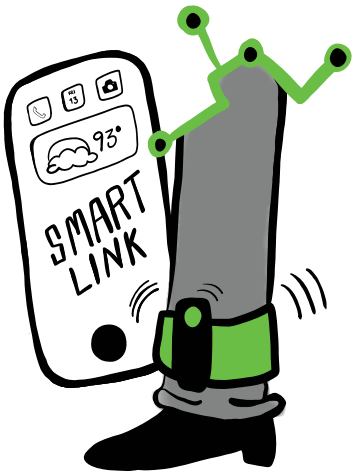


Your DNA information that was collected by CBP, ICE, local police, or other agency that feeds into HART.



Your iris scan, such as when you pass through a pedestrian border crossing.

Your license information, captured by license plate readers or your registration with the DMV. ICE agents have already run millions of searches for driver's license photos at DMVs around the country, using facial recognition to search for matches.



Your location, voice, and face. For example, if you are subject to ICE's Alternatives to Detention program, which uses biometric check-ins to track you through location tracking, voice recognition, and facial recognition.

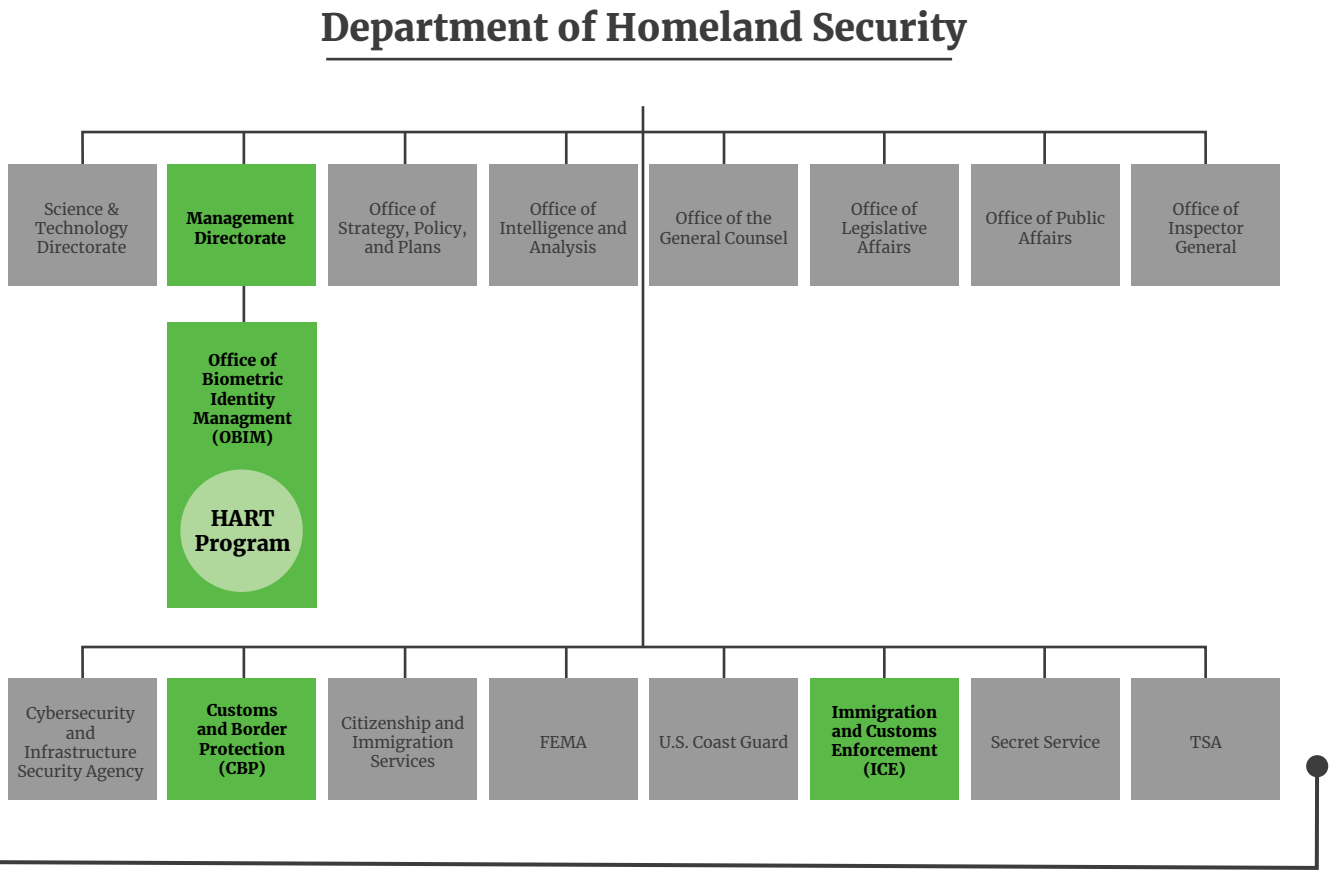
What is HART?

HART will be a centralized DHS-wide biometric and biographic database, expected to be the largest biometric database in the United States.[7] HART is intended to "match" people's identities and create digital profiles of individuals within minutes. It will link biometric information to other information about people, including their political affiliations, location, religious activities, and relationship patterns. HART will also draw from commercial and publicly available sources.[8] It will be the new foundation for immigration enforcement operations and immigrant processing, interfacing with local, state, federal and international databases. This will allow DHS to make target lists for raids; expand deportations, surveillance, arrests and immigrant detention; approve or deny immigration benefits; and increase the technology-fueled "smart border."

HART is a massive overhaul of the Automated Biometric Identification System (IDENT), a 1994 "legacy Immigration and Naturalization Service (INS)" system that currently vets immigrants for visas and immigration enforcement.[9] In 2015, the DHS Office of Biometric Identity Management (OBIM) announced its plans to replace IDENT with HART, and released its plans for HART several years later. OBIM is a separate sub-agency from ICE or CBP, and is housed within DHS' "management directorate." At this time, IDENT contains 272 million unique identities, including 6.7 million iris pairs and 1.1 billion face images.[10]

DHS is rolling out HART in three stages that they call "increments," but the rollout is now multiple years behind schedule. **HART Increment 1, which has not been completed,** involves migrating IDENT to the Amazon Web Services GovCloud. Each increment will include new tech capabilities, machine learning, vast storage, and new biometrics.[11] (See Appendix A for a summary of the three increments and Appendix B for more details on Increment 1.) Very little is known about these increments, except through infrequent "Privacy Impact Assessments" (PIAs) and hard-to-find contract specifications.[12] These companies stand to make billions of dollars from their contracts to develop the database and its components.

Figure 1: This figure shows how OBIM relates to DHS' organizational infrastructure. HART resides in OBIM, which is part of the Management Directorate, a subagency of DHS. The Management Directorate controls OBIM's budget and HART's implementation. Currently, OBIM has its own analysts and it interacts with DHS core operations, such as CBP and ICE.



What will go into HART?

DHS is designing HART to be a digital profile repository of hundreds of millions of people composed of the personal information—biographic and biometric data—that makes up our daily lives.[13] Even though HART is not yet built, the Office of Biometric Identity Management (OBIM) already contains the largest collection of biometric information in the US government, all of which will feed into HART. As of 2019, OBIM was already running hundreds of thousands of transactions and checks for CBP, ICE, TSA, and other DHS components.[14] OBIM shares biometrics with state and federal agencies, as well as with international governments.[15] OBIM's contractors and employees provide biometric verification and identification services. OBIM's Biometric Support Center employs approximately 70 BSC examiners.[16] In addition to biometric and biographic data, HART will also rely on artificial intelligence and machine learning capability.

Biometric data

This includes but is not limited to fingerprints, palm prints, latent prints,[17] DNA,[18] iris scans, facial recognition, thermal scans, and voice prints. DHS has not explicitly ruled out the collection of other types of biometric and biographic information. Similar concerns remain for the collection and retention of cardiac signatures, breathing patterns, individuals' walking gait, or even typing cadence.[19]

Biographic data

This includes biographic information, "encounter data" and "derogatory information," and DHS officers' impressions of a person's life. More specifically:

- **Biographic information** includes nicknames and aliases, personal physical details (scars, tattoos, etc.), gender, ethnicity, occupation, publication records, online identifiers (e.g. social media handles), age, computer name, level of education, signature, and a long list of number identifiers, including A-Number, Social Security Number, FBI Number (FNU), Department of Defense Biometric Identifier (DoD BID), civil record number, and state identification number, and other agency system-specific fingerprint records locator information.[20]
- **Encounter and derogatory information** includes immigration violations, arrests, criminal record, foreign criminal convictions, wants and warrants, sexual offender registration, "known or suspected" terrorist designation, and even "known or suspected" gang membership, which can be submitted by data providers who are not authorized users.[21]

- **Agents' impressions or feelings** will also be included in HART. DHS officers will also be able to add "miscellaneous officer comment information,"[22] and to note what they perceive to be individuals' political affiliations, religious activities, and friends and family relationships. This could mean that an agent's beliefs or opinions will make it into HART, even if wholly unsubstantiated.

Artificial Intelligence (AI) and Machine Learning

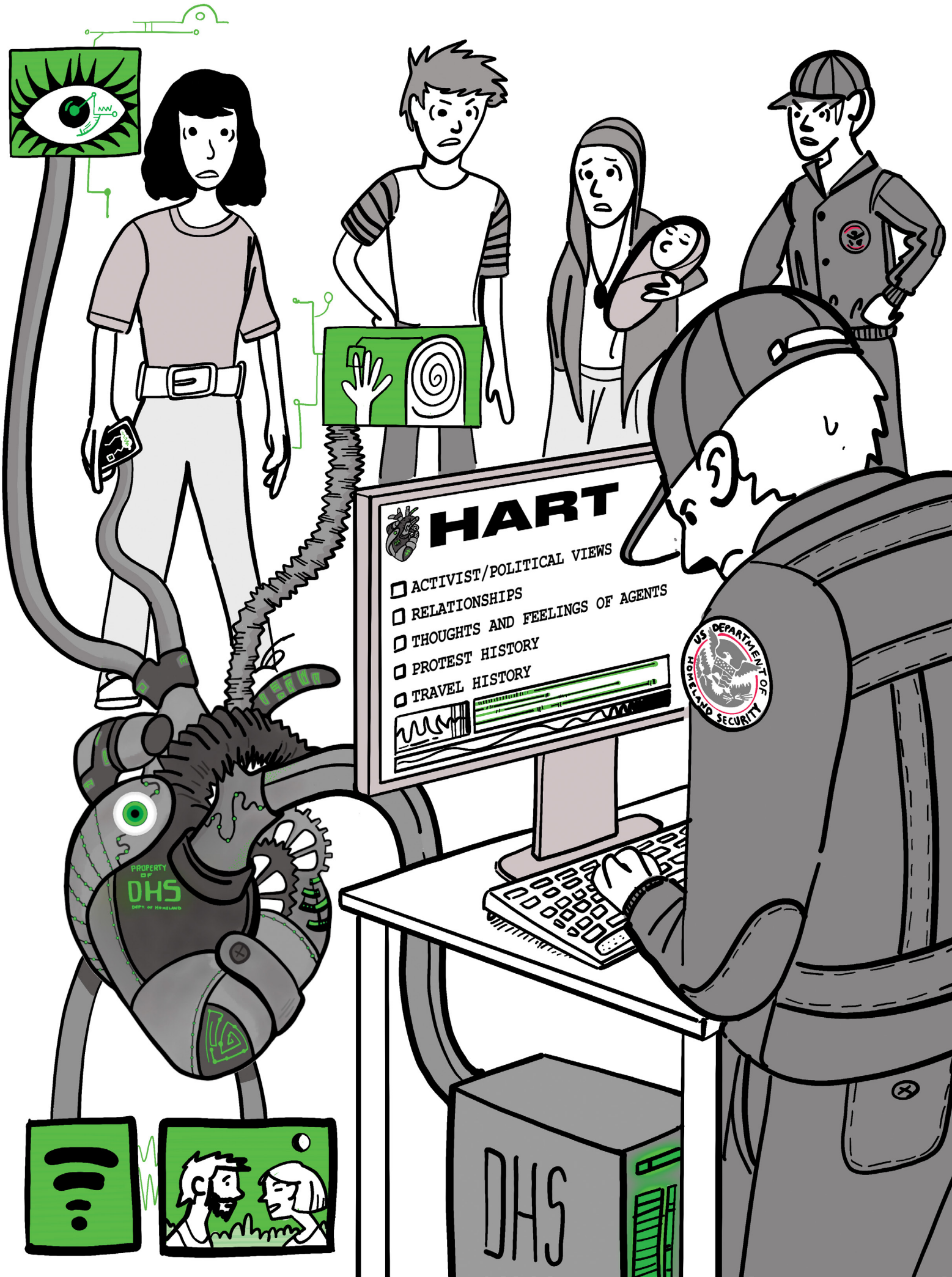
DHS will include AI and machine learning capability through several programs. For example, DHS is developing RAVEn, a $300 million system aimed at identifying immigration targets through "mining social-media information, and processing surveillance footage and biometric data."[23] HART will be a source repository for RAVEn, allowing it to process information from noncitizens and US citizens—including social media information, biometrics (face, iris, photograph, etc.), location-related data including any geolocation information from surveillance, license plate readers, financial data including "suspicious" financial activity, and case-related information including information from the "darknet."[24]

What is AI and Machine Learning?

Artificial Intelligence (AI): AI refers to certain computer functions that humans associate with the human mind, but is not the AI in books and movies. AI applications include systems in Google, YouTube, Amazon, Siri or Alexa, self-driving cars, or even chess.

Machine Learning: Machine learning involves the processing of vast amounts of data and is part of AI. DHS' systems already process billions of pieces of data, and it relies on machine learning to crunch and analyze these vast amounts of information.

Much of this data is collected without people's consent or even knowledge. Companies and government agencies increasingly use data collection and data harvesting to bypass constitutional requirements around warrants and consent, which protect people's rights if they are suspected of wrongdoing. As a result, international, federal, state and local agencies could have access to HART's biometric and biographic personal information without receiving an individual's consent or obtaining a warrant. Moreover, people will have no control over how their information is collected, used, accessed, or shared.


HART
ACTIVIST/POLITICAL VIEWS
RELATIONSHIPS
THOUGHTS AND FEELINGS OF AGENTS
PROTEST HISTORY
TRAVEL HISTORY
US DEPARTMENT OF HOMELAND SECURITY
PROPERTY OF DHS DEPT OF HOMELAND
DHS

What will change when HART comes online?

HART's capacity and scale go far beyond DHS' existing web of surveillance systems, which already collect and handle billions of pieces of biographic information.[25] When HART comes online, DHS' existing systems will either link to or flow into HART.[26] Currently, when individuals apply for immigration benefits such as a green card, temporary protected status, or DACA, DHS runs their biometrics, including fingerprints, through IDENT or another system to check for any flags in law enforcement and security databases.[27] HART will drastically increase the amount and types of data collected, and expand DHS' interoperability with other agencies. Yet HART offers limited opportunities for people to hold DHS accountable for violations.

Under HART, there will be virtually no pathways to challenge DHS' life-and-death decisions. Information in HART will be used to approve and deny immigration benefits and target people for raids, arrests, surveillance, and deportations. However, people most impacted by HART will not be able to know if their data is even included in HART, much less challenge the collection and use of their data. People will be subject to decisions made in seconds, without the ability to apply for redress later on. See more on privacy concerns and lack of redress mechanisms in the report's section of HART's violations of basic rights.

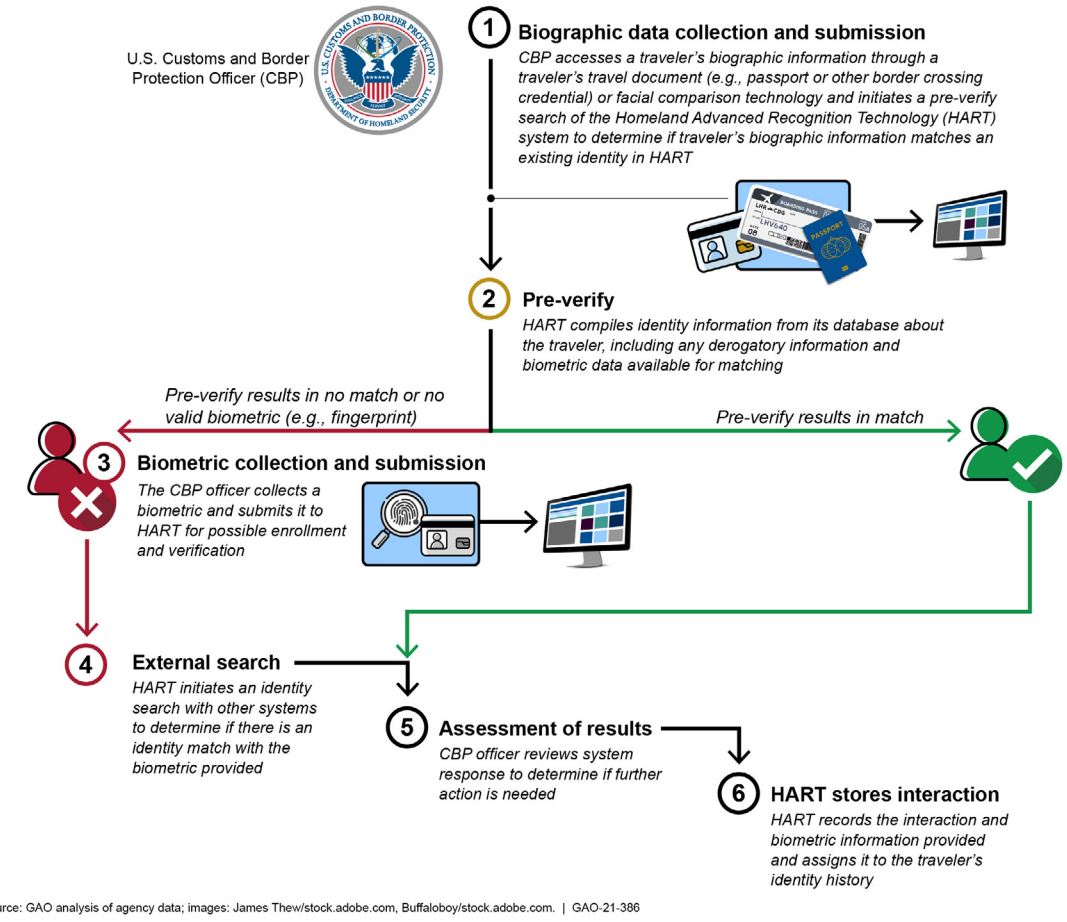
Here are a handful of examples of what data will immediately end up in HART. A more detailed snapshot is in Appendix C.

- **Voice scans:** ICE's Alternatives to Detention (ATD) program uses electronic monitoring devices, including telephonic check-ins, to gather data for voice recognition and location tracking.[28]
- **Facial scans:** Facial recognition includes photos taken by CBP and ICE, as well as images scraped from social media by ICE contractors, and images from some DMVs.[29]
- **Social media:** Data from the National Vetting Center,[30] a CBP-led initiative, incorporates social media screening into the vetting of anyone seeking entry or a visa.
- **USCIS biometrics data:** HART will include information from USCIS biometric appointments that are required for people applying for a green card, work permit, Temporary Protected Status, and other types of status.
- **Fingerprints:** Agents collect fingerprints using a handheld mobile biometrics application called EDDIE, with data now feeding into IDENT and soon HART.[31] CBP uses an application called the e3 Portal to collect fingerprints and photos of migrants, data that is also transferred to IDENT.[32]

- **Location Data:** DHS purchases geolocation cell phone data from commercial sources, like Venntel.[33] Agencies argue no warrant requirement exists for them to buy and use this data.

Below is a figure[34] that shows the CBP systems flow for travelers entering the United States. As this picture shows, vast amounts of information from travelers and US residents will be enrolled into HART.

Figure 2: Illustration of how HART will process information from any traveler who enters the United States. "Planned Process Flow between U.S. Customs and Border Protection and the Homeland Advanced Recognition Technology (HART) System for Biometric Identification or Verification for Air, Land, or Sea Entry"



GAO, "DHS Needs to Fully Implement Key Practices," 14

How Much is HART Projected to Cost?

HART is a massive project that requires billions of dollars to build and hundreds of millions to maintain. The reality is that HART is shaping up to be an expensive disaster with massive cost overruns and nearly a 5-year delay.[35] When initiated, HART was expected to be completed in 2021[36] about four years after the start of the project. Several revisions were proposed.[37] In March 2022, the US General Accounting Office (GAO) found HART had failed all contract deliverables, and there is still no estimated date of complete implementation.[38] In that same report, the GAO again revised HART's life cycle cost: now the program will likely **cost $6.158 billion**. This is a $1.86 billion dollar increase over the January 2021 GAO estimate of $4.3 billion.[39]

Figure 3: APB Thresholds vs. Current Estimate. (Dollars in Millions). This illustrates the massive changes and/or steep increases for the total HART acquisitions.

	PC&I COST	O&S COST	LIFE-CYCLE COST
Initial APB (04/2016)	273	5,563	5,836
Current APB (05/2019)	214	3,709	3,923
Current estimate (06/2021)	455	5,703	6,158

Acquisition Program Baseline (APB), Procurement, Construction & Improvements (PC&I), Operations & Support (O&S). "DHS Annual Assessment: Most Acquisition Programs Are Meeting Goals Even with Some Management Issues and COVID-19 Delays," United States General Accounting Office, March 8, 2022; GAO-22-104684, p. 39

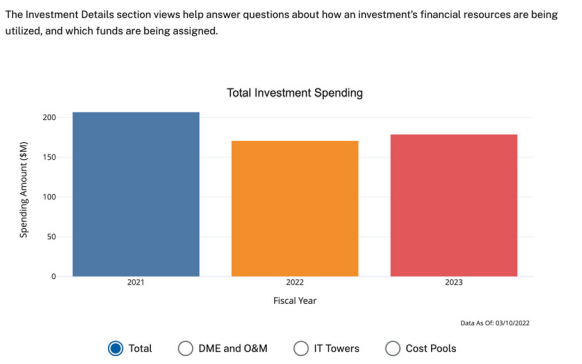
Over the last few years, DHS has invested at least $170 to $200 million per year, despite the fact that DHS has failed to meet every contract milestone.[40] In FY 2021, the US government spent $183.9 million for HART.[41] The new DHS FY 2023 budget includes an increase of $23.4 million for HART "Operations" (cloud hosting, storage, analytics, contractor services, etc.),[42] as well as $38.1 million for procurement, construction, and improvement.[43] The FY 2023 base for the program is $221.5 million,[44] although it is not clear how the different investments and budget lines add up.

DHS' accounting practices are confusing at best. The GAO criticized DHS in 2021 for its lack of clarity in HART's spending data and budget lines, writing that, "While the program reported to OMB via the IT Dashboard that it had spent about $577 million, in total, from fiscal years 2016 through 2020, it was unclear how much of this spending was specifically associated with the HART program. This was because the figure also included the operations and maintenance costs for IDENT. DHS officials explained that HART's spending data on the IT Dashboard included costs related to IDENT because the department had decided to track the operations and maintenance costs for both systems under a single funding account."[45]

According to ITDashboard.gov, a tool used by the US government to oversee performance of federal contracts, the HART program is **"high risk."**[46] The Dashboard and reports cited a few reasons for the technical delays, such as the fingerprint matching system not meeting accuracy requirements and inability to meet contract specifications.

The figure below shows how the GAO has repeatedly revised and extended the production cycle of HART since 2016 due to contract breaches.

Figure 4: Investment Spending Details from ITDashboard.gov. This figure shows fiscal year spending for HART from 2021 through 2023.



ITDashboard.gov, DHS - Homeland Advanced Recognition Technology (HART) / 024-000005253 FY2022, https://viz.ogp-mgmt.fcs.gsa.gov/investment-details/024-000005253, accessed April 4, 2022.

Figure 5: HART Schedule. This GAO graphic shows program breaches and "rebaseline" shifts for the HART program.

US General Accounting Office (GAO), "DHS Annual Assessment: Most Acquisition Programs Are Meeting Goals Even with Some Management Issues and COVID-19 Delays, GAO-22-104684" March 8, 2022, 39, https://www.gao.gov/assets/gao-22-104684.pdf

Congress has raised concerns about HART expenditures

The House Committee on Appropriations submitted a report on the Department of Homeland Security Appropriations Bill for Fiscal Year 2022 (H.R. 4431), stating that "program delays" necessitated a reduction in HART funds by $25 million. In addition, the Committee mandated a series of accountability measures, including a comprehensive review, multiple audits, and compliance reviews by the Office of the Inspector General.[47] Similarly, the Senate Committee recommended a $25 million reduction "in recognition of ongoing cost, schedule and performance challenges."[48] Additionally, they demanded more transparency from DHS regarding the rollout of emerging and untested technologies. The Explanatory Statement for the 2022 Homeland Security Appropriations Bill states:

"The Committee requests that the Department provide adequate disclosure of its technologies, data collection mechanisms, and sharing agreements among DHS immigration enforcement agencies, other Federal, State, local, and foreign law enforcement agencies, and fusion centers as relates to the development of the HART biometric database that will replace the Automated Biometric Identification System [IDENT] database."[49]

While these introductory inquiries are helpful, Congress must do more to ensure that HART's deployment is immediately halted for FY2023.

The Committee requests that the Department provide adequate disclosure of its technologies, data collection mechanisms, and sharing agreements...

Which Companies are Behind HART?

The corporate players behind HART

Companies are making millions, potentially billions, of dollars off the HART contract and are lining up to make more. Companies aggressively compete for additional billions of dollars in DHS contracts,[50] including for biometric and surveillance technologies such as biometric device collectors, data brokers, social media scraping companies, analytics, facial recognition, and much more.

Northrop Grumman

The Military Defense Contractor Originally Contracted to Develop HART

In September 2017, DHS awarded a contract to develop the first two increments of HART to Northrop Grumman, a publicly-held military defense contractor.[51] In December 2020, Veritas Capital, a private equity firm, acquired Northrop Grumman's federal IT business that was involved in making HART for $3.4 billion in cash.[52]

Veritas Capital

Peraton

The Private Equity Company Building HART, via a Subsidiary

HART is currently being developed by Peraton, a subsidiary of a private equity firm, Veritas Capital, removing the project even further from public scrutiny and raising further concerns about the exorbitant expenses associated with the project. HART has exceeded its initial cost estimate for the contract to develop the first two increments multiple times (the initial contract was for $95 million and has been increased to a $143 million).[53] Private equity firms increasingly see the intelligence and surveillance sector as a lucrative investment opportunity. Ramzi Mussalam helms Veritas Capital, and his estimated worth is $4 billion.[54] Mr. Muzzalam is perceived as a key player in the government contracting space, and has turned multiple public companies private.[55]

Veritas placed this purchase in its private equity subsidiary **Peraton**, which focuses on IT and other technology-related government services.[56] With the acquisition of Northrop Grumman's IT services and the subsequent acquisition of huge IT contractor Perspecta—

which Veritas acquired for $7.1 billion—Peraton increased its business by 700%. Currently, HART's development and contract is in Peraton's name.[57] Peraton recently established its own Political Action Committee (PAC) to support lobbying on its issues.[58] Peraton's annual revenues of approximately $7 billion, a three-year qualified pipeline of $200 billion, and its 22,000 employees are now in the hands of Veritas Capital.[59]

What is the impact of HART's acquisition by a private equity firm?

Unlike Northrop Grumman, a publicly-traded company, Peraton shares far less information with the Securities Exchange Commission, which functions as an oversight agency for businesses. Peraton is not subject to any oversight from shareholders. In contrast, in 2019, nearly one third of Northrop Grumman's shareholders voted in favor of a resolution that called on the company to issue a report on due diligence on its human rights policy.[60] The resolution stated its concerns about HART including that the database "will amplify the surveillance capabilities of government agencies, presenting risks to privacy and First Amendment rights and causing harm to immigrant communities."[61]

With this limited oversight removed, **it will be difficult to know what is being built by Peraton and how they are building it.**

If DHS continues with HART, far more money will have to be awarded to Peraton and Veritas Capital or other contractors. For example, Peraton owns Perspecta Engineering, which was just awarded a $2.6 billion contract over 10 years to build a "full suite of hybrid compute operations services to manage and operate the DHS Hybrid Computing Environment" (HCE). The HCE is a collection of enterprise computing resources including a data center, colocation sites, private cloud services, and DHS furnished commercial cloud services."[62]

Thales, NEC, and Fingerprints

DHS' Core Biometrics Contractors

Currently, OBIM uses the following contractors for various biometrics programs.[63] These programs largely exist to power IDENT, the precursor to HART.

- Thales Corporation[64] for fingerprinting matching. They also built powerful technologies for the DOD.
- NEC Corporation,[65] a multinational information technology corporation, that specializes in biometrics, especially facial recognition. NEC has a separate contract[66] with OBIM for the provision of facial recognition services, for a potential $23.9 million through 2022.
- NEC and Fingerprints[67] (formerly Delta ID) for iris recognition

Amazon Web Services

Hosting Our Biometrics on the Cloud

HART will be hosted in Amazon's government cloud platform—Amazon Web Service (AWS) GovCloud environment—despite being managed by OBIM.[68] AWS GovCloud is the most commonly used cloud platform by DHS, hosting many ICE and USCIS systems—including the Palantir-designed Investigative Case Management system used by ICE to track and target people for deportation.[69] While it is hard to know the true value of Amazon's contracts with DHS and the rest of the U.S. federal government since many contracts are with third-party providers, Amazon was awarded approximately $1.4 billion in government contracts from 2007 to August 2021, and at least $6.3 billion in additional contracts with companies that provide its cloud products.[70]

Complicit Corporate Partners

There is a long list of technology companies that provide other services to DHS, some of which could end up as biographical data in HART as components continue to add subject records and miscellaneous comments.[71] For example, companies like **NTT Data Federal Services, Inc.**[72], **Global Infotek, Inc**.[73], **The Mitre Corporation**[74], and **Bayfirst Solutions**[75] have provided human resources, analytics, testing, and assessments for the deployment of HART.

In September 2020, military contractor **General Dynamics** was awarded a contract[76] for work at OBIM worth a potential $64 million through 2025.

What other companies could expand HART's reach?

Data Brokers

Thomson Reuters and **LexisNexis** both provide commercial and government data on individuals to ICE and CBP, via multi-million dollar contracts. The personal data they sell with their CLEAR and Accurint platforms, respectively, includes DMV records, utility and cell phone bills, court records, credit histories, and license plate reader data, among many other sources.

Social Media Companies

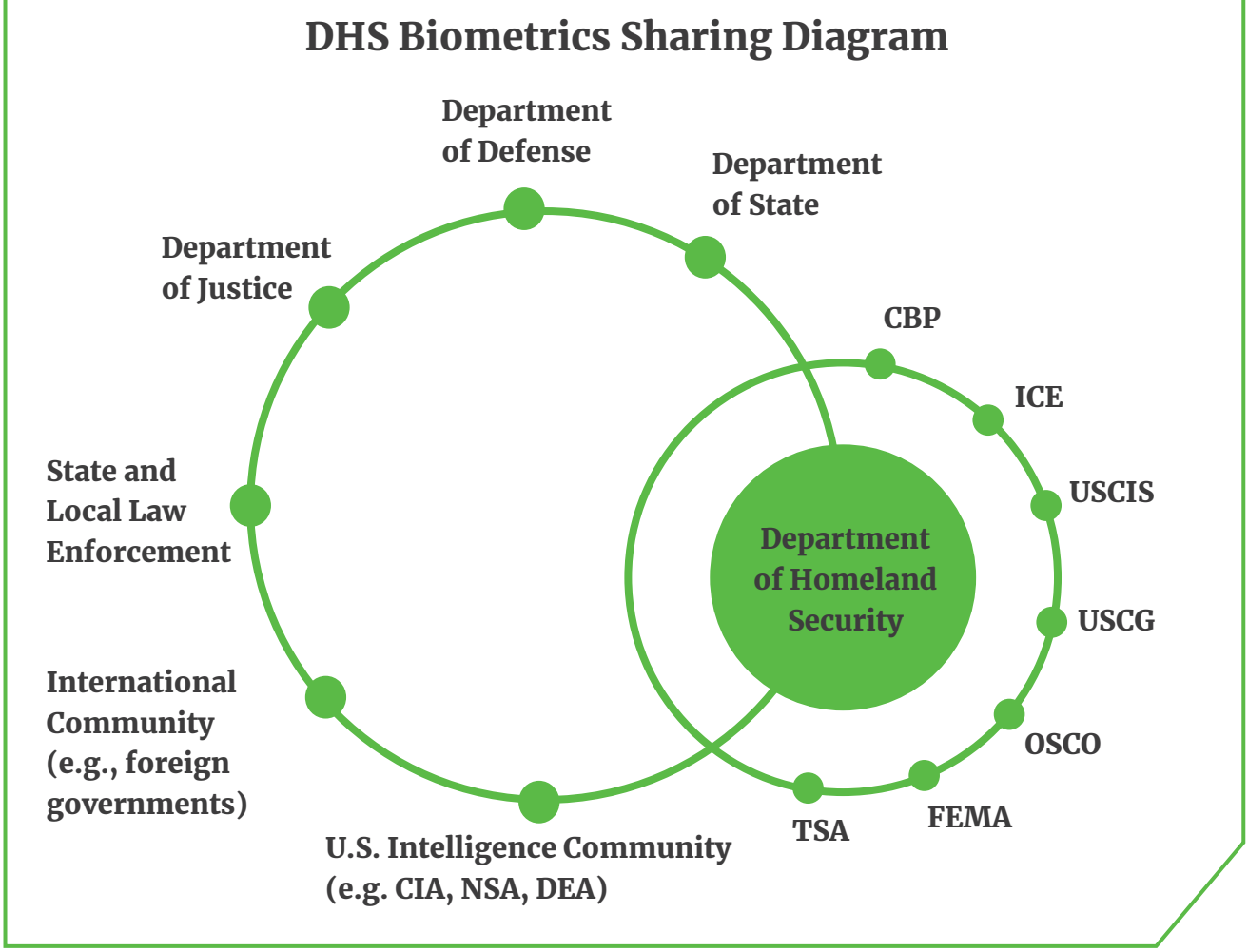
Data from social media could also end up on HART, whether in the form of facial images scraped by private ICE contractor **Clearview AI**, or through social media analytics company **Giant Oak**, which has a contracting vehicle[77] worth up to $37 million with DHS through 2022.

Biometrics Services Contractors

The numerous private contractors that provide biometric services to HART data providers will indirectly expand the platform's capacity. On the same day that Northrop Grumman was awarded the principal HART contract, the Department of State awarded a contract to **CSRA** (now **General Dynamics**), developer of the IDENT platform, to implement a mass biometric collection program on behalf of the Government of Mexico, called the Digitus Agreement. The multi-modal data collected through this program is the same third-country national biometric data that is shared by Mexico's immigration authorities with DHS under their January 2017 biometric data sharing agreement. Under this agreement, Mexican immigration authorities collect and share biometric data on all third-country nationals seeking authorization to travel, work, or live in Mexico or the United States, or who have been detained.[78] This data will end up in HART.

Who Will Use and Access HART?

Figure 6: This figure illustrates how HART plans to share and collect information within DHS, and with other federal agencies, law enforcement agencies, various intelligence agencies, international agencies, and foreign governments.



DHS intends for HART to be a one-stop shop, a "single authoritative biometric system" that can be accessed and used by international, federal, state, and local agencies.[79] Information Sharing Access Agreements (ISAA) are one way that DHS executes data sharing agreements with other agencies, governments, and corporations. Data providers can determine which users have access to their data. The Privacy Impact Assessment goes into some detail about access for only one stage, Increment I of HART, as shown in Appendix B.

In addition to sharing information across DHS agencies,[80] one of the key objectives behind HART is to increase "interoperability" with other agencies' biometric systems, meaning that HART will interact with other databases in the United States and abroad. DHS will use information in HART to identify people who may turn up at ports of entry, border crossings and refugee camps, in civil or criminal records, through surveillance cameras in public, and even via social media usage. HART will be used in asylum cases and to make lists for raids, for arrests, and for deportations.

US federal agencies that will interact with HART

The short list below does not constitute a full and complete list of all the databases HART is expected to connect and interact with.

Department of Defense (DOD)

Automated Biometric Identification System (ABIS): DoD implemented the first ABIS in 2004 to track and identify "national security threats" by running biometric searches. It collects data from military and other intelligence sources. This system was built by military contractor Northrup Grumman.[81] Individuals encountered during military operations may also end up in HART.[82]

Department of Justice (DOJ)

FBI's Next Generation Identification System (NGIS): NGIS is the largest biographic and biometric repository on U.S. citizens and noncitizens who have had contact with a criminal legal system. Maintained by the FBI, it includes information about arrests, convictions, outstanding warrants, and other criminal history along with fingerprint, pictures, face scans, palm prints, and other biometrics.[83] It will be the second largest such database after HART.

Department of State (DOS)

Consolidated Consular Database (CCD):[84] This is a database of real-time consular activity all over the world. This means that any agent can have access to sensitive personal information supplied to a consulate for a visa, immigration, or refugee processing.

What are some other databases that will interact with HART?

The short list below does not constitute a full and complete list of all the databases HART is expected to connect and interact with.

State, local, tribal, and territorial law enforcement agencies	These agencies will provide data to HART, and those that have entered into information sharing access agreements (ISAAs) with DHS for biometric identification and analysis services will be authorized HART users.[85]
United Nations High Commissioner for Refugees (UNHCR)	DHS has signed an agreement with UNHCR to acquire sensitive information that it has collected from refugees.[86]
Foreign Governments	Several foreign governments are expected to have various degrees of access to HART. This includes the Five Eyes/Migration Five Partners—Canada, the United Kingdom, Australia and New Zealand. DHS already has biometric data sharing agreements in place with Mexico, Guatemala, Honduras, El Salvador, Greece, Italy, the United Kingdom, Canada, New Zealand, and Australia. Additionally, a number of countries have authorized Criminal History Information Sharing (CHIS) agreements with DHS, to exchange criminal conviction information on people being deported from the United States. ICE has this type of agreement with Mexico, Honduras, Guatemala, the Dominican Republic, El Salvador, Jamaica, and the Bahamas.[87] Mexico's immigration authority, for example, through a series of agreements signed by DHS and the Government of Mexico, already submits "its collected biometric and biographic holdings, in bulk, to DHS [...] on individuals whom they believe to be nationals of a third country."[88] The agreements enable the Mexican government to submit electronic fingerprint queries to the DHS's fingerprint database, and all biometric and associated biographic information obtained by Mexico on migrants will be enrolled in the DHS fingerprint repository.[89]

Why HART Must Be Stopped

HART promises a fantasy that a vast data collection system powered by militarized technologies will provide security and safety. Instead, it will vastly expand the Department of Homeland Security's surveillance capabilities and the immigration enforcement dragnet by yielding accurate lists of undocumented people, their undocumented families, and others deemed "undesirable." HART will put BIPOC communities, including immigrant communities, at greater risk of profiling, arrest, and detention. Furthermore, HART is not designed to ensure accuracy nor protect people's rights. As mentioned above, HART also puts enormous power to develop these technologies into the hands of corporate entities—first a military defense contractor, and now billionaire private equity investors—that are not concerned with the rights of communities but rather with maximizing profits.

HART is a black box with dangerous unknowns. DHS has actively prevented oversight of HART and related systems and ignored calls for transparency. DHS has shrouded the project in secrecy, despite the massive taxpayer investment. There has been limited government review and almost no public scrutiny. Very little is known about how DHS will collect, keep, or share information in HART with third parties, such as corporations, other government agencies, or other countries. Specifically, DHS refuses to share information about HART's actual technologies, data collection mechanisms, the analytical tools, where the data is harvested, or whether the collection was authorized or consensual. We are also left in the dark about information sharing agreements between DHS immigration enforcement agencies, other federal, state, local, and foreign law enforcement agencies, and fusion centers as they relate to the development of the HART biometric database. It is unclear what information will ultimately be contained in HART, as DHS has indicated that the definition of biometrics can continue to expand.[90] We already know that HART will include biometrics that have been shown to be unreliable such as facial recognition, biographic information, and subjective information on perceived relationship patterns. It may also include other biometrics in experimental stages such as voice prints, and biometrics like DNA collection that present serious ethical concerns.

What we do know about HART raises grave concerns.

HART presents unacceptable threats

HART will powerfully expand DHS' surveillance capabilities, enabling ICE, CBP, and other domestic and foreign policing agencies to fuel discriminatory policing and violate the rights of hundreds of millions of people.

Over the past couple decades, DHS agencies have subjected broad categories of people—including Muslims, unaccompanied minors, undocumented workers, immigrant rights activists, and more—to unwarranted surveillance, detention, and deportation. The harms of racialized local policing have multiplied as police have become a feeder into the immigrant detention and deportation system; studies have shown that Black immigrants are disproportionately deported due to criminal convictions.[91] ICE deploys its surveillance technology against Black and brown immigrant communities, as well as at Black Lives Matter and Indigenous activists. With HART, DHS continues these violations, creating a massive biometric database and enabling info sharing between local, state, federal, and foreign policing agencies, without meaningful safeguards to protect against discriminatory policing and abuse of power.

HART will harvest and exploits facets of our day-to-day lives, jeopardizing the rights of political activists and freedom of assembly.

The collection of biometric and biographic data from people's daily lives has a chilling effect on their everyday activities. HART includes "encounter data" such as information on the "location and circumstance of each instance resulting in biometric collection."[92] Combined with the "records related to the analysis of relationship patterns among individuals and organizations"[93] contained in federal

databases such as External Biometrics Records (EBR), HART will create digital human profiles and map people's intimate connections to community, places, and people. HART will use personal, intimate data to make it possible for CBP and ICE to identify and track people in real time,[94] presenting ethical concerns. It will also greatly expand DHS' ability to locate individuals for immigration policing, including raids and deportations, as the systems that feed into HART include personal and sensitive information from citizens and noncitizens. DHS and its components have also increasingly criminalized and surveilled protests, raising risks for protestors that their biometrics could also be entered into HART.

HART will weaponize information that people are required to submit to access basic government services or in order to travel.

HART will collect and use information that individuals must provide to the government in order to access rights and basic services, such as driver's licenses, travel and immigration benefits. For example, ICE has demanded access to driver's license holders' photos to target people for immigration enforcement, especially after states across the country passed laws granting people access to driver's licenses regardless of immigration status. Images obtained by ICE in this manner would end up in HART. The database would enable users to also have access to facial recognition data on millions of people, captured at airports and metropolitan regions near the border such as Tijuana-San Diego and Ciudad Juárez-El Paso. This means the facial images of those who travel by air or through ports of entry by foot and car would be in HART.

HART will contain data for which DHS cannot ensure accuracy and quality.

DHS collects massive amounts of data, but does not prioritize quality and accuracy of data in HART. It is deeply problematic that OBIM analysts may make recommendations for enforcement actions or on immigration decisions based on low-quality or inaccurate data. Even if OBIM wanted to correct data, OBIM does not officially own the data in HART—it is either held by other DHS subagencies or by third parties. This makes oversight almost impossible, since it is difficult to hold third parties accountable for sharing and selling of data, and for errors in that data. Moreover, DHS has not released permission or privacy protocols for HART—to date, all DHS has provided so far is a notice and comment process that does not allow the public or Congress oversight into this massive system. OBIM recommends, but does not require, that the data providers follow certain best practices and guidelines and places the onus on "the original data owner" to be "responsible for ensuring the accuracy, completeness, and quality of the data submitted to OBIM."[95] OBIM acknowledges the risk that "data quality will not be maintained since HART users have the ability to manually apply derogatory and disposition information" is not mitigated and that OBIM "cannot ensure accuracy."[96]

HART will rely on untested, racially-biased, and unreliable biometrics.

In addition to the risks associated with inaccurate data, HART would rely on biometrics that are experimental and inherently biased. Contrary to the public perception that biometrics provides airtight identity confirmation, the risks around matching errors are numerous—OBIM acknowledges this risk in the only Privacy Impact Assessment of HART to date.[97] Searches in HART generally provide an array of possible matches, leaving verification

in the hands of the user agencies. Facial recognition is highlighted as an important element of HART, yet OBIM acknowledges that "there is a risk that HART facial image matching results may be inaccurate or result in a disproportionate impact to certain populations,"[98] due to inherent biases based on factors including race, sex and age.[99] OBIM stipulates that its users must accept the risk of the accuracy of facial recognition searches, "which reflect the contextual factors identified by the program," including race, age, and sex.[100] This is profoundly concerning for many reasons. Facial recognition use by police has already been shown to result in false positives and wrongful arrests, particularly of Black people and women of color.[101]

HART will retain data for 75 years.

DHS compounds these risks through a requirement that international and law enforcement records be retained in HART for 75 years.[102] Notably, data retention and review is also managed by data owners and providers—not HART. In other words, it is up to the data providers to properly manage their records. OBIM acknowledges that there is an unmitigated risk that data owners may not delete records in a timely manner in accordance with the applicable retention schedule.[103]

HART will contain data on juveniles.

HART will include juvenile biometric data from its data providers. Apart from the ethical issues with that practice in general, relying on such data carries an additional risk of inaccuracies, since some biometric data and images can change during young people's growth. OBIM itself specifies, "there is a risk that retaining the fingerprint, face, or iris biometrics

for juveniles may result in inaccurate results due to factors including growth and image quality," and that this risk is not mitigated.[104]

HART is explicitly designed to shield DHS from scrutiny, accountability, and consequences for errors and use of data to violate rights.

DHS has exempted databases that feed into HART, such as the DHS External Biometric Records (EBR), from multiple provisions of the Privacy Act including requirements regarding accuracy.[105] The World Privacy Forum (WPF) notes that the exemption for the requirements of the Privacy Act regarding accuracy is "remarkable for a system of such high sensitivity and for a system that will have a high impact on individuals' civil liberties."[106] The WPF adds, "Data collected at the border . . . as well as data collected by foreign governments and commercial entities, can contain a high number of errors. This is problematic, because errors entered into the EBR database could (and we predict will) cause erroneous deportations or erroneous criminal charges, and meanwhile, the errors are challenging (or impossible) for the data subject to access or correct."[107] These exemptions also shield DHS from other transparency requests.

HART takes away our privacy.

Although DHS claims that privacy is important, HART and its supporting products actively take away our privacy. The biggest criticism of the privacy framework for DHS systems is that it relies on meta collection to rectify inaccuracies and bias. For example, DHS claims that other biometrics that are collected on a person will mitigate against errors. This erodes the line of what information is "sensitive" and private and "justifies" the collection of more biometrics. DHS has issued a Privacy

Impact Assessment (PIA) for only Increment 1 of HART; DHS has not yet issued a System of Records Notice (SORN), mandated by the Privacy Act of 1974 for newly created systems of records, even though it recognizes it is required.[108] The DHS Office of Biometric Management (OBIM), the custodian of HART, itself acknowledges that "there is a risk of collecting and sharing more information than is required for the purposes of the system."[109]

HART's so-called "redress" measures are effectively non-existent.

The Privacy Act was created to ensure accuracy and for individuals to access redress for incorrect information or the improper collection, storage, or sharing of information. It is widely known that these laws are not very protective. From what we have seen to date, DHS has made even these limited protections either non-existent or incredibly difficult for individuals to access in HART.[110] For example, OBIM states that US citizens, legal permanent residents, and others covered under the Judicial Redress Act (JRA) may file a Privacy Act request or file a Freedom of Information Act request to access their information or correct erroneous information in HART.[111] But in order to do so, one would have to be aware or suspect that their information is stored in HART. Moreover, no point of contact exists for people to address errors in the system or to protect against sharing. Accessing information will be nearly impossible for anyone but DHS agencies, contractors, or law enforcement—even when the data is your own.

HART thrives on data collection without consent.

DHS does not hold itself responsible for gaining consent from individuals for their personal information to be accessible through HART, because, as noted by OBIM in the PIA, HART is not a data owner but "merely a service provider and data repository."[112] Data providers are therefore responsible for complying with laws and policies related to notice and consent. Since HART gathers information from a myriad of sources, individuals will have to refer to the consent and opt-out policies of multiple data providers to HART. OBIM adds that it cannot fully mitigate the risk that an individual may not be aware that their information, collected through an application for a benefit or credential, for example, may be stored in HART and shared with other HART users. It adds, "OBIM partially mitigates this risk through publication of this PIA."[113] For example, individuals who apply for immigration benefits or for programs that ease travel, such as through the DHS Trusted Traveler Programs, may be unknowingly and involuntarily submitting a potentially broad array of biometric data, including new and experimental modalities, to ICE, CBP, the FBI, other intelligence agencies, and foreign governments. Concerningly, OBIM recognizes that an individual may not be aware that biometrics collected during an application for an immigration benefit can be stored in HART and shared with other HART users, and that this privacy risk cannot be mitigated.[114]

HART's data comes from controversial sources.

For example, ICE agents can submit facial images obtained from providers including Clearview AI, which scrapes social media images, without permission either from the social media companies or users, into a database of more than 3 billion pictures. Clearview AI's facial recognition has been banned for use by law enforcement in New Jersey, deemed illegal by the Privacy Commissioner of Canada, and is the subject of a lawsuit by the Vermont Attorney General and multiple civil rights, racial justice, and community organizations.[115] Facebook,[116] LinkedIn,[117] Google,[118] and Twitter[119] have all sent cease-and-desist letters to Clearview AI for violating their terms of service by scraping data. A December 2021 government study on DHS Privacy report noted that IT systems managed by third party contractors were at "increased risk of misuse and insufficient protection."[120]

Conclusion

Dismantling HART is the only way to protect our communities.

We can and must resist the continued development of HART by exposing the companies and agencies involved, and explicitly naming the harm they will wreak on heavily policed people and communities, including protestors, Black and brown communities, and immigrants. HART is neither a "safe" or "smart" way to think of immigration enforcement. It is a dangerously powerful enforcement tool that operates in the shadows, and DHS must not be allowed to continue the project's development.

In the interim, we recommend an immediate halt for the funds allocated to HART for fiscal year 2023.

This reflects concerns from Congress and advocates—HART continues to move forward, largely with bipartisan support, despite the profound dangers and potential impact on privacy rights and civil liberties. Both Senate and House DHS appropriation committees previously recommended slashing HART's budget and demanded that DHS disclose HART technologies, collection mechanisms, and sharing agreements with international, federal, state, local partners, and fusion centers. While we welcome these recommendations as a first step, disclosure of HART technologies and agreements is not enough.

There is no safeguard, privacy clause, or complaint mechanism strong enough to protect against HART's dangers, inaccuracies, and potential harms.

Only a complete freeze on the 2023 HART funding—and a full dismantling of the program—will prevent continued and future privacy, civil, and human rights violations.

Appendices

Appendix A: HART's Development Increments

Increment 1

The new data architecture will be assembled and the transition of IDENT data into HART will be complete.[121] This means HART will include fingerprint, iris, and facial recognition data. "Identity, encounter, and image data" shall be "converted to the HART data structure."[122] 270 million unique identifiers will flow into HART immediately. These initial vast data sets will live on the cloud, run by Amazon Web Services.

Increment 2

This stage will include many more machine learning components to increase "matching" capabilities for face and iris recognition. This means HART will have access to or use several biometric "matching" programs to improve accuracy[123]—but it is not clear why having more modes of matching improves reliability and accuracy. With HART, DHS intends to create the capability of having one system provide a "person-centric" visual for each individual, linking all biometric, biographic, and relational information to a single unique identity.

Increment 3 & Increment 4

According to the June 2021 GAO report, DHS has elected to merge these increments, calling them "future capabilities."[124] Although, DHS has not explicitly spelled out requirements for these increments, they anticipate adding advanced "analytic" capabilities to HART so that analysts can review vast quantities of data and share their analysis with ICE, CBP, and USCIS, and make a web portal for this system that is accessible to a number of external partners.

Appendix B: HART Services in Increment 1[125]

Service	Description
Identity and Encounter Creation	When a HART authorized user initially enrolls an individual's fingerprint and basic biographic information, HART will create a Fingerprint Identification Number (FIN) for that individual. While the fingerprint and basic biographic information establish an identity, every subsequent encounter receives a new HART-generated Encounter Identification Number (EID).
Fingerprint Matching	Fingerprint data sets may include submissions related to visa applicants and other individuals seeking immigration benefits, credentials to secure facilities, submissions from law enforcement actions, or fingerprints associated with national security. After searching the entire fingerprint gallery during an identification request, HART returns the identity with the best match to the fingerprint submitted.
Facial Recognition Services	HART will provide facial recognition services, pursuant to written agreement between OBIM and authorized users. HART users will accept risk of the accuracy of match or no match responses from HART based on metrics provided by OBIM, which reflect the contextual factors identified by the program. Contextual factors may include the demographic of the population (e.g., age, sex, race), camera quality, the rate of throughput, lighting, distance, and size of the database, as well as other factors.

Facial 1 to 1 (Verification)	Facial 1 to 1 verification will allow a HART authorized user to match a single facial image to an existing facial image associated with a known identity in HART. An authorized user will submit a facial image and EID that asserts an identity. HART then will provide a response indicating if the face submitted with the asserted identity matches the face of the same identity on file. The threshold for matching is set by OBIM through testing and measuring error rates and statistical representations of matching accuracy to reduce errors and potential bias. OBIM's Biometric Support Center (BSC) reviews specific situations in which the submitted image does not correctly match to a known identity in HART. This scenario is called a mismatch.
Facial Comparison (2-Photo Submission)	The facial comparison feature will allow a HART authorized user to submit two photos in a single transaction to determine if the submitted images match at or above a given threshold, as established by OBIM.
Facial 1 to Many (Identify Candidates)	Facial 1 to Many biometric search will allow an authorized HART user to submit a face image and request a search of facial images held in one or more specified HART face galleries. Submitted face images may come from a photo or video capture. OBIM is working to determine the optimal 1 to Many face threshold through testing and measuring error rates and statistical representations of matching accuracy for best performance and to reduce potential bias. HART will not provide a single match for 1 to Many searches. It will return candidate lists, devoid of biographic data.
Iris Matching Capability	HART will have an operational iris gallery, allowing 1 to Many iris matching capability. As with facial images, all iris enrollments are associated with fingerprints and basic biographic information. The 1 to Many service searches a submitted iris against the iris gallery in HART. If there is no match above an OBIM-selected threshold, then OBIM's BSC will review and provide a hit or no hit response.

Latent Fingerprint Identification	Latent fingerprints ("latent prints") refers to prints deposited on a surface from a person whose identity is unknown. For each image compared, HART will assign numerical values that indicate the similarity between known fingerprints in HART and the latent fingerprint submitted. HART will return a candidate list to the submitter with the top twenty (or less, if twenty do not exist) unique highest-scoring candidates authorized by HART data owners for automated sharing with the associated EID.
HART Identity Services	HART authorized users will be able to request a service or provide information to the HART system. Authorized users will have the ability to determine which services they need based on mission needs and technical capabilities.
HART Data Filtering	Each HART authorized user will have an Organization/Unit/Subunit (O/U/S) account for their specific agency or organization, and their account receives information in accordance with defined filtering rules. HART will have the ability to either filter or share HART data from an O/U/S in accordance with permissions set by the data owner at the request of the user requesting the data.

Appendix C: Examples of Biometric Collection by DHS Components Under IDENT

Fingerprints	**ICE** • When ICE makes an arrest, fingerprints are collected as part of the process of building an A-file. A handheld mobile biometrics application called **"EDDIE"** is used to facilitate the collection and recordkeeping of aliens in ICE custody. This handheld application collects fingerprints and photographs in about 30 seconds, which are then transferred to IDENT. Source • **NeoScan fingerprint devices** purchased from NEC Corporation for field operations work in conjunction with EDDIE. **CBP** • **e3 Portal:** "USBP agents use e3 to store and transmit biographic information to ICE's EID and biometric information to IDENT for processing, identification, and verification of identity of individuals encountered or apprehended at the border. e3 transmits data in real-time from USBP agents to EID and IDENT and retrieves records from those systems for CBP enforcement action purposes." Source • "CBP is now implementing technical demonstrations to use **BE-Mobile devices** in the land and sea environments in order to record departures, both biographically and biometrically (including facial images and fingerprints)." Source **USCIS** • **Application Support Center** biometrics appointments collect fingerprints, as well as other biometrics data. Source

Facial Recognition

ICE

- ICE currently uses both commercial and government sources for facial recognition, including **social media images** scraped by Clearview AI. Source
- ICE agents have run millions of searches for driver's license photos at DMVs around the country, using facial recognition to search for matches.[126]
- **ATD check-ins:** Alternatives to Detention technologies include BI SmartLink app (Geo Group) with facial recognition. Source with ATD program stats.
- **EDDIE** facial recognition. Source

CBP

- **e3 Portal:** "USBP agents use e3 to store and transmit biographic information to ICE's EID and biometric information to IDENT for processing, identification, and verification of identity of individuals encountered or apprehended at the border. e3 transmits data in real-time from USBP agents to EID and IDENT and retrieves records from those systems for CBP enforcement action purposes." Source
- "CBP is now implementing technical demonstrations to use **BE-Mobile devices** in the land and sea environments in order to record departures, both biographically and biometrically (including facial images and fingerprints)." Source
- **Incident-Driven Video Recording Systems (IDVRS)** Evaluation: Some law enforcement encounters do not provide the opportunity for CBP Officers/Agents to notify individuals even in close proximity to an incident that their facial image or voice will be/has been recorded. Source
- **Biometric Entry-Exit:** "CBP has successfully operationalized and deployed facial recognition technology, now known as the Traveler Verification Service (TVS), to support comprehensive biometric entry and exit procedures in the air, land, and sea environments." Source

	• **Facial biometric comparison** at Laredo, San Ysidro, Otay Mesa Progreso, Cross Border Xpress, and Tecate Border Crossings for **Simplified Arrival** (facial recognition only). Source Source Source Source • Moving vehicle facial recognition **(Vehicle Face System)** tested at Nogales and Anzalduas. Source (This program had a major security breach.)
Iris Scanning	**CBP** • Iris scan pilot program at Otay Mesa border crossing. Source **DHS Science and Technology Directorate** • In March 2021, DHS held a Biometric Technology Rally aimed to test face and face/iris recognition systems. Source
DNA	**ICE** • "ICE is deploying **Rapid DNA technology** as a factor to determine if removable aliens who represent themselves as a family unit (FAMU) when apprehended by DHS do, in fact, have a bona fide parent-child relationship." Source • As of January 2020: "In order to implement the requirements of the amended regulations, ICE conducts a **DNA sample collection pilot** at one ICE Enforcement and Removal Operations (ERO) facility to determine operational and resource needs for full scale implementation at all ICE locations. Participation in the pilot program is limited to ERO. ICE's Homeland Security Investigation (HSI) will not participate, as the new rule has limited impact on HSI operations because it is already ICE practice to collect DNA samples from individuals, including U.S. Persons, arrested and detained by ICE for criminal prosecution. Under this pilot, ERO is not collecting DNA from U.S. Persons who only commit administrative immigration violations." Source

	CBP • "Effective January 2020, CBP began collecting DNA from any person in CBP custody who is subject to fingerprinting. This includes aliens as well as U.S. citizens and Lawful Permanent Residents (U.S. Persons). As with all other DNA samples that federal law enforcement agencies collect under the authority of the DNA Fingerprint Act, CBP sends DNA samples from its DNA population to the FBI, which enters results into CODIS." Source **DHS (ICE and CBP) for DOJ** • "The DOJ is assisting DHS in developing and implementing a plan to phase in DNA-sample collection from non-U.S. persons who are detained under the authority of the United States, as well as certain U.S citizens and Lawful Permanent Residents (U.S. Persons) who are being arrested or facing criminal charges. The non-U.S. Persons (including those detained for criminal or administrative purposes) have their DNA collected by ICE or CBP designated officers, who follow the collection and submission procedures described in the respective implementation sections below. CBP and ICE send all DNA samples to the FBI Laboratory, which processes the samples and stores the resulting DNA profile in CODIS. NDIS contains the DNA profiles contributed by federal and state agencies and participating forensic laboratories." Source [Method: buccal (cheek) swab]
Voice print	**ICE** • **ATD check-ins:** BI VoiceID (Geo Group) used through 2019. Since then, only "telephonic reporting" is reported statistically. Source with ATD program stats. **CBP** • **Incident-Driven Video Recording Systems (IDVRS):** "Some law enforcement encounters do not provide the opportunity for CBP Officers/Agents to notify individuals even in close proximity to an incident that their facial image or voice will be/has been recorded." Source
Palm print	• Proposed USCIS rule change, which applies to ICE and CBP as well, would require palm prints.

Endnotes

1 US Department of Homeland Security (DHS), "Homeland Advanced Recognition Technology System (HART) Increment 1 Privacy Impact Statement (PIA), DHS/OBIM/PIA-004," February 24, 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf;
US Department of Homeland Security (DHS), "Management Directorate Budget Overview, Fiscal Year 2023 Congressional Justification," 2022, 24, https://www.dhs.gov/sites/default/files/2022-03/Management%20Directorate_Remediated.pdf.

2 US General Accounting Office (GAO), "DHS Annual Assessment: Most Acquisition Programs Are Meeting Goals Even with Some Management Issues and COVID-19 Delays, GAO-22-104684" March 8, 2022, 39, https://www.gao.gov/assets/gao-22-104684.pdf.

3 "The Department of Homeland Security (DHS) initially expected to implement the entire Homeland Advanced Recognition Technology (HART) by 2021; however, no segments of the program have been deployed to date." US Government Accountability Office (GAO), "DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management Systems," June 8, 2021, 1, https://www.gao.gov/products/gao-21-386.

4 DHS, DHS/OBIM/PIA-004; DHS, "Management Directorate Budget Overview Fiscal Year 2023."

5 DHS, DHS/OBIM/PIA-004.

6 Jennifer Lynch, "HART: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' [sic] 'Non-Obvious Relationships,'" Electronic Frontier Foundation, June 7, 2018, https://www.eff.org/deeplinks/2018/06/harthomeland-securitys-massive-new-database-will-include-face-recognition-dna-and.

7 Center for Homeland Defense and Security Naval Postgraduate School, "How DHS Utilizes Biometric Identity," November 22, 2019, video, 12:57, https://www.youtube.com/watch?v=sxR4SP7e17I.

8 DHS, DHS/OBIM/PIA-004, 18.

9 The Request for Proposals (RFP) lays out the desired architecture for HART. Corporations then "bid" on this RFP to build HART. US Department of Homeland Security, "Solicitation Number HSHQDC-16-R-00080," February 13, 2017, https://www.fai.gov/sites/default/files/periodic_table/HART_RFP_HSHQDC-16-R-00080.pdf.

10 US Department of Homeland Security, "FY 2023 Budget in Brief," 14, 2022, https://www.dhs.gov/sites/default/files/2022-03/22-%201835%20-%20FY%202023%20Budget%20in%20Brief%20FINAL%20with%20Cover_Remediated.pdf.

11 In June 2021, the GAO noted that DHS "had decided to combine increments 3 and 4 into a single increment, now referred to as future capabilities." GAO, "DHS Needs to Fully Implement Key Practices," 17; DHS, DHS/OBIM/PIA-004.

12 DHS releases a "Privacy Impact Assessment" (PIA), which is supposed to examine the privacy implications of a new system. In this case, the OBIM PIA for HART only covers Increment 1; OBIM will release additional PIAs when other increments are released.

13 Justin Rohrlich, "Homeland Security will soon have biometric data on nearly 260 million people," Quartz, November 7, 2019, https://qz.com/1744400/dhs-expected-to-have-biometrics-on-260-million-people-by-2022/.

14 Center for Homeland Defense and Security Naval Postgraduate School, "How DHS Utilizes Biometric Identity," 2:43.

15 "Office of Biometric Identity Management," US Department of Homeland Security, accessed May 4, 2022, https://www.dhs.gov/obim.

16 OBIM responses to answers posed by advocates at Just Futures Law, National Immigration Project of the NLG, and National Immigration Law Center. On file with authors.

17 Latent fingerprints ("latent prints") refers to prints deposited on a surface from a person whose identity is unknown.

18 According to the HART PIA, DNA retention is not expected during the first stages of HART. DHS, DHS/OBIM/PIA-004.

19 National Immigration Law Center, "Homeland Advanced Recognition Technology (HART): DHS is Building a Massive Database of Personal Information," November 16, 2021, https://www.nilc.org/wp-content/uploads/2021/12/HART-factsheet-2021-11-10.pdf.

20 DHS, DHS/OBIM/PIA-004.

21 DHS, DHS/OBIM/PIA-004.

22 DHS, DHS/OBIM/PIA-004.

23 Caroline Haskins, "Amazon, Google, Microsoft, and other tech companies are in a 'frenzy' to help ICE build its own data-mining tool for targeting unauthorized workers," Business Insider, September 1, 2021, https://www.businessinsider.com/amazon-google-microsoft-ice-raven-data-mining-tool-undocumented-workers-2021-8?op=1.

24 US Department of Homeland Security (DHS), "Privacy Impact Assessment for the Repository for Analytics in a Virtualized Environment (RAVEn), DHS/ICE/PIA-055," May 13, 2020, 8-9, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice055-raven-may2020.pdf.

25 Lynch, "HART."

26 National Immigration Law Center, "Homeland Advanced Recognition Technology."

27 According to a HART fact sheet, HART will not only make assist with immigration enforcements, but assist with background biometric checks for the U.S. Department of State on more than 30,000 visa applicants, "processing of more than 92,000 international travelers without any increase in wait times at U.S. ports of entry, and 14,000 immigration benefits applicants for U.S. Citizenship and Immigration Services. US Department of Homeland Security (DHS), "Information Paper: Homeland Advanced Recognition Technology (HART)," February, 2020, https://events.afcea.org/FedID20/CUSTOM/pdf/DHS_OBIM_0220_InfoPaper_HART_Final.pdf.

28 "Detention Management Statistics," US Immigration and Customs Enforcement, accessed March 1, 2022, www.ice.gov/detain/detention-management; Aly Panjwani,"ICE Digital Prisons: The Expansion of Mass Surveillance as ICE's Alternative to Detention," Just Futures Law; Mijente, May 2021, https://www.flipsnack.com/justfutures/ice-digital-prisons-1u8w3fnd1j/full-view.html.

29 US Department of Homeland Security, "Privacy Impact Assessment for the ICE Use of Facial Recognition Services, DHS/ICE/PIA-054," May 13, 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.

30 US Department of Homeland Security, "Strategic Framework for Countering Terrorism and Targeted Violence Public Action Plan," September 2020, 3, https://www.dhs.gov/sites/default/files/publications/cttv_action_plan.pdf.

31 US Department of Homeland Security, "Privacy Impact Assessment Update for the Enforcement Integrated Database (EID) – EAGLE, EDDIE, and DAVID, DHS/ICE/PIA-015(j)," May 14, 2019, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-eid-may2019.pdf.

32 U.S. Department of Homeland Security, "Privacy Impact Assessment for theCBP Portal (e3) to EID/IDENT, DHS/CBP/PIA-012(b)," August 10, 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp012-e3-august2020.pdf.

33 Hamed Aleaziz and Caroline Haskins, "DHS Authorities are buying Moment-by-Moment GeolocationCellphone Data to Track People," Buzzfeed News, October 30, 2020, https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation Sarah Morrison, "A surprising number of government agencies buy cellphone location data. Lawmakers want to know why," Vox, December 12, 2020, https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel Byron Tau and Michelle Hackman, "Federal Agencies Use Cellphone Location Data for Immigration Enforcement," Wall Street Journal, Feb. 7, 2020, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

34 GAO, "DHS Needs to Fully Implement Key Practices," 14.

35 Aaron Boyd, "DHS faces rising costs as planned biometrics cloud gets pushed back," Nextgov, June 9, 2021, https://www.nextgov.com/it-modernization/2021/06/dhs-faces-rising-costs-planned-biometrics-cloud-gets-pushed-back/174607/.

36 GAO, "DHS Needs to Fully Implement Key Practices."

37 In June 2021, the General Accounting Office (GAO) issued a report which highlighted HART's repeated schedule delays and cost breaches. According to the GAO's findings, since 2017, "DHS has modified the development contract 12 times and increased the cost to over $143 million" and "pushed out the program's full deployment date by nearly three years (September 2021 to June 2024). GAO, "DHS Needs to Fully Implement Key Practices"; USASpending.gov, "Contract Award HSHQDC17J00370," September 28, 2017-October 31, 2022, accessed May 4, 2022, https://www.usaspending.gov/award/CONT_AWD_HSHQDC17J00370_7001_HSHQDC14DE2035_7001.

38 US Government Accounting Office (GAO), "DHS Annual Assessment: Most Acquisition Programs Are Meeting Goals Even with Some Management Issues and COVID-19 Delays, GAO-22-104684," March 8, 2022, 39, https://www.gao.gov/assets/gao-22-104684.pdf.

39 The price tag for the HART system only became known when the GAO reported information about the contract in January 2021. US Government Accountability Office (GAO), "DHS Annual Assessment: Most Acquisition Programs are Meeting Goals but Data Provided to Congress Lacks Context for Effective Oversight," January 2021, 37-38, https://www.gao.gov/assets/gao-21-175.pdf.

40 "DHS - Homeland Advanced Recognition Technology (HART) / 024-000005253 FY2022," ITDashboard.gov, accessed April 4, 2022, https://viz.ogp-mgmt.fcs.gsa.gov/investment-details/024-000005253.

41 US Department of Homeland Security (DHS), "Management Directorate: Budget Overview, Fiscal Year 2021 Congressional Justification," February 8, 2020, https://www.dhs.gov/sites/default/files/publications/management_directorate.pdf.

42 DHS, "Management Directorate: Budget Overview, Fiscal Year 2023."

43 DHS, "FY 2023 Budget in Brief."

44 DHS, "Management Directorate: Budget Overview, Fiscal Year 2023."

45 GAO, "DHS Needs to Fully Implement Key Practices," 34.

46 ITDashboard.gov, "DHS - Homeland Advanced Recognition Technology (HART) / 024-000005253."

47 "H. Rept. 117-87 - Department of Homeland Security Appropriations Bill, 2022," 117th Congress (2021), May 5, 2022, 21-24, https://www.congress.gov/117/crpt/hrpt87/CRPT-117hrpt87.pdf.

48 US Senate Committee on Appropriations, "Explanatory Statement for the Homeland Security Appropriations Bill," 2022, https://www.appropriations.senate.gov/imo/media/doc/DHSRept_FINAL.PDF.

49 US Senate Committee on Appropriations, "Explanatory Statement."

50 Office of the Chief Procurement Officer, "How to Do Business with DHS," US Department of Homeland Security, last updated September 14, 2020, https://www.dhs.gov/sites/default/files/publications/how_to_do_business_with_dhs_presentation.pdf.

51 "Northrop Grumman wins 95 million award from Department of Homeland Security to develop next generation biometric identification services system," Northrop Grumman, February 26, 2018, https://news.northropgrumman.com/news/releases/northrop-grumman-wins-95-million-award-from-department-of-homeland-security-to-develop-next-generation-biometric-identification-services-system.

52 Valerie Insinna,"Northrop sells IT business to Veritas Capital for $3.4B," Defense News, December 8, 2020, https://www.defensenews.com/industry/2020/12/08/northrop-sells-it-business-to-veritas-capital-for-34b/.

53 GAO, "DHS Needs to Fully Implement Key Practices."

54 "Profile: Ramzi Musallam," Forbes, accessed March 17, 2022, https://www.forbes.com/profile/ramzi-musallam/?sh=3b3a36537648.

55 Naomi Cooper, "Ramzi Musallam, Veritas Capital CEO & Managing Partner, Receives 2022 Wash100 Recognition for Asset Growth Strategy and Fund Management Leadership," GovCon Wire, March 8, 2022, https://www.govconwire.com/2022/03/veritas-capital-ceo-ramzi-musallam-named-to-wash100-for-7th-straight-year/.

56 Cooper, "Ramzi Musallam."

57 USAspending.gov, "Contract Award HSHQDC17J00370."

58 Peraton, "Peraton Strategically Invests in Expanding Government and Customer Relations Capabilities, PR Newswire, March 23, 2022, https://www.prnewswire.com/news-releases/peraton-strategically-invests-in-expanding-government-and-customer-relations-capabilities-301507896.html.

59 "Peraton Completes Acquisition of Perspecta," Peraton, May 6, 2021, https://www.peraton.com/news/peraton-completes-acquisition-of-perspecta/.

60 Susana McDermott, "Nearly one third of Northrop Grumman shareholders voice support for improved human rights due diligence," Interfaith Center on Corporate Responsibility, May 15, 2019, https://www.iccr.org/nearly-one-third-northrop-grumman-shareholders-voice-support-improved-human-rights-due-diligence.

61 McDermott, "Nearly one third of Northrop Grumman shareholders"; "Northrop Grumman Shareholder Resolution," May 15, 2019, https://www.iccr.org/sites/default/files/page_attachments/immig_hr_northop.pdf.

62 "Peraton Awarded $2.685 billion contract to provide data center and cloud optimization support services to U.S. Department of Homeland Security," Peraton, Feb. 16, 2022, https://www.peraton.com/news/peraton-awarded-2-685-billion-contract-to-provide-data-center-and-cloud-optimization-support-services-to-u-s-department-of-homeland-security/.

63 Answers to advocacy questions posed by Just Futures Law, National Immigration Project of the National Lawyers Guild and National Immigration Law Center. On file with authors.

64 "DHS's Automatic Biometric Identification System IDENT – the heart of biometric visitor identification in the USA," Thales, January 19, 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/ident-automated-biometric-identification-system.

65 "NEC Homepage," NEC, accessed March 17, 2022, https://www.nec.com/.

66 USASpending.gov, "Contract Award 70RCSA20C00000006," September 30, 2020-September 29, 2023, accessed May 4, 2022, https://www.usaspending.gov/award/CONT_AWD_70RCSA20C00000006_7001_-NONE-_-NONE-.

67 "Fingerprints Homepage," Fingerprints, accessed March 17, 2022, https://www.fingerprints.com/.

68 DHS, DHS/OBIM/PIA-004.

69 "Amazon.com Inc," Investigate (A Project of The American Friends Service Committee), October 5, 2021), https://investigate.afsc.org/company/amazon; Sam Biddle and Ryan Devereaux, "Peter Thiel's Palantir was Used to Bust Relatives of Migrant Children, New Documents Show," The Intercept, May 2, 2019, https://theintercept.com/2019/05/02/peter-thiels-palantir-was-used-to-bust-hundreds-of-relatives-of-migrant-children-new-documents-show/.

70 Investigate, "Amazon.com Inc."

71 Northrop Grumman's HART contract includes 81 subawards given to 20 subcontractors for computer software and hardware products, accounting for nearly a quarter of the total disbursed funds. These companies include FCN, INC., JAVLIN INC., CARAHSOFT TECHNOLOGY CORP., EMERGENT, LLC, NETAPP, INC., IT1 SOURCE LLC, DLT SOLUTIONS, LLC, NO MAGIC INCORPORATED, CRUNCHY DATA SOLUTIONS, INC., AUGUST SCHELL ENTERPRISES, INC., PLUS3 IT SYSTEMS, LLC, EQUINIX GOVERNMENT SOLUTIONS LLC, GEMALTO COGENT, INC., THE VOLTZ GROUP, BOOZ ALLEN HAMILTON INC., ATHENA SCIENCES CORPORATION, LAKOTA SOFTWARE SOLUTIONS, INC, TTW SOLUTIONS, INC.,OASYS INTERNATIONAL CORPORATION, and STERLING COMPUTERS CORPORATION. For details on these contracts, please see usaspending.gov.

72 USAspending.gov, "Contract Award HSHQDC17J00002," December 23, 2016-December 31, 2020, accessed May 4, 2022, https://www.usaspending.gov/award/CONT_AWD_HSHQDC17J00002_7001_HSHQDC13DE2014_7001.

73 USAspending.gov, "Contract Award HSHQDC15J00177," May 20, 2015-June 7, 2020, accessed May 4, 2022, https://www.usaspending.gov/award/CONT_AWD_HSHQDC15J00177_7001_HSHQDC13DE2065_7001.

74 USAspending.gov, "Contract Award 70RNPP18FR0000002," January 12, 2018-January 14, 2020, accessed May 4, 2022, https://www.usaspending.gov/award/CONT_AWD_70RNPP18FR0000002_7001_HSHQDC14D00006_7001.

75 USAspending.gov, "Contract Award 70RCSA19FR0000011," August 6, 2019-February 5, 2023, accessed May 4, 2022, https://www.usaspending.gov/award/CONT_AWD_70RCSA19FR0000011_7001_GS06F0951Z_4732.

76 USAspending.gov, "Contract Award 70RCSA20FR0000078," September 21, 2020-July 23, 2025, accessed May 4, 2022, https://www.usaspending.gov/award/CONT_AWD_70RCSA20FR0000078_7001_47QTCK18D0003_4732

77 USAspending.gov, "Contract Award HSCEMD17D00001," June 6, 2017-August 31, 2022, accessed May 4, 2022, https://www.usaspending.gov/award/CONT_IDV_HSCEMD17D00001_7012.

78 Secretaría de Gobernación (SEGOB) and US Department of Homeland Security (DHS), "Memorándum de Cooperación entre la Secretaría de Gobernación de los Estados Unidos Mexicanos y el Departamento de Seguridad Nacional de los Estados Unidos de América," April 17, 2013, obtained under the Mexican Federal Law of Transparency and Access to Public Government Information (LFTAIP) from the Mexican Secretariat of the Interior, National Institute of Migration, received August 2018.

79 DHS, "Management Directorate: Budget Overview, Fiscal Year 2023."

80 DHS Agencies include ICE, CBP, USCIS, US Coast Guard, Transportation Security Administration (TSA), Federal Emergency Management Administration (FEMA), U.S. Secret Service (USSS), and the DHS Under Secretary for Management (USM)

81 Department of Defense, "DOD Automated Biometric Identification Systems FY14 Army Programs," 2014, https://www.dote.osd.mil/Portals/97/pub/reports/FY2014/army/2014dodabis.pdf?ver=2019-08-22-110519-453.

82 DHS, DHS/OBIM/PIA-004.

83 "The Eyes Have It, Iris Biometric Added to Next Generation Identification System," FBI, Dec. 11, 2020, https://www.fbi.gov/news/stories/fbi-adds-iris-biometric-to-next-generation-identification-system-121120.

84 US Department of State, "Privacy Impact Assessment Consular Consolidated Database (CCD)," October 2018, https://www.state.gov/wp-content/uploads/2019/05/Consular-Consolidated-Database-CCD.pdf.

85 DHS, DHS/OBIM/PIA-004.

86 US Department of Homeland Security (DHS), "Privacy Impact Assessment for the United Nations High Commissioner for Refugees (UNHCR) Information Data Share, DHS/USCIS/PIA-081," August 13, 2019, https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis081-unhcr-august2019.pdf.

87 US Department of Homeland Security (DHS), "Congressional Budget Justification FY 2017 - Volume II," 2017, https://preview.dhs.gov/sites/default/files/publications/FY%202017%20Congressional%20Budget%20Justification%20-%20Volume%202_1.pdf.

88 US Department of Homeland Security (DHS), "Appendix CC: U.S. Mexico Biometric Immigration Information Sharing," in "NPPD, IDENT Privacy Impact Assessment Appendices, DHS/NPPD/PIA-002," November 2017, 126-136, https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-identappendices-november2017.pdf.

89 DHS, "Appendix CC: U.S. Mexico Biometric Immigration Information Sharing."

90 National Immigration Law Center, "Homeland Advanced Recognition Technology."

91 Juliana Morgan-Trostle, Kexin Zheng, and Carl Lipscombe, The State of Black Immigrants, Black Alliance for Just Immigration and NYU School of Law Immigrant Rights Clinic, 2016, https://stateofblackimmigrants.com/assets/sobi-fullreport-jan22.pdf.

92 DHS, DHS/OBIM/PIA-004,16.

93 US Department of Homeland Security (DHS), "Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL-041 External Biometric Records (EBR) System of Records," Federal Register 83, no. 79 (April 24, 2018): 17829-17833, https://www.federalregister.gov/documents/2018/04/24/2018-08454/privacy-act-of-1974-implementation-of-exemptions-department-of-homeland-securityall-041-external.

94 Lynch, "HART."

95 DHS, DHS/OBIM/PIA-004, 22.

96 DHS, DHS/OBIM/PIA-004, 24.

97 DHS, DHS/OBIM/PIA-004.

98 DHS, DHS/OBIM/PIA-004, 21.

99 DHS, DHS/OBIM/PIA-004.

100 DHS, DHS/OBIM/PIA-004, 8.

101 See, for example: Adi Robertson, "Detroit man sues police for wrongfully arresting him based on facial recognition," The Verge, April 13, 2021, www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-aclu-lawsuit-facial-recognition-wrongful-arrest.

102 Currently, international records are retained for 75 years, and law enforcement records are retained for 75 years after the end of the calendar year in which it was collected. DHS, DHS/OBIM/PIA-004, 28.

103 DHS, DHS/OBIM/PIA-004, 29.

104 DHS, DHS/OBIM/PIA-004, 24.

105 EBR will allow DHS "to receive, maintain, and disseminate biometric and associated biographic information from non-DHS entities, both foreign and domestic." DHS, "Notice of a new system of records," 17831.

106 World Privacy Forum, "Comments of World Privacy Forum to Department of Homeland Security regarding Proposal to Establish a New DHS System of Records, Department of Homeland Security/ALL-041 External Biometric Records (EBR) System of Records and Proposal to Exempt New DHS External Biometric Records (EBR) From Key Provisions of the Privacy Act of 1974," May 24, 2018, 3, http://www.worldprivacyforum.org/wp-content/uploads/2018/06/WPF_Comments_DHS_ExternalBiometricRecordsDatabase_24May2018_fs.pdf.

107 World Privacy Forum, "Comments," 4.

108 US Department of Homeland Security (DHS), "Privacy Threshold Analysis, Version 1-2014," 23, https://www2.epic.org/foia/dhs/hart/EPIC-2018-06-18-DHS-FOIA-20190422-Production.pdf.

109 DHS, DHS/OBIM/PIA-004; DHS, "EBR System of Records, 17766.

110 DHS, "EBR System of Records;" DHS, DHS/OBIM/PIA-004.

111 DHS, DHS/OBIM/PIA-004.

112 DHS, DHS/OBIM/PIA-004, 26.

113 DHS, DHS/OBIM/PIA-004, 27.

114 Chris Burt, "Inside the HART of the DHS Office of Biometric Identity Management," Biometric Update, Sep 4, 2018, https://www.biometricupdate.com/201809/inside-the-hart-of-the-dhs-office-of-biometric-identity-management; GAO, DHS/OBIM/PIA-004.

115 Johana Bhuiyan, "Clearview AI uses your online photos to instantly ID you. That's a problem, lawsuit says," Los Angeles Times, March 9, 2021, https://www.latimes.com/business/technology/story/2021-03-09/clearview-ai-lawsuit-privacy-violations

116 Caroline Haskins, Ryan Mac, and Logan McDonald, "Clearview AI Wants To Sell Its Facial Recognition Software To Authoritarian Regimes Around The World," BuzzFeed News, February 5, 2020, https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22.

117 Caroline Haskins, Ryan Mac, and Brianna Sacks, "A Clearview AI Patent Application Describes Facial Recognition For Dating And Identifying People Who Are Unhoused Or Use Drugs," BuzzFeed News, February 11, 2021, https://www.buzzfeednews.com/article/carolinehaskins1/facial-recognition-clearview-patent-dating.

118 Alfred Ng and Steven Musil, "Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection," CNET, February 5, 2020, https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/.

119 Caroline Haskins, Ryan Mac, and Logan McDonald, "Clearview AI Once Told Cops To "Run Wild" With Its Facial Recognition Tool. It's Now Facing Legal Challenges," BuzzFeed News, January 28, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-cops-run-wild-facial-recognition-lawsuits.

120 Dell Cameron, "Privacy 'Incidents' at DHS on the Rise, Report Says," gizmodo, December 20, 2021, https://gizmodo.com/privacy-incidents-at-dhs-on-the-rise-report-says-1848247337; US Government Accountability Office (GAO), "DHS Privacy: DHS component agencies generally provided oversight of Contractors, but Further Actions are Needed to Address Gaps, GAO-22-104144," December 16, 2021, https://www.gao.gov/products/gao-22-104144.

121 US Department of State (DHS), "Solicitation Number HSHQDC-16-R-00080 - Homeland Advanced Recognition Technology (HART) Office of Biometric Identity Management National Protection and Programs Directorate," Feb.13, 2017, 16, https://www.fai.gov/sites/default/files/periodic_table/HART_RFP_HSHQDC-16-R-00080.pdf.

122 DHS, "Solicitation Number HSHQDC-16-R-00080," 40.

123 DHS, "Solicitation Number HSHQDC-16-R-00080," 16-17.

124 GAO, "DHS Needs to Fully Implement Key Practices," 17.

125 GAO, DHS/OBIM/PIA-004.

126 Friedland, "How ICE Uses Driver's License Photos and DMV Databases." See also: Harwell and Cox, "ICE has run facial-recognition searches on millions of Maryland drivers."

mijente

JUST
FUTURES
LAW

IDP
IMMIGRANT
DEFENSE
PROJECT