epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA EMAIL

June 18, 2018

Sam Kaplan
Chief Privacy Office/ Chief FOIA Office
The Privacy Office
U.S. Department of Homeland Security
245 Murray Lane SW
STOP-0655
Washington, D.C. 20528-0655

Dear Mr. Kaplan,

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Department of Homeland Security ("DHS").

EPIC seeks the DHS's Privacy Impact Assessment ("PIA") for DHS's Homeland Advanced Recognition Technology ("HART") and related records.

Documents Requested

(1) The required PIA conducted for HART.

(2) Any Privacy Threshold Analysis or similar initial privacy assessment that assessed the need for a PIA for HART.

Background

The DHS's Automated Biometric Identification ("IDENT") system, which is used for processing and storing biometric and associated biometric information,[1] houses a gallery with over 220 million unique identities.[2] Implemented in 1994,[3] the current IDENT system can process 300 hundred thousand daily transactions.[4] Use of biometric data in the DHS has

[1] *DHS/NPPD/PIA-002 Automated Biometric Identification System*, U.S. Dep't of Homeland Sec. (Nov. 17, 2017), https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.
[2] *Biometrics*, U.S. Dep't of Homeland Sec. (Feb. 6, 2017), https://www.dhs.gov/biometrics.
[3] U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the Automated Biometric Identification System (Dec. 12, 2012), https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system-ident.
[4] Mark Crego & Janice Kephart, *What it Will Take for the Department of Homeland Security to be Successful in Biometrics, and a revised definition of 'fusion'*, Identity Strategy Partners, https://www.identitystrategy.com/single-post/2017/02/03/DHS-Office-of-Biometric-Identity-

increased significantly, and the agency now seeks to expand its biometric capacity and capability.[5]

As part of this large-scale shift towards biometrics, the DHS has announced it will replace IDENT with HART.[6] The HART system features expanded capacity, functionality, and an increase in transaction speed.[7] It will support a multitude of biometric data including: facial images, fingerprints, iris images, voice, DNA, "scars, marks and tattoos," and "other modalities."[8] It will also contain biometric-associated data such as personal physical details, citizenship identifiers, "derogatory information," and "miscellaneous officer comment information."[9] HART's data will be disseminated to other Federal government agencies, the intelligence community, state and local law enforcement, and foreign governments.[10] Relative to IDENT, HART's system will offer a "broader range of service" to these third parties.[11]

As discussed in greater detail below, Section 208 of the E-Government Act of 2002 requires the federal government conduct PIAs on its data collection and storage systems in order to ensure the protection of personal information.[12] In assessing privacy risks associated with IDENT, DHS identified numerous dangers including the collection of data without an individual's knowledge, incorrect matching of biographic (e.g. physical details) and biometric data (e.g. fingerprints), over-collection of information, excessively long retention of data, and the dissemination of individual's data with 3rd parties who do not have the appropriate authority or need for the data.[13]

There are likely even greater risks associated with a more advanced system such as HART that seeks to utilize the latest biometric technologies. For example, facial recognition, a biometric that will be deployed in the HART system, can be used for the real-time identification and surveillance of individuals.[14] Such uses can result not only in a loss of anonymity but also the chilling of free speech. Unlike fingerprints, facial biometric data can be collected without an

---

Management-Outlining-Mission-Success-in-the-Modernization-of-Existing-System-and-Reassessing-the-Definition-of-Fusion.

[5] *Id.*

[6] *DHS reveals details of RFP for HART*, Planet Biometrics (Mar. 9, 2017), http://www.planetbiometrics.com/article-details/i/5614/desc/dhs-reveals-details-of-rfp-for-hart.

[7] *Id.*

[8] HART: *Privacy Act of 1974; System of Records*, 83 Fed. Reg. 17289 (Proposed Apr. 24, 2018).

[9] *Id.*

[10] *DHS reveals details of RFP for HART*, *supra* note 6.

[11] *Id.*

[12] *E-GOVERNMENT ACT OF 2002*, U.S. Dep't of Justice (June 18, 2014), https://www.justice.gov/opcl/e-government-act-2002.

[13] U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the Automated Biometric Identification System (Dec. 12, 2012), https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system-ident.

[14] *See* Jeramie Scott, *Facial Recognition Surveillance is Here — But Privacy Protections Are Not*, The Hill (June 13, 2017), http://thehill.com/blogs/pundits-blog/technology/341906-opinion-facial-recognition-surveillance-is-here-but-privacy.

individual's knowledge — a photo can easily be captured from afar.[15] Moreover, research at Massachusetts Institute of Technology shows that leading facial recognition technology has greater difficulty correctly identifying females and those with darker skin relative to males and those with lighter skin.[16] Error rates neared 35% for females with darker skin.[17] The heavy burden of misidentification that will result from such algorithmic bias will fall disproportionately on minority communities. Despite these well-known problems, DHS maintains that facial recognition biometrics is a priority for the HART database.[18]

The DHS's rapidly expanding use of biometric data has come under scrutiny by Congress and the U.S. Government Accountability Office ("GAO"). Senators Edward Markey (D-MA) and Mike Lee (R-UT) expressed concerns last year about the Biometric Exit program and specifically the DHS's use of facial biometric data at airports.[19] They made clear that "Congress has not authorized face scans on American citizens" and said that that DHS should suspend the program. Their letter also highlighted the troubling gender and race-based accuracy problems associated with the use of facial recognition.[20] The GAO criticized the DHS for its failure to both "assesses the value of collecting biometric data" and to provide an "evaluation framework" for its Biometric Exit program, which aims to use biometric identifiers for travel and immigration-related security.[21]

The existence of plans to develop HART have been made known to the public.[22] HART, like its predecessor IDENT, clearly constitutes a system of data collection subject to the production of a PIA under the E-government Act of 2002.

PIA Requirement

According to Section 208 of the E-Government Act, an agency is required to undertake a Privacy Impact Assessment ("PIA") when a federal agency "develop[s] or procur[es] information technology that collects, maintains, or disseminates information that is in an identifiable form," and (2) when an agency "initiat[es] a new collection of information" that

---

[15] *See* EPIC, *Spotlight on Surveillance: The FBI's Next Generation Identification Program: Big Brother's ID System?*, (Dec. 2013), https://epic.org/privacy/surveillance/spotlight/ngi.html; *see also* Clare Garvie, et al., *Perpetual Line Up*, Georgetown Law Center on Privacy & Technology (Oct. 18, 2016), https://www.perpetuallineup.org.

[16] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. of Machine Learning Res., 1, 1 (2018), https://dam-prod.media.mit.edu/x/2018/02/05/buolamwini-ms-17_WtMjoGY.pdf.

[17] *Id.*

[18] U.S. Gov't Accountability Office, GAO-18-339SP, Homeland Security Acquisitions: Leveraging Programs' Results Could Further DHS's Progress to Improve Portfolio Management (2018), https://www.gao.gov/assets/700/691817.pdf.

[19] *Id.*

[20] *Id.*

[21] Letter from Edward J. Markey, Sen. Mass., et al., to Kirstjen Nielson, Sec., U.S. Dep't of Homeland Sec. (Dec. 21, 2017), https://www.markey.senate.gov/download/dhs-biometrics-markey-lee-letter.

[22] *DHS reveals details of RFP for HART*, Planet Biometrics (Mar. 9, 2017), http://www.planetbiometrics.com/article-details/i/5614/desc/dhs-reveals-details-of-rfp-for-hart.

"includes any information in an identifiable form."[23] This identifiable information, referred to as personally identifiable information ("PII"), is any information in a program or system that allows the identity of an individual to be directly or indirectly inferred.[24] The Office of Management and Budget ("OMB"), for the purposes of the E-Government Act, follows the Clinger-Cohen Act definition of information technology: "any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information."[25]

The OMB further states: "Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection." PIAs at the "IT development stage":

> 1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
>
> 2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;
>
> 3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.[26]

Like its predecessor, IDENT, HART triggers Section 208 obligations. HART's system constitutes "information technology that collects, maintains, or disseminates information that is in an identifiable form," HART will be collect, maintain, and disseminate PII — specifically, biometric and associated biometric data. Moreover, the DHS has already "commence[d]" the "development" of HART, which means the PIA must already be completed. The HART contract

---

[23] E-Government Act of 2002, Pub. L. No. 107-347, § 208 (b)(1)(A)(i)-(ii), 116 Stat. 2899 (2002).
[24] U.S. Dep't of Homeland Sec., Privacy Impact Assessments: The Privacy Office Official Guidance 4 (2010), https://www.dhs.gov/sites/default/files/publications/privacy_pia_guidance_june2010_0.pdf [hereinafter DHS PIA Official Guidance].
[25] Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6) (2011) (emphasis added); *See* Exec. Office of the President, Office of Mgmt and Budget, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf [hereinafter OMB E-Government Act Guidance].
[26] OMB E-Government Act Guidance, *supra* note 25, at 5–6 (emphasis added).

was awarded to Northrup Grumman in February 2018[27] and DHS timelines appear to indicate that the HART implementation will be complete in the 2019 fiscal year.[28]

Pursuant to Section 208, the DHS Privacy Office requires that every technology system complete a Privacy Threshold Analysis ("PTA") as a first step in its Certification and Accreditation process, an internal security and operating compliance process that seeks to assure that the information technology systems meet the appropriate standards.[29] If the DHS Privacy Office determines that the DHS program or system has privacy implications, then it will require additional privacy compliance documentation, including a Privacy Impact Assessment.

Records regarding the Privacy Impact Assessment for the HART system should be in the possession of the agency.

Request for Expedition

This request warrants expedited processing under the FOIA and the DHS's FOIA regulations. 5 U.S.C §552(a)(6)(E)(v)(II); 6 C.F.R. § 5.5(e)(1)(ii). Specifically, this request is entitled to expedited processing because there is an "urgency to inform the public about an actual or alleged federal government activity," and because the request is "made by a person who is primarily engaged in disseminating information." §5.5(e)(1)(ii).

First, the development of a new, publicly acknowledged DHS system for processing and storing biometric and associated biometric information constitutes an "actual… federal government activity." "Urgency" to inform the public about HART's collection, use, retention and dissemination of their personal data is clear given the magnitude of the privacy risks associated with its predecessor, IDENT, as well as the rapid timeline for its phased implementation, in which the first deployment was initially set for December 2018.[30] Additionally, HART's expanded capabilities relative to IDENT, and its prioritization of high risk technologies such as facial recognition introduce added risks that must be accounted for. These considerations are further magnified by the vast network of agencies, state and local governments and foreign partners who will have access to HART.

Second, EPIC is an organization "primarily engaged in disseminating information." 6 C.F.R. §5.5(e)(1)(ii). As the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media'" entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

---

[27] *Northrop Grumman Wins $95 Million Award from Department of Homeland Security to Develop Next-Generation Biometric Identification Services System*, Northrop Grumman (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.
[28] U.S. Gov't Accountability Office, GAO-18-339SP, *supra* note 18.
[29] DHS PIA Official Guidance, *supra* note 24, at 1; *See also* Privacy Compliance: Privacy Threshold Analysis (PTA), Dept. of Homeland Sec. (Mar. 30, 2017), https://www.dhs.gov/compliance.
[30] *Id.*

In submitting this request for expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. 6 C.F.R. § 5.5(e)(3); 5 U.S.C. § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. DOD*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because (i) "disclosure of the requested information is in the public interest because it is likely to contribute to the public understanding of the operations or activities of the government" and (ii) "disclosure of the information is not primarily in the commercial interest" of EPIC, the requester. 6 C.F.R. § 5.11(k)(1); 5 U.S.C. § 552(a)(4)(A)(iii). EPIC's request satisfies this standard based on the DHS's considerations for granting a fee waiver. 6 C.F.R. §§ 5.11(k)(2–3).

(1) Disclosure of the requested information is likely to contribute to the public understanding of the operations or activities of the government.

Disclosure of the requested documents is "in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government." 6 C.F.R. § 5.11(k)(2). DHS components evaluate four considerations to determine whether this requirement is met: (i) the "subject of the request must concern identifiable operations or activities of the federal government, with a connection that is direct and clear, not remote or attenuated"; (ii) disclosure "must be meaningfully informative about government operations or activities in order to be 'likely to contribute' to an increased public understanding of those operations or activities"; (iii) "disclosure must contribute to the understanding of a reasonably broad audience of persons interested in the subject, as opposed to the individual understanding of the requester," and (iv) "[t]he public's understanding of the subject in question must be enhanced by the disclosure to a significant extent." *Id.*

First, the subject of the request clearly concerns "identifiable operations or activities of the federal government." 6 C.F.R. § 5.11(k)(2)(i). HART will replace IDENT, the DHS's system for processing and storing biometric and associated biometric information.

Second, disclosure would be "meaningfully informative" regarding the government activity and is thus "'likely to contribute' to an increased understanding of government operations or activities." Not only does disclosure of the requested documents fulfill the requirements of Section 208 of the E-Government Act of 2002, but it provides the public transparency into the DHS's collection, use, dissemination and retention of their personal data.

Third, disclosure will "contribute to the understanding of a reasonably broad audience of persons interested in the subject" because, as provided in the DHS FOIA regulations, DHS components will "presum[e] that a representative of the news media will satisfy this

consideration." 6 C.F.R. § 5.11(k)(2)(iii). Additionally, it is likely HART data will include the personal information of a significant segment of the American public. HART seeks to expand IDENT's database, which houses over 220-million unique identities.[31] The DHS's growing use of biometrics, and specifically facial recognition, have also drawn congressional and academic criticism.[32]

Fourth, the public's understanding of DHS's use of biometric data will "be enhanced by the disclosure to a significant extent." The public is currently unaware of how the transition to HART will impact the collection, use, retention and dissemination of their personal data. As with IDENT, a PIA will provide substantial amounts of previously unknown information regarding the scope, policies and procedures associated with the DHS's biometric data system, the privacy risks the DHS has identified and the steps the DHS is taking to mitigate such risks.

(2) Disclosure of the information is not primarily in the commercial interest of the requester

The "[d]isclosure of the information is not primarily in the commercial interest" of EPIC. § 5.11(k)(3). The DHS components evaluate two considerations in assessing this requirement: (i) whether there are "any commercial interest of the requester . . . that would be furthered by the requested disclosure"; and/or (ii) whether "the public interest is greater than any identified commercial interest in disclosure" and "[c]omponents ordinarily shall presume that where a news media requester has satisfied the public interest standard, the public interest will be the interest primarily served by disclosure to that requester." *Id.*

First, there is no "commercial interest of the requester . . . that would be furthered by the requested disclosure." 6 C.F.R. § 5.11(k)(3)(i). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[33] EPIC has no commercial interest in the requested records.

Second, "the public interest is greater than any identified commercial interest in disclosure." 6 C.F.R. § 5.11(k)(3)(ii). Again, EPIC is a non-profit organization with no commercial interest in the requested records and has established that there is significant public interest in the requested records. Moreover, the DHS should presume that EPIC has satisfied 6 C.F.R. § 5.11(k)(3)(ii). The DHS FOIA regulations state "[c]omponents ordinarily shall presume that where a news media requester has satisfied the public interest standard, the public interest will be the interest primarily served by disclosure to that requester." *Id.* Here, EPIC is a news media requester and this request should satisfy the public interest standard.

For these reasons, a full fee waiver should be granted for EPIC's request.

---

[31] *Biometrics,* U.S. Department of Homeland Security (last updated Feb. 6, 2017), https://www.dhs.gov/biometrics.
[32] *See, e.g.* Letter from Edward J. Markey, Sen. Mass., et al., to Kirstjen Nielson, Sec., U.S. Dep't of Homeland Sec., *supra* note 21; Harrison Rudolph, et.al, *Not Ready for Take-Off*, Georgetown Law Center on Privacy & Technology (Dec. 21, 2017), https://www.airportfacescans.com.
[33] *About EPIC*, EPIC.org, http://epic.org/epic/about.html.

Conclusion

Thank you for your consideration of this request. I anticipate your determination on our request within ten calendar days. 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x104 or Zhou@epic.org, cc: FOIA@epic.org.

Respectfully submitted,

/s Sherry Safavi
Sherry Safavi
EPIC Summer Clerk

/s Jeramie D. Scott
Jeramie D. Scott
EPIC National Security Counsel

/s Enid Zhou
Enid Zhou
EPIC Open Government Fellow