epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

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

VIA EMAIL

June 10, 2020

Fernando Pineiro
FOIA Officer
U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street, S.W., Stop 5009
Washington, D.C. 20536-5009
Email: ICE-FOIA@dhs.gov

Dear Mr. Pineiro:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to U.S. Immigration and Customs Enforcement ("ICE").

EPIC seeks records related to the agency's use of facial recognition software ("FRS").

Documents Requested

1. All contracts between ICE and commercial FRS vendors;
2. All documents related to ICE's approval process for new commercial FRS vendors, including but not limited to:
    a. Document detailing the approval process and requirements for commercial FRS vendors
    b. Documents related to the approval of all commercial FRS vendors currently in use by ICE
    c. Documents related to reviewing commercial FRS vendors that have been used under "exigent circumstances" without prior approval;
3. All training materials and standard operating procedures for Homeland Security Investigations ("HSI") agents regarding use of FRS, including but not limited to the following:
    a. Existing training materials and standard operating procedures around HSI agent use of FRS
    b. Existing training materials and standard operating procedures regarding restrictions on the collection of probe photos

c. Training materials and standard operating procedures being developed for HSI agent use of FRS
d. Training materials and standard operating procedures being developed regarding the use of probe photos;

4. All audits conducted by the ICE Office of Professional Responsibility or by HSI supervisors related to HSI agent use of FRS, including but not limited to:
    a. All audits conducted on commercial FRS vendors
    b. All audits of the ICE Investigation Case Management system case files that include use of FRS;
5. All documents related to agreements between ICE and law enforcement agencies regarding use of law enforcement agency FRS, including but not limited to:
    a. Memorandums of understanding ("MOU") or other documents of agreement between ICE and law enforcement agencies regarding use of law enforcement agency FRS
    b. Documents detailing ICE's approval process and requirements for law enforcement agency FRS
    c. Documents related to ICE's approval of all law enforcement agency FRS currently in use by ICE
    d. Documents related to ICE reviewing law enforcement agency FRS that have been used under "exigent circumstances" without prior approval.

Background

On May 13, 2020, the Department of Homeland Security released a Privacy Impact Assessment ("PIA") for ICE's use of facial recognition services.[1] The PIA details how HSI agents use FRS.[2] According to the PIA, HSI agents use FRS to generate candidate lists to identify unknown persons or to locate unknown persons.[3] HSI agents typically submit facial images called probe photos that are collected during routine investigative activity.[4] The PIA lists procedures that HSI agents must follow when submitting probe photos to the FRS, including the requirement that HSI agents must first make "reasonable efforts" to identify an unknown individual through "existing means and methods."[5] After using the FRS, HSI agents are supposed to vet any potential match from the FRS using other available information before using the potential match as a lead should use any information received from the FRS as a lead, and use other available information as corroboration for the information received from the FRS.[6] According to the PIA, leads returned from FRS are "never the sole basis used to establish probable cause, determine wrongdoing, or deny a benefit."[7] The PIA does not include information on the current training that HSI agents receive on these procedural requirements, but does state that ICE Privacy and HSI are working to create trainings for

[1] U.S. Dep't of Homeland Sec., 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 [hereinafter ICE PIA].
[2] *Id.* at 5.
[3] *Id.*
[4] *Id.* at 6.
[5] *Id.*
[6] *Id.* at 10.
[7] *Id.* at 11.

HSI agents regarding the proper procedure surrounding use of FRS.[8] The PIA also does not identify specific requirements regarding how HSI agents may collect probe photos,[9] but does state that ICE will be developing training for HSI agents on how to maximize image quality of probe photos.[10]

The PIA also states that the HSI Operational System Development and Management unit ("OSDM") must approve all FRS being used by ICE.[11] Under "exigent circumstances," HSI agents may seek approval from HSI supervisors to use a FRS that has not been reviewed by OSDM.[12] Afterwards, OSDM will conduct a review of the FRS that was used.[13] According to the PIA, HSI supervisors regularly audit agent case files to ensure that FRS is being used properly,[14] and case files will also be audited by ICE Office of Professional Responsibility to ensure that the system is being used properly.[15]

Finally, the PIA details the types of different facial recognition services currently in use by HSI. The PIA specifies four different categories: FRS from state and local law enforcement agencies,[16] FRS from intelligence fusion centers,[17] FRS from federal agencies (which include DHS's own facial recognition service),[18] and FRS from commercial vendors.[19]

There has been growing concern over ICE's use of facial recognition technology, particularly its partnership with law enforcement agencies. The PIA revealed that some of FRS provided by state and local law enforcement agencies may connect directly with associated Department of Motor Vehicle ("DMV") databases.[20] According to the PIA, some states have granted HSI offices access to submit probe photos directly to their FRS.[21] The PIA does not specify which state and local law enforcement agencies it works with, and which states have granted HSI offices direct access.

But media outlets have identified certain states that have granted direct access to ICE. On February 26, 2020, the *Washington Post* reported that ICE officials had logged nearly 100 sessions into Maryland's state's driver's license database since 2018, raising concerns that ICE was exploiting Maryland's laws that allow undocumented immigrants to hold driver's licenses.[22] Soon

---

[8] *Id.* at 22.
[9] *Id.* at 23.
[10] *Id.* at 27
[11] *Id.* at 7.
[12] *Id.*
[13] *Id.*
[14] *Id.* at 22, 25.
[15] *Id.* at 25.
[16] *Id.* at 12.
[17] *Id.* at 13.
[18] *Id.*
[19] *Id.* at 16.
[20] *Id.* at 12.
[21] *Id.*
[22] Drew Harwell & Erin Cox, *ICE Has Run Facial-Recognition Searches on Millions of Maryland Drivers*, Wash. Post (Feb. 26, 2020), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/.

after, Maryland state lawmakers proposed legislation that would require ICE agents to get a warrant if they wanted to access Maryland's motor vehicle records and diver license pictures.[23]

Similarly, on Feb 29, 2020, Utah state lawmakers introduced a bill that imposes limits on the use of facial recognition technology, and would declare that the Utah Department of Public Safety is the only government entity in the state authorized to use a facial recognition system.[24] The Utah bill came as a result of increased scrutiny on ICE using facial recognition technology to search the Utah's DMV databases, first reported by the *Washington Post* and the *New York Times* on July 7, 2019.[25] The *New York Times* also reported that ICE had used facial recognition technology on Vermont's DMV photos.[26]

There has also been increasing concern over ICE's use of commercial FRS vendors. The PIA detailed that HSI works with commercial vendors who provide facial recognition services. These commercial vendors "maintain their own repository of images," some of which may be obtained by "'scraping' internet websites."[27] According to the PIA, HSI will discontinue use of a commercial FRS if it discovers that the FRS violates the privacy settings of an open source system.[28] The PIA does not include any information on what qualifies as a violation of privacy settings. The PIA does not specify which commercial vendors ICE works with, and does not specify if ICE has previously relied on any FRS that violated the privacy settings of an open source system.

Media outlets have reported that ICE relies on facial recognition technology that violates the terms of service and privacy settings of online social media sites. On February 27, 2020, *Buzzfeed News* reported that ICE had contracted with Clearview AI, a startup that provided facial recognition software that scrapes online websites and social media for images.[29] According to the *New York Times*, Clearview AI collects images by "scraping" Facebook and other social media sites, which is against the terms of service of these sites.[30] There has been widespread concern about the privacy

---

[23] Kevin Rector, *ICE Has Access to Maryland Driver's License Records. State Lawmakers Want to Limit It.,* Balt. Sun (Feb. 26, 2020), https://www.baltimoresun.com/politics/bs-md-pol-ice-mva-bill-20200227-rsgqqajmwne4hollsz4svgpa6m-story.html.
[24] S.B. 218, 2020 Gen. Sess. (Utah 2020), *available at* https://le.utah.gov/~2020/bills/static/SB0218.html; *see also* Ben Winslow, *Bill to Regulate Facial Recognition Technology in Utah is Unveiled in the Legislature*, Fox 13 Salt Lake City (Feb. 29, 2020), https://www.fox13now.com/news/local-news/bill-to-regulate-facial-recognition-technology-in-utah-is-unveiled-in-the-legislature.
[25] Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, Wash. Post (Jul. 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/; Catie Edmonson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. Times (Jul. 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.
[26] Edmonson, *supra* note 25.
[27] ICE PIA, *supra* note 1, at 16.
[28] *Id.* at 16–17.
[29] Ryan Mac, Caroline Haskins, & Logan McDonald, *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, Buzzfeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.
[30] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

risks posed by Clearview AI, and other similar commercial FRS vendors.[31] Despite these risks, ICE has not publicly announced that it will discontinue the use of Clearview AI. ICE also has not disclosed if it relies on other commercial FRS vendors, which may pose concerns similar to those posed by Clearview AI.

Request for Expedited Processing

EPIC is entitled to expedited processing of this request 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." 6 C.F.R. §5.5(e)(1)(ii).

First, there is "urgency to inform the public concerning actual or alleged federal government activity." 6 C.F.R. § 5.5(e)(1)(ii). ICE's use of facial recognition technology constitutes an "actual . . . federal government activity." There is "urgency" to release the requested information because ICE use of FRS poses serious privacy concerns that are not adequately addressed in the PIA. According to the PIA, individuals have very limited ability to consent to their images being used in FRS, and to access or amend any of their images being used in FRS.[32] In FRS maintained by federal, state, and local agencies, images are often collected in "non-consensual" situations, like mugshots, where individuals do not have the ability to consent to their image being collected.[33] Even in "consensual" situations, an individual who opts out of having their image collected may forfeit the ability to use the service—for example, those who opt out of presenting a photo for a visa may forfeit the ability to get a visa.[34] In a commercial FRS, an individual may correct, update, or remove images in the open source system from which the image was collected, but those changes may not be reflected in FRS.[35] The PIA admits that this is an "unmitigated" risk.[36] The PIA also fails to address the concern that many facial recognition systems might be biased.[37] While the PIA lays out procedure to mitigate the risk of a FRS returning an incorrect result,[38] it does not address the concern of bias or contain any mitigating measures.

There is further "urgency" because there is significant interest in the federal government's use of facial recognition technology. On February 12, 2020, Senators Jeff Merkley (D-OR) and Cory Booker (D-NJ) introduced the *Ethical Use of Facial Recognition Act*, which would institute a moratorium on all federal governmental use of technology until Congress passes legislation

---

[31] *See id.*
[32] *See* ICE PIA, *supra* note 1, at 20–21.
[33] *Id.* at 20.
[34] *Id.*
[35] *Id.* at 21
[36] *Id.*
[37] *See* Patrick Grother, Mei Ngan & Kayee Hanaoka, Face Recognition Vendor Test (FRVT), National Institute of Standards and Technology (Dec. 12, 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; *see also* Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.
[38] ICE PIA, *supra* note 1, at 27.

regulating it.[39] Several state governments, including New York, Massachusetts, Hawaii, and Michigan, are also considering bans on facial recognition technology.[40]

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). EPIC is a non-profit organization committed to privacy, open government, and civil liberties that consistently discloses documents obtained through FOIA on its website, EPIC.org, and its online newsletter, the *EPIC Alert*.[41]

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

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); 6 C.F.R. § 5.11(d)(1)–(2).

Further, any duplication fees should also be waived because disclosure is (1) "in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government" and (2) "not primarily in the commercial interest of" EPIC, the requester. 5 U.S.C. § 552(a)(4)(A)(iii); 6 C.F.R. § 5.11(k)(1). 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 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). The DHS evaluates four factors to determine whether the "public interest" condition is met: (i) the "subject of the request must concern identifiable operations or activities of the federal government"; (ii) disclosure must be "meaningfully informative about government operations or activities"; (iii) disclosure "must contribute to the understanding of a reasonably broad audience of persons interested in the subject"; and (iv) "[t]he public's understanding of the subject in

[39] Ethical Use of Facial Recognition Act, S.3284, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/3284; *see also* Press Release, Sen. Jeff Merkley, Merkley Booker Introduce Legislation to Prohibit Irresponsible Government Use of Facial Recognition Technology (Feb. 12, 2020), *available at* https://www.merkley.senate.gov/news/press-releases/merkley-booker-introduce-legislation-to-prohibit-irresponsible-government-use-of-facial-recognition-technology-2020.

[40] *See* Ryan Tracy, *Tech Firms Seek to Head Off Bans on Facial Recognition*, Wall Street J. (March 8, 2020), https://www.wsj.com/articles/tech-firms-seek-to-head-off-bans-on-facial-recognition-11583498034.

[41] EPIC, *About EPIC*, https://epic.org/epic/about.html.

question must be enhanced by the disclosure to a significant extent." *Id*. EPIC's request satisfies all four factors.

First, the requested records clearly "concern identifiable operations or activities of the Federal Government" 6 C.F.R. § 5.11(k)(2)(i). The PIA refers to procedures that HSI agents must follow when using FRS,[42] the requirement that OSDM approve all FRS before use,[43] and audits that HSI supervisors and the ICE Office of Professional Responsibility conduct.[44] The PIA also refers to agreements between ICE and law enforcement agencies and commercial FRS vendors.[45]

Second, disclosure of the requested records is "'likely to contribute' to an increased public understanding of those operations or activities." 6 C.F.R. § 5.11(k)(2)(ii). Disclosure would "be meaningfully informative about government operations or activities" because the agency has not released any more information about its use of FRS. *Id.*

Third, disclosure will "contribute to the understanding of a reasonably broad audience of persons interested in the subject," because DHS components must "presume[] that a representative of the news media," such as EPIC, "will satisfy this consideration." 6 C.F.R. § 5.11(k)(2)(iii). The requested records will reach a large audience through EPIC's widely read website, https://epic.org, where EPIC routinely posts and interprets privacy-related government documents obtained under the FOIA. EPIC's FOIA work is also frequently covered through major media outlets. [46]

Fourth, "[t]he public's understanding of the subject in question [will] be enhanced by the disclosure to a significant extent." 6 C.F.R § 5.11(k)(2)(iv). The PIA laid out general procedure that HSI agents are expected to follow when using FRS, but the degree of training that agents receive about these requirements are unknown. The extent to which the procedures are followed is also unknown. The PIA also referenced ICE's use of FRS provided by law enforcement agencies, but did not disclose which law enforcement agencies it works with or which ones have granted HSI agents direct access to FRS. Similarly, the PIA referenced ICE's use of commercial FRS vendors, but did not specify which vendors it uses, and the extent to which ICE evaluated these vendors before approving them. The requested records will clarify the public's understanding on all of these issues.

(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. 6 C.F.R. § 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.*

---

[42] *See* ICE PIA, *supra* note 1, at 5.
[43] *See id.* at 9.
[44] *See id.* at 22, 25.
[45] *See id.* at 12, 16.
[46] *See* EPIC, *EPIC in the News*, https://epic.org/news/epic_in_news.php/.

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.[47] 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 satisfies the public interest standard.

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

Conclusion

Thank you for your consideration of this request. EPIC anticipates your determination on its request within ten calendar days. 5 U.S.C. § 552(a)(6)(E)(ii)(I); 6 C.F.R. § 5.5(e)(4). For questions regarding this request contact Enid Zhou at 202-483-1140 x104 or zhou@epic.org, cc: FOIA@epic.org.

Respectfully Submitted,

/s/ Tracy Zhang
Tracy Zhang
EPIC Clerk

/s/ Enid Zhou
Enid Zhou
EPIC Open Government Counsel

[47] EPIC, *About EPIC*, http://epic.org/epic/about.html.