Homeland Advanced Recognition Technology (HART): DHS is Building a Massive Database of Personal Information

November 16, 2021

INTRODUCTION

The U.S. Department of Homeland Security (DHS) is surreptitiously assembling an enormous database of personal information called Homeland Advanced Recognition Technology (HART). DHS describes HART as a database containing biometrics and associated biographical information,[1] but it will in fact enable unfettered surveillance of non–U.S. citizens and citizens. Massive amounts of information such as encounter data, officer comments, derogatory information, relationship patterns, and more yet-to-be-disclosed data will also be included.[2] DHS intends to share the information in HART about noncitizens and citizens widely, both domestically and internationally.

HART IS A PUZZLE WITH MANY PIECES MISSING

HART will include a vast, open-ended range of biometrics

DHS's ultimate vision for HART is steeped in vagueness. As the agency outlined in 2015, HART will centralize access to federal and international databases, provide real-time access in the field, and involve the use of "multi-modal biometrics."[3]

While many of the key pieces of HART remain unclear, HART[4] is set to replace DHS's current biometrics database IDENT (Automated Biometric Identification System),[5] which, at present, stores fingerprints, photographs, and signatures.[6] Both IDENT and HART are meant to serve wide-ranging and undefined law enforcement, national security, immigration, and administrative purposes.

DHS currently describes the term biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated recognition" and are "used to detect and prevent

---

[1] Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA DHS/OBIM/PIA-004 (Feb. 24, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf (hereafter HART PIA).

[2] *Id.*

[3] Zack Martin, "Homeland Security Releases Biometric Framework," *Secure ID News*, Aug. 31, 2015, https://www.secureidnews.com/news-item/homeland-security-releases-biometric-framework/. See https://www.dhs.gov/sites/default/files/publications/DHS%20Biometrics%20%20Strategic%20Framework%20Webinar%20Slidedeck%20-%20October%2020%202015_2.pdf for an overview. The Strategic Framework itself no longer appears to be publicly available.

[4] Supplemental Programmatic Environmental Assessment (SPEA) for the Proposed Establishment and Operations of the Office of Biometric Identity Management and the Homeland Advanced Biometric Technology (HART), 81 Fed. Reg. 90862 (Dec. 15, 2016), https://www.govinfo.gov/content/pkg/FR-2016-12-15/pdf/2016-30187.pdf.

[5] DHS describes IDENT as "a centralized and dynamic DHS-wide biometric database that also contains limited biographic and encounter history information needed to place the biometric information in proper context." IDENT System of Records, 72 Fed. Reg. 31080–82 (June 5, 2007), https://www.govinfo.gov/content/pkg/FR-2007-06-05/html/07-2781.htm.

[6] Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), DHS/NPPD/PIA-002, (December 7, 2012), https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf. IDENT currently holds more than 260 million unique identities and processes more than 350,000 biometric transactions per day." https://www.dhs.gov/biometrics.

illegal entry into the U.S., grant and administer proper immigration benefits, [for] vetting and credentialing, facilitating legitimate travel and trade, enforcing federal laws, and enabling verification for visa applications to the U.S."[7]

DHS's fuzzy description of biometrics does not begin to make clear the full range of physical and behavioral characteristics that "biometrics" may encompass. In September 2020, during the Trump administration, DHS issued a Notice of Proposed Rulemaking (NPRM) that offered a sweeping definition of biometrics to include a wide range of intimate physical and behavioral characteristics, such as fingerprints, palm prints, photographs (including "facial images specifically for facial recognition, as well as photographs of physical or anatomical features such as scars, skin marks, and tattoos"), signatures, voice prints, iris images, and DNA test results.[8] DHS, under the Biden administration, withdrew the NPRM.[9]

But there is no indication that the current administration has rejected the NPRM's definition of biometrics or that it will take a narrower approach to expanded biometrics inclusion in HART. In fact, the notice of withdrawal explicitly approved the proposed rule's goal of flexibility in biometrics collection practices and policies and in biometrics use.[10] And, as described below, one of the components of HART – the External Biometric Records (EBR) System of Records – put in place in 2018 an expanded biometrics definition that the withdrawn rule would have authorized, namely, facial images, fingerprints, latent fingerprints, iris images, palm prints, voice prints, scars, marks, and tattoos, DNA or DNA profiles, and other modalities.[11]

DHS is offering clues about how the definition of biometrics could expand even further. The agency recently issued a system of records notice which defined biometric data to include "typing cadence, cardiac signature, [and] vascular patterns."[12] Data about an individual's gait, heart rate, or breathing pattern, and electrodermal activity[13] potentially could be included in a biometrics database.

The little that is publicly known about HART indicates that DHS is anticipating expansions of biometrics collection, handling, and sharing.

---

[7] https://www.dhs.gov/biometrics (last updated June 9, 2021).

[8] Notice of proposed rulemaking. Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, DHS Docket No. USCIS–2019–0007, 85 Fed. Reg. 56338-56422 (Sept. 11, 2020) https://www.govinfo.gov/content/pkg/FR-2020-09-11/pdf/2020-19145.pdf (hereafter NPRM), at 56341.

[9] Collection and Use of Biometrics by U.S. Citizenship and Immigration Services; Withdrawal, DHS Docket No. USCIS– 2019–0007, 86 Fed. Reg. 24750 (May 10, 2021), https://www.govinfo.gov/content/pkg/FR-2021-05-10/pdf/2021-09671.pdf.

[10] *Id.,* at 24750.

[11] Notice of a new system of records. Department of Homeland Security/ALL–041 External Biometric Records (EBR) System of Records, Docket No. DHS– 2017–0039, 83 Fed. Reg. 17829 (Apr. 24, 2018), https://www.govinfo.gov/content/pkg/FR-2018-04-24/pdf/2018-08453.pdf at 17831 (hereafter EBR notice).

[12] Notice of a modified system of records. DHS/Science & Technology Directorate (S&T)-001 Research, Development, Test, and Evaluation System of Records, 86 Fed. Reg. 58084 (Oct. 20, 2021), https://www.govinfo.gov/content/pkg/FR-2021-10-20/pdf/2021-22849.pdf, at 58086.

[13] "Electrodermal activity (EDA; sometimes known as galvanic skin response, or GSR) refers to the variation of the electrical conductance of the skin in response to sweat secretion (often in minute amounts)." Bryn Farnsworth, Ph.D, *What is EDA? And how does it work?*, Imotions (June 4, 2019), https://imotions.com/blog/eda/.

HART's incremental development leaves its full picture unclear

DHS is developing HART in four increments, only the first of which is in progress.

- "HART Increment 1 implements a new data architecture, which includes conceptual, logical, and physical data models, a data management plan, and physical storage of records where each associated record may have multiple associated biometric modality images." HART Increment 1 will include migration to the Amazon Web Services (AWS) GovCloud and will provide mission partners a biometric matching capability based on multiple biometric modalities (fingerprint (including latent prints), face (including a photo), and iris), and additional means by which to identify an individual such as a unique identifier (e.g., Social Security number (SSN), Alien Number (A-Number)). The data and system architecture have been designed for scalability to address projected growth in identity and image data volumes and to accommodate any needs associated with larger files."[14] [footnotes omitted]
- "Increment 2 will provide additional biometric capabilities to HART to meet customer needs and provide increased interoperability with agency partners and improved reporting features."[15]
- "Increments 3 and 4 will include a web portal and user interface capability, support for additional modalities, and improved reporting tools."[16]

These amorphous descriptions offer few clues to HART's ultimate content and use, but clearly indicate that its reach will expand, and that personal information will be consolidated and shared widely. And while DHS issued a Privacy Impact Assessment (PIA) in 2020 about Increment 1 of HART,[17] the agency has not issued a System of Records Notice (SORN) that describes HART's full operation.

HART WILL INCLUDE PERSONAL INFORMATION BEYOND BIOMETRICS

DHS has used piecemeal "system of records" notices (SORNs) to stealthily build HART's enormous capabilities well beyond the problematic biometrics context. The two components that DHS has identified to date are External Biometrics Records (EBR)[18] and Enterprise Biometric Administrative Records (EBAR).[19]

But these records systems will include far more than biometrics and will provide a means for DHS to centralize a wide range of unverified information about noncitizens and citizens that can be shared broadly. Here's what EBR and EBAR will include:

---

[14] HART PIA, *supra*, note 1, at 3.
[15] *Id.*
[16] *Id.*
[17] *Supra*, note 1.
[18] Notice of new system of records, External Biometric Records (EBR) System of Records, DHS/ALL–041 System of Records, Docket No. DHS–2017–0039, 83 Fed. Reg. 17829–33 (Apr. 24, 2018), https://www.govinfo.gov/content/pkg/FR-2018-04-24/pdf/2018-08453.pdf.
[19] Notice of new system of records, Enterprise Biometric Administrative Records (EBAR)S, Docket No. DHS–2019–0047, 85 Fed. Reg. 14955–58 (Mar. 16, 2020), https://www.govinfo.gov/content/pkg/FR-2020-03-16/pdf/2020-04979.pdf.

HART COMPONENT	WHAT'S INCLUDED AND FOR WHAT PURPOSES	SOURCES AND SHARING
DHS/ALL–041 External Biometric Records (EBR) System of Records.	EBR will include biometrics, associated biographic information identifiers for derogatory information, miscellaneous officer comment information, encounter data, and records related to the analysis of relationship patterns among individuals and organizations. The data may be used for law enforcement; national security, immigration screening; border enforcement; intelligence, national defense, and background investigations relating to national security positions, credentialing, and certain positions of public trust.	Allows DHS to receive, maintain, and disseminate biometric and associated biographic information from non-DHS foreign and domestic entities. Either formal or informal information sharing agreements or arrangements or simply the approval of the entity from which information is obtained may be used to obtain "external information."
DHS/ALL–043 Enterprise Biometric Administrative Records (EBAR)	EBAR will cover the administrative and technical records associated with IDENT and HART. DHS's only listed example of EBAR's function is that it will "link individuals with their encounters, biometrics, records, and other data elements."	Sharing of EBAR data within DHS agencies will be based on their "need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions." DHS may also share information with "appropriate" federal, state, local, tribal, territorial, foreign, or international government agencies.

EBR and EBAR will include data from other records systems not mentioned in the notices.

HART will collect data not only from government entities, but according to the 2020 PIA, "HART may use information from publicly available sources, collected according to the data provider's authority. Specific publicly available sources are discussed in more detail in the appropriate data provider's privacy compliance documentation."[20] This unrestricted data collection would prevent oversight, accountability, and transparency of commercial data that finds its way into HART.

Commercial entities have become a major source of data for immigration enforcement.[21] Companies with a record of unfettered biometrics collection, data sharing, and analytics continue to build and host systems for U.S. Immigration and Customs Enforcement (ICE), yet little is known about their contracts or their use, collection, and third-party sharing of data with other federal, local, and state agencies or other companies.[22] And on the infrequent occasions when reviews are performed (for example, the Government Accountability Office's review of U.S. Customs and Border Protection's supervision of companies' compliance with privacy standards for facial recognition programs), DHS's failure to conduct audits was soundly criticized.[23]

HART WILL ENABLE GOVERNMENT SURVEILLANCE

As the table above shows, HART will facilitate DHS's ability to share biometrics and sweeping categories of unverified information, such as derogatory information and relationship patterns, with federal, state, and local law enforcement, intelligence community entities, and foreign governments. But it has not explained transparently when and how this may occur.

In 2018, DHS announced the DHS/USCIS Immigration Biometric and Background Check (IBBC) System of Records.[24] IBBC is a system "to collect and maintain biographic, biometric, and background check records on applicants, petitioners, sponsors, beneficiaries, or other individuals in connection with a benefit request"[25] that may be shared with federal, state, local, tribal, territorial, foreign, or international agencies for a variety of "national security, law enforcement, criminal justice, immigration and border management, and intelligence purposes."[26]

DHS explained that IBBC's records would be stored in IDENT, but it did not even mention the role of HART, which was already in development when the IBBC notice was issued. Since HART will replace IDENT, IBBC's records as well as its increased data-sharing capabilities will become part of HART.

---

[20] *Supra*, note 1 at 18.
[21] *Who's Behind ICE: The Tech and Data Companies Fueling Deportations*, Mijente, National Immigration Project of the National Lawyers Guild, and Immigrant Defense Project, (Aug. 2018), https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf.
[22] Felipe De La Hoz, "DHS Plans to Start Collecting Eye Scans and DNA – with the Help of Defense Contractors," *The Intercept*, Nov. 17, 2020, https://theintercept.com/2020/11/17/dhs-biometrics-dna/; "Immigrant Rights Groups, Law School and Legal Organization FOIA for Info on Thomson Reuters, RELX Group Contracts with ICE," Center for Constitutional Rights press release, Sept. 14, 2020, https://ccrjustice.org/home/press-center/press-releases/immigrant-rights-groups-law-school-and-legal-organization-foia-info.
[23] De La Hoz, *supra* note 22.
[24] Notice of new system of records. Immigration Biometric and Background Check System of Records, docket number DHS–2018–0003, 83 Fed. Reg. 36950 (July 31, 2018), https://www.govinfo.gov/content/pkg/FR-2018-07-31/pdf/2018-16138.pdf.
[25] *Id.* at 36950.
[26] *Id.* at 36951.

In addition, the Trump administration explicitly endorsed a policy of extreme and continuous vetting of noncitizens, based on a "person-centric" model that aggregates data on individuals with biometrics as a key element.[27] The Biden administration's withdrawal of the proposed biometrics rule did not include a rejection of that policy and model.[28]

DHS HAS EXEMPTED HART COMPONENTS FROM NUMEROUS MEANINGFUL PRIVACY ACT PROTECTIONS

DHS is building HART on a foundation of opacity and unaccountability by exempting each component from multiple provisions of the Privacy Act.

DHS recognizes that "[t]he Privacy Act of 1974, 5 U.S.C. 552a, provides protection to individuals by ensuring that personal information collected by federal agencies is limited to that which is legally authorized and necessary, and is maintained in a manner which precludes unwarranted intrusions upon individual privacy."[29] Nonetheless, DHS consistently exempts HART components from the full range of the Privacy Act's accuracy, notice, and redress requirements. For example, DHS exempted EBR from these Privacy Act sections in 5 U.S.C. 552a:[30]

- Provide an accounting to individuals of disclosures: (c)(3) and (4);
- Permit individuals to have access to and request amendment of records that are not accurate, relevant, timely, or complete: (d);
- Only maintain records that are relevant and necessary: (e)(1);
- Collect records directly from the individual to the greatest extent possible: (e)(2);
- Inform the individual of the information's collection and use: (e)(3);
- Notify individuals of procedures to find out if information is about them: (e)(4)(G);
- Notify individuals of the content of records and how to contest their content: (e)(4)(H);
- Maintain records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination: (e)(5)
- Notify individuals when records are made available under compulsory legal process: (e)(8);
- Establish procedures for notice to individuals and review of records: (f);
- Provide a civil remedy when Privacy Act provisions are violated: (g).

[27] Biometrics NPRM, *supra*, note 1, at 56340.
[28] That the Biden administration will expand biometrics collection is illustrated by its failure to withdraw a Trump proposed rule to expand an entry-exit system to collect biometrics, instead re-opening the comment period. https://www.govinfo.gov/content/pkg/FR-2020-11-19/pdf/2020-24707.pdf; https://www.govinfo.gov/content/pkg/FR-2021-02-10/pdf/2021-02699.pdf. And biometrics collection may occur as migrants travel to the US. According to NBC News, "[i]n the long term, according to other documents obtained by NBC News, DHS would collect more biometric data about migrants as they cross borders on the way to the U.S. so more is known about who might soon be approaching the U.S. border…." https://www.nbcnews.com/politics/immigration/biden-admin-build-intelligence-gathering-cell-track-groups-migrants-headed-n1281578.
[29] DHS Privacy Act Statement (Oct. 2020), https://www.dhs.gov/publication/privacy-act-statement.
[30] EBR notice, *supra,* note 11, at 17833.

The HART Increment 1 PIA recognizes that HART presents serious privacy risks.[31] Some risks can't be mitigated at all, such as risks related to the inclusion of derogatory information, information sharing with foreign partners, or inaccurate database "hits" or results for juveniles whose physical characteristics change as they age.[32] And some risks can only be partially mitigated such as data sharing with unauthorized groups, sharing too much data, and the inability of non-U.S. persons to correct inaccurate information.[33]

In addition, whether other risks may be mitigated depends simply on DHS assertions, with no independent evaluations required and minimal processes, if they exist at all, to correct incorrect information. And as mentioned above, DHS's acquisition of commercial data prevents accountability and oversight over that data.

HART HAS BEEN FUNDED DESPITE ITS FAILINGS

HART remains central to DHS's strategic planning.[34] And despite the deficiencies listed above, Congress has provided substantial money for its development. Northrop Grumman was the first "prime contractor"[35] for HART, receiving a $95 million contract with DHS in 2018 to develop increments 1 and 2.[36] Peraton, a subsidiary of the private equity firm Veritas, acquired Northrop Grumman's government information technology business in 2020 and is now HART's prime contractor.[37] HART's lifecycle cost will reportedly exceed $4 billion, and "[o]ver the last few years, Congress has appropriated close to $200 million every year. In FY 2021, Congress appropriated $183 million for HART, including $29 million for new procurement, construction, and improvement."[38]

This substantial funding has not led to effective development and implementation of HART, and HART is not yet operational. In June 2021, the Government Accountability Office (GAO) criticized the significant delays in HART's deployment, as well as DHS's improper characterization of oversight requirements as "low risk" rather than "high risk".[39] Likewise, both

---

[31] Dave Nyczepir, *DHS's forthcoming biometrics system presents unmitigated privacy risks*, Fedscoop (May 6, 2020), https://www.fedscoop.com/dhs-biometrics-system-privacy-risks/

[32] HART PIA, note 1, *supra,* at 24, 29, 32.

[33] HART PIA, note 1, *supra*, at 22, 27, 28, 29, 31, 33, 36.

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

[35] DHS Annual Assessment: Most Acquisition Programs Are Meeting Goals but Data Provided to Congress Lacks Context Needed for Effective Oversight, U.S. Government Accountability Office (Jan. 2021) https://www.gao.gov/assets/gao-21-175.pdf, at 38.

[36] Northrop Grumman Wins $95 Million Award from Department of Homeland Security to Develop Next-Generation Biometric Identification Services System (Feb. 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

[37] Valerie Insinna, *Northrop sells IT business to Veritas Capital for $3.4B*, DefenseNews (Dec. 8, 2020), https://www.defensenews.com/industry/2020/12/08/northrop-sells-it-business-to-veritas-capital-for-34b/; Cal Biesecker, *DHS Still Working on New Schedule for HART Biometric Program*, Defense Daily (2/16/2021) https://www.defensedaily.com/dhs-still-working-new-schedule-hart-biometric-program/homeland-security/.

[38] *Freeze Expansion of the HART Database*, Immigrant Defense Project, Just Futures Law, Mijente (Apr. 2021) https://justfutureslaw.org/wp-content/uploads/2021/04/HART-Appropriations-2022.pdf.

[39] *DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System*, GAO-21-386, Government Accountability Office (June 2021) https://www.gao.gov/assets/gao-21-386.pdf.

the House and Senate Appropriations Committees have recommended in 2021 that DHS funding for HART be reduced by $25 million in fiscal year 2022 because of continuing delays.[40]

But implementation delays should not be the central focus of the GAO's review or appropriations legislation. Rather, the bigger concern for immigrant communities and the public at large is the fact that neither the GAO nor any other entity has conducted any meaningful evaluation of HART's content and use.

The House Appropriations Committee report for the 2022 DHS appropriations bill directed "the OIG to conduct a review of HART technologies, data collection mechanisms, sharing agreements, and privacy protections and determine if OBIM is complying with 28 C.F.R. 23, Criminal Intelligence Systems Operating Policies. Within 180 days of the date of enactment of this Act, the OIG shall brief the Committee on the results of the review."[41] If this provision becomes law, the review may shed some light on HART's functions. But HART Increment 1 has not yet been completed and HART is not yet operational, so any review may also be incomplete. In addition, it is vital that any review cover HART's use for civil immigration purposes, as well as criminal investigations.

The Senate Appropriations Committee's report for the 2022 DHS appropriations bill has a broader transparency and review provision, requesting that DHS "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…" It also calls for "an independent review and evaluation of revised program plans during fiscal year 2022," as well as requiring reporting within 24 hours to the DHS Office of Inspector General and Office for Civil Rights and Civil Liberties if HART is used in family separation cases at the U.S.-Mexico border.[42]

The lack of government accountability and oversight to date has allowed DHS to build HART surreptitiously and to expand governmental surveillance and erode privacy rights for citizens and noncitizens alike.

WHAT YOU CAN DO

Here are some steps that advocates can take:

- Advocate against Congressional funding for HART and for continued House and Senate oversight with results that are made public.[43]

---

[40] Department of Homeland Security Appropriations Bill, 2022, Report of the Committee on Appropriations, https://docs.house.gov/meetings/AP/AP00/20210713/112896/HMKP-117-AP00-20210713-SD002.pdf, at 20-21 (hereafter House Report); Explanatory Statement for the Homeland Security Appropriations Bill, 2022, https://www.appropriations.senate.gov/imo/media/doc/DHSRept_FINAL.PDF, at 20 (hereafter Senate Statement).

[41] House Report, *supra,* note 40 at 24.

[42] Senate statement, *supra* note 40 at 19.

[43] See, e.g., *Freeze Expansion of the HART Database, supra*, note 38.

- Encourage your state and local officials to limit collection and sharing of biometric and other personal information that might become part of HART and be used for immigration enforcement.
- Spread the word about government efforts to collect or share personal or biometric information through community education, social media, and personal contacts, so that community members are aware of the potential changes.
- Join campaigns that target companies with systems that build DHS surveillance capacity and inform their employees of the role their companies play.[44]
- Monitor and keep track of developments as DHS builds HART and expands its surveillance capacity.[45]

[44] See, e.g. No Tech for ICE, https://notechforice.com .
[45] For updates on HART's development and implementation, see, e.g. the National Immigration Law Center, https://nilc.org; Just Futures Law, https://justfutureslaw.org ; Mijente, https://mijente.net ; Electronic Frontier Foundation, https://eff.org; Immigrant Defense Project, immigrant defense project.org