May 24, 2022

Adam Selipsky
Chief Executive Officer
Amazon Web Services

Dear Mr. Selipsky,

We the undersigned human rights, immigrant rights, and digital rights organizations write to express our urgent concerns and begin a dialogue about Amazon Web Service's (AWS) hosting of the U.S. Department of Homeland Security's (DHS) Homeland Advanced Recognition Technology (HART) biometric database.

According to a new report from immigrant rights groups, DHS will rely on AWS to host this new database, which will vastly expand its surveillance capabilities and supercharge the deportation system. HART will be the largest biometric database in the U.S., initially holding and sharing invasive personal and biometric data on over 270 million people, including 6.7 million iris scans and 1.1 billion face images.

HART has been under construction since 2016 and will aggregate data from U.S. federal agencies, local and state police, and foreign governments. When final, the database will include data on children, adults, immigrants, and U.S. citizens, including unsubstantiated information on people's relationships, physical characteristics, religion, and travel patterns.

This mass biometric data collection by DHS is a deep invasion of privacy, an assault on human rights, and places hundreds of millions of people at risk of raids, detentions, deportations, and family separation. **By hosting DHS' HART database, AWS is directly facilitating the creation of an invasive biometrics database that will supercharge surveillance and deportation, risking human rights violations.**

We request that Amazon Web Services end its agreement to host HART, due to the many concerns outlined below:

I. Mass surveillance

HART not only undermines our rights to privacy and data protection, but also threatens our rights to free assembly and association, and freedom of expression. HART is a tool of mass surveillance, which will most violently harm immigrants and Black and brown communities already targeted by discriminatory policing.

Biometrics are sensitive data that reveals intimate information about a person's identity. Since this information is unique to a person, once it is collected the person is forever exposed to targeted

surveillance —causing irreparable harm. This threatens the human rights of government dissenters, and all our rights to protest, assemble, associate, and live our daily lives.

In addition to immigration authorities, DHS plans to make HART interoperable with several U.S. federal agencies, UNHCR, and foreign governments. Right now, DHS is amassing massive amounts of biometric data on people in countries across Latin America and the Caribbean, as the U.S. government continues to externalize its borders and train foreign immigration officers. To date, the U.S. government has been training officers in Mexico, El Salvador, Guatemala, the Dominican Republic, Jamaica, and the Bahamas to collect biometric information of people seeking to immigrate to the United States — all of this data would be stored in the HART database on AWS servers.

II. Discrimination

HART also undermines our rights to equality and non-discrimination. This is because collecting sensitive information makes it possible to develop incredibly detailed profiles of people, including everything from race to eye color to ancestry. This will fuel the existing policing and targeting of noncitizens and communities of color in discriminatory ways.

For example, DHS could leverage HART to target criminalized communities by using iris scanners. This has already happened across the U.S. and along the U.S.-Mexico border. ICE — which *Georgetown's Center on Privacy and Technology* calls a "domestic surveillance agency" — has used biometric scanners, such as the "EDDIE" app, to racially profile people for arrests and deportation. What's more, this technology and its data sharing impacts the rights of migrants and their families who disproportionately face retaliation, injury, and other harm by immigration authorities.

III. Data protection risks

The HART database is rife with data protection concerns, as DHS's own Office of Biometric Identity Management's HART Privacy Impact Assessment makes abundantly clear. These risks are exacerbated given there is no comprehensive federal data protection law in the United States. Our main data protection concerns include:

No informed consent: DHS acknowledges that people will not be able to fully consent to DHS collecting, storing, and sharing their data through HART. In many if not most cases, DHS will store people's personal and biometric data in HART without their knowledge.

Inaccurate and assumed data: DHS claims it "cannot ensure accuracy" and quality of the data in HART, since it says it does not actually own the data in the system. DHS officers and non-DHS data providers will also be able to enter unsubstantiated information about people's encounters, personal relationships, political affiliations, and religious activities, with little oversight or confirmation. Data may also come from private companies that already contract with DHS and ICE, including Clearview AI and data broker LexisNexis, which have been criticized for human rights violations and inaccuracies in data. In addition, there is significant racial bias inherent to biometric data collection.

Unacceptable data retention: HART will retain data for at least 75 years, and information may never be deleted.

Risks of rampant data sharing: HART's data will be shared with various local, state, tribal, and other federal agencies, as well as some foreign governments, but DHS has refused to share full information about these data sharing agreements.

No real methods for redress: People whose data is collected and stored in HART do not have an accessible way to challenge or correct erroneous biometric and biographic information.

These concerns lead us to ask several pressing questions to Amazon Web Services:

- **Did you perform a human rights due diligence before agreeing to host the HART database?**
- **What steps, if any, have you taken to identify, address, and mitigate the human rights risks of hosting sensitive biometric data? What steps will AWS take in case of human rights violations associated with the HART database?**
- **Are there any agreements on liabilities regarding the information AWS hosts? Do your agreements include any provisions on human rights obligations?**

As outlined in the UN Guiding Principles on Business and Human Rights, private companies have a duty to respect and promote people's human rights. AWS is no exception. **This is a critical moment for your company to live up to its commitments and end AWS' agreement to host HART. This would help ensure that AWS does not support and facilitate dangerous technology that puts people's privacy, security, and other fundamental rights at risk.**

We ask you to begin a constructive dialogue by meeting with us to discuss our concerns and by publicly responding to this letter by June 7.

Your policies and practices have an indelible impact on society. We encourage you to prioritize people's lives and well-being over your profit margins.

Signed,

ORGANIZATIONS

Access Now
Action Center on Race and the Economy (ACRE)
American Baptist Home Mission Societies
Asian Americans Advancing Justice - Asian Law Caucus
Asian Americans Advancing Justice | AAJC
Asociación por los Derechos Civiles (ADC)
Athena Coalition
Barracón Digital - Honduras
Coalición de Derechos Humanos
Coding Rights
comun.al, Digital resilience laboratory - Mexico
Demos
Electronic Privacy Information Center (EPIC)
Fight for the Future
Fundación InternetBolivia.org
Immigrant Defense Project
Inter-Faith Committee on Latin America
Investor Advocates for Social Justice
Investor Alliance for Human Rights
Just Futures Law
Kairos
La Resistencia
Make the Road New York
Media Alliance
MediaJustice
Mijente
Muslim Justice League
National Immigrant Justice Center
National Immigration Law Center
Oakland Privacy
R3D: Red en Defensa de los Derechos Digitales
Ranking Digital Rights
Respond Crisis Translation
Restore the Fourth
Seventh Generation Interfaith Coalition for Responsible Investment
Sisters of Charity of St. Elizabeth
Sisters of St. Francis of Philadelphia
Sursiendo - Mexico
Surveillance Technology Oversight Project (STOP)