October 19, 2020

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

U.S. Customs and Border Protection
FOIA Officer
90 K Street, NE
FOIA Division
Washington, D.C. 20229

U.S. Department of Homeland Security
Dena Kozanas
Chief Privacy Officer/Chief FOIA Officer
Privacy Office, Mail Stop 0655
2707 Martin Luther King Jr. Ave SE
Washington, D.C. 20528-0655
foia@hq.dhs.gov

Via email, U.S. Mail, and online portal

Re: Freedom of Information Act request regarding use of Clearview AI Facial Recognition Software

To Whom It May Concern:

We write on behalf of Mijente, Immigrant Defense Project (“IDP”), Just Futures Law (“JFL”), and the American Civil Liberties Union of Northern California (“ACLU-NC”) (“Requesters”) to request records related to the acquisition and use of Clearview AI facial recognition software by U.S. Immigration and Customs Enforcement (“ICE”), U.S Customs and Border Protection (“CBP”), and the U.S. Department of Homeland Security (“DHS”). This request is made pursuant to the Freedom of Information Act, 5 U.S.C. § 522 et seq., implementing regulations 6 C.F.R. § 5.1 et seq., and any other applicable regulations.
We ask that you direct this request to all appropriate offices, components, divisions, and/or directorates within ICE, CBP and DHS, including but not limited to Homeland Security Investigations (“HSI”) and the Office of Biometric Identity Management (“OBIM”) divisions of ICE.¹

The Requesters seek records related to ICE, CBP and DHS’s plans for, acquisition of, and past and present use of Clearview AI’s facial recognition technology.² In this letter, “facial recognition” means the use of an automated or semi-automated process to identify or attempt to identify a person based on the characteristics of their face. Clearview AI technology employs facial recognition software to map, collect, and/or monitor facial features from photographs or videos gathered from a vast array of sources including but not limited to websites and social media profiles.

The Requesters seek these records to provide the public with greater understanding of how ICE, CBP and DHS use facial recognition technology in immigration enforcement activities.

I. Background

Facial recognition technology affords government and private actors the unprecedented ability to identify, locate, and track individuals, raising serious civil and human rights and civil liberties concerns. Foremost among those concerns is the impact of the technology on Black people and other over-policed communities, drawing them further into criminal and immigration systems. Facial recognition has been repeatedly demonstrated to be less accurate when used to identify Black people, people of Asian descent, and women.³ Last December, the National Institute of Standards and Technology released results for a comprehensive study of facial recognition systems finding that African American and Asian people were up to 100 more times likely to be misidentified than white men, depending on the algorithm and use case.⁴ These findings built on an earlier ACLU study, in which 1 in 5 California legislators were erroneously matched to a mugshot of persons who have been

---

² The term “records” as used herein includes all records or communications preserved in written or electronic form, including but not limited to: correspondence, documents, data, videotapes, audio tapes, emails, faxes, files, guidance, guidelines, evaluations, instructions, analyses, memoranda, agreements, notes, orders, policies, procedures, protocols, reports, rules, training manuals, other manuals, or studies. With respect to privacy concerns for members of the public, we will accept copies that are redacted to protect identifying information such as names, social security numbers, and alien numbers, but we would object to the redaction of birthdates and birthplaces that would interfere with our ability to determine the ages and countries of origin for members of the public. In addition, we request that members of the public whose identifying information is redacted be identified with an alphanumeric code so that multiple records related to the same individual will be recognized as such. This redaction agreement does not apply to identifying information such as names and badge numbers for federal agents.
³ Black and Brown people, especially women and young people, are more likely to be misidentified by discriminatory algorithms like facial recognition systems that are built using biased data. See Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research,(2018) http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
arrested, with facial recognition disproportionately misidentifying lawmakers of color.\(^5\) Many face recognition algorithms also misgender transgender and gender nonconforming people, while others purport to identify a person’s sexual orientation by relying on and perpetuating harmful stereotypes about physical appearance.\(^6\) These inaccuracies have led to wrongful detentions for crimes people did not commit, such as the false arrest of Robert Julian-Borchak Williams recently documented in the *New York Times*.\(^7\)

Even when the technology accurately identifies people, it poses an unprecedented threat to individuals’ privacy and security. Over the past several years, face recognition systems have been used to criminalize poverty, facilitate mass arrests and incarceration of ethnic and racial groups, surveil demonstrators exercising their First Amendment rights at protests, and target immigrants for deportation.\(^8\) Last year, *the New York Times* reported that ICE officials had mined state driver’s license databases using facial recognition technology, analyzing millions of driver photos without their knowledge.\(^9\) Clearview AI is a software company that has significantly expanded the reach of facial recognition by scraping and scanning billions of personal photos from the internet, including social media sites, to create a massive database. Clearview AI sells access to this trove of information to both law enforcement agencies and private businesses. It has provided accounts to a range of international entities and police departments, including those in countries with explicit anti-LGBTQ laws.\(^10\) This development of a massive facial recognition database makes it possible to find people’s names and social media accounts or identify them as they protest, shop, and seek essential and sensitive government services.

In recent years, DHS, ICE and CBP have deployed mass surveillance tools and purchased access to databases of personal information to target, arrest, and detain immigrants. Reporters have uncovered records revealing that dozens of accounts registered to ICE and CBP agents have run thousands of facial recognition searches with the Clearview AI technology.\(^11\) Most recently, ICE purchased access to the Clearview AI technology and services under Contract ID 70CMSD20P0000130. These agencies have amassed a horrifying record of medical abuse, forced

---


\(^9\) Id.


\(^11\) Id.
family separation, discrimination and psychological torture.\(^\text{12}\) The Requesters, the immigrant communities they serve, and the public have an urgent need to know whether the social media services on which they rely to connect with family and friends are being exploited for facial recognition and deportation.

**II. Records Requested from DHS, ICE and CBP**

We request the following records:

1. The purchase order or contract entered into between ICE and Clearview AI under Contract Award ID 70CMSD20P00000130 (the “Contract”), along with any purchase records, purchase orders, invoices, sole source letters or justifications, budget request, and grant applications.

2. All requests for quotations or proposals issued by ICE that led to the award of the Contract.

3. All records identifying the companies, individuals, or vendors that submitted quotations, proposals, or submissions in connection with the Contract.

4. All records identifying the list(s) of facial recognition technology vendors approved for acquisition and/or use by DHS and any of its offices, components and/or directorates, including but not limited to all Facial Recognition Services (“FRS”) used by ICE as specified in Privacy Impact Assessment DHS/ICE/PIA-054 (May 2020).\(^\text{13}\) This includes FRS classified under several types, namely: "State and Local Facial Recognition Services," "Regional and subject matter-specific intelligence fusion centers," "Federal Agency Facial Recognition Services," and "Commercial Vendors," the last of which includes Clearview AI facial recognition technology.

5. Purchase records related to Clearview AI facial recognition technology, including but not limited to requests for proposal, purchase orders, invoices, sole source letters or justifications, budget requests, and grant applications, that were created or operative on or after September 1, 2017.

---


6. Draft or finalized agreements related to Clearview AI facial recognition software and the above transactions, including but not limited to e-mail negotiations, contracts, memoranda of understanding, terms of service, and master services agreements, that were created or operative on or after September 1, 2017.

7. Correspondence among or between DHS, CBP and ICE personnel and/or an individual or agency acting on behalf of DHS, CBP, and ICE, regarding Clearview AI facial recognition technology, including but not limited to e-mails, internal reports or dossiers, and instant messages\(^\text{14}\), that were created on or after September 1, 2017.

8. Correspondence between DHS, CBP and ICE personnel and/or an individual or agency acting on behalf of DHS, CBP, and ICE, and any employee of Clearview AI, that was created on or after September 1, 2017. Please search for all email communications to and from help@clearview.ai; and all email communications to and from email accounts utilizing the “clearview.ai” email domain.

9. All records relating to how the Clearview AI facial recognition product or service functions (or malfunctions), including manuals, instructions, training materials, e-mails, handouts, PowerPoint presentations, advertisements, or specification documents, that were created on or after September 1, 2017. Please include all records that describe validation, accuracy, reliability, and policy compliance of Clearview AI technology.

10. All manuals, policies, procedures, and practices governing the use or monitoring of Clearview AI facial-recognition products or services or related information or databases, that were created on or after September 1, 2017. This request includes, but is not limited to:
   a. Procedures for and restrictions on using, minimizing, deleting, or retaining photos of subjects to be identified;
   b. Records identifying any sources of such photos, such as mobile devices, body cameras, surveillance videos, social media photos, identification photos, or arrest photos;
   c. Policies or procedures relating to the legal standard, if any, (e.g. probable cause, court order, relevance, consent) that is required before using Clearview AI’s facial recognition product or service;
   d. Procedures ICE, CBP and DHS follow after a positive result generated by Clearview AI, such as requiring independent or in-person verification; and
   e. Permitted uses of the information created from a positive match.

11. Training materials related to any Clearview AI products or services by employees of ICE, CBP and DHS, that were created on or after September 1, 2017.

12. All records indicating the number of DHS personnel and/or individuals acting on behalf of DHS, including personnel and individuals working for or acting on behalf of HSI or

---
\(^{14}\) For purposes of this request, “instant messages” means any electronic messages other than email, including but not limited to chat messages (i.e., Google Apps, Slack, Skype) and text messages.
Enforcement and Removal Operations divisions, that possess accounts that provide access to any Clearview AI product, service, or technology.

13. All records indicating the number of ICE personnel and/or individuals acting on behalf of ICE, including personnel and individuals working for or acting on behalf of HSI or Enforcement and Removal Operations divisions, that possess accounts that provide access to any Clearview AI product, service, or technology.

14. All records indicating the number of CBP personnel and/or individuals acting on behalf of CBP, that possess accounts that provide access to any Clearview AI product, service, or technology.

15. All records indicating the number of facial recognition scans or queries initiated by ICE, CBP and DHS personnel utilizing Clearview AI products or services on or after September 1, 2017, including but not limited to daily, weekly, monthly, and/or annual datasets, logs, and/or reports. Please include the “audit log” Clearview AI makes available to the designated agency administrator(s).

16. All records indicating the number of positive and negative facial recognition results generated via Clearview AI facial recognition software on or after September 1, 2017, including but not limited to daily, weekly, monthly, and/or annual datasets, logs, and/or reports. Please include the “audit log” Clearview AI makes available to the designated agency administrator(s).

17. All records identifying any sources of photos utilized by ICE, CBP and DHS for purposes of initiating or conducting Clearview AI facial recognition scans or queries, including but not limited to sources such as mobile devices, body cameras, surveillance videos, social media sites, traditional newspapers and/or magazines, digital newspapers and/or magazines, aerial surveillance, identification photos, arrest photos, and/or photos collected or stored by other federal, state, or local agencies.

18. All records indicating the number of warrant applications, warrants, arrests and/or prosecutions associated with a facial recognition scan or query utilizing Clearview AI conducted on or after September 1, 2017, including warrant applications, warrants, arrests or prosecutions where a facial recognition scan or query was not cited as a basis for a warrant application, the issuance of a warrant, an arrest, or a prosecution.

19. All manuals, policies, procedures, and practices that were created or operative on or after September 1, 2017 regarding the use or monitoring of Clearview AI facial-recognition products or services or related information or databases. This request includes, but is not limited to:

   a. Any Privacy Impact Assessments;
   b. Procedures for and restrictions on using, minimizing, deleting, or retaining photos of subjects to be identified;
c. Records identifying any sources of such photos, such as mobile devices, body cameras, surveillance videos, social media photos, identification photos, or arrest photos;

d. Policies or procedures relating to the legal standard, if any, (e.g. probable cause, court order, relevance, consent) that is required before using Clearview AI’s facial recognition product or service;

e. Procedures ICE, CBP and DHS follow after a positive result generated by Clearview AI, such as requiring independent or in-person verification; and

f. Permitted uses of the information created from a positive match.

III. Expedited Processing

We request expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E) and the statute’s implementing regulations. There is a “compelling need” for these records, as defined in the statute and regulations, because there is urgency to inform the public concerning actual or alleged Federal Government activity and the request has been made by a group of organizations primarily engaged in disseminating information. See 5 U.S.C. § 552(a)(6)(E)(v); 6 C.F.R. § 5.5(e)(1)(ii).

First, Mijente, IDF, JFL and the ACLU-NC are requesters “primarily engaged in disseminating information.” 5 U.S.C. § 552(a)(6)(E)(v)(II); 6 C.F.R. § 5.5(e)(1)(ii).

i. Mijente

Mijente Support Committee is a national organization that coordinates and organizes with its members in several states to address issues relating to immigration enforcement and Latinx political participation. Among the campaigns run by Mijente Support Committee is #NoTechForICE, launched in 2019 (https://notechforice.com/). Mijente plans to analyze and disseminate to the public the information gathered through this Request at no cost, and the records are not sought for any commercial purpose.

ii. Immigrant Defense Project

Immigrant Defense Project is a non-profit organization whose mission is to promote fundamental fairness for immigrants accused or convicted of crimes. IDP works to protect and expand the rights of immigrants who have contact with the criminal legal system, including: 1) working to transform unjust deportation laws and policies; 2) minimizing the harsh and disproportionate immigration consequences of contact with the criminal legal system; and 3) educating and advising immigrants, their criminal defenders, and other advocates. IDP disseminates information about the immigration system to the public in accessible ways and is a leader in providing training and support for legal practitioners, community-based organizations, and community members. IDP provides expert information and community-based education on ICE tactics, including surveillance practices, and possible legal and policy remedies. IDP plans to analyze and disseminate to the public the information gathered through this Request at no cost, and the records are not sought for any commercial purpose.
iii. Just Futures Law

Just Futures Law is a non-profit organization that works in partnership with immigrant and racial justice organizers and base-building groups to develop legal and advocacy strategies aimed at disrupting criminalization and deportation; file litigation aligned with organizing; and build a political home for lawyers and legal workers who center directly-impacted communities in the immigrants’ rights movement. JFL disseminates information about the immigration system to the public in accessible ways and is a leader in providing training and support for legal practitioners, community-based organizations, and community members. JFL provides expert information and community-based education on ICE tactics, including surveillance practices, and possible legal and policy remedies. JFL plans to analyze and disseminate to the public the information gathered through this Request at no cost, and the records are not sought for any commercial purpose.

iv. ACLU of Northern California

The ACLU-NC is a non-profit organization and an affiliate of the ACLU, a national organization that works to protect civil liberties of all people, including the safeguarding of the basic constitutional rights to privacy, free expression, and due process of law. The ACLU-NC is responsible for serving the population of northern California. ACLU-NC staff persons are frequent spokespersons in television and print media and make frequent public presentations at meetings and events. The ACLU-NC plans to analyze and disseminate to the public the information gathered through this Request at no cost, and the records are not sought for any commercial purpose.

Dissemination of information about actual or alleged governmental activity is a critical and substantial component of the ACLU-NC’s mission and work. The ACLU-NC actively disseminates and frequently garners extensive media coverage of the information it obtains about actual or alleged government activity through FOIA and California’s statutory counterpart, the California Public Records Act. It does so through a heavily visited website (averaging around 31,000 visitors per week) and a paper newsletter distributed to 92,000 members. In the past, FOIA requests, litigation over FOIA responses, and information obtained by the ACLU-NC through FOIA about the federal government’s immigration enforcement, ethnic and racial profiling, and detention operations have been the subject of articles on the ACLU-NC’s website. They have also garnered coverage by other news media. ACLU-
NC staff persons are frequent spokespersons in television and print media and make frequent public presentations at meetings and events.

Courts have found that the ACLU and similar organizations are “primarily engaged in disseminating information” for purposes of expedited processing under FOIA. See ACLU v. Dep’t of Justice, 321 F. Supp. 2d 24, 30 n.5 (D.D.C. 2004) (finding that a non-profit, public interest group that “gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience” is “primarily engaged in disseminating information” (internal citation omitted)); see also Leadership Conference on Civil Rights v. Gonzales, 404 F. Supp. 2d 246, 260 (D.D.C. 2005) (finding Leadership Conference—whose mission is to “disseminate[] information regarding civil rights and voting rights to educate the public [and] promote effective civil rights laws”—to be “primarily engaged in the dissemination of information”).


There is an urgent need to inform the public of the nature of the contracts ICE currently holds with Clearview AI and how Clearview AI’s facial recognition technology is being deployed to identify, locate, track, and target immigrants for detention and/or deportation. Requesters Mijente, Immigrant Defense Project, Just Futures Law, and the ACLU-NC represent and work for communities whose members are being arrested, detained, and deported every day, potentially in part on the basis of information collected, analyzed and provided to ICE, CBP and DHS by facial recognition companies like Clearview AI. Recent reports of medical abuses like forced sterilizations occurring in ICE detention facilities have generated increased public interest and concern about the human rights abuses associated with ICE enforcement activities, and the involvement of information technology companies such as Clearview AI in ICE operations. This request will inform an urgent ongoing debate about the use of facial recognition tracking by government agencies, and specifically seeks to inform the public’s understanding of how federal agencies utilize data obtained via Clearview AI in immigration enforcement.

IV. Application for Waiver or Limitation of Processing Fees

A. Release of the records is in the public interest

We request a waiver of search, review, and reproduction fees on the grounds that disclosure of the requested records is in the public interest because it is likely to contribute significantly to the public understanding of the United States government’s operations or activities and is not primarily in the commercial interest of the requester. 5 U.S.C. § 552(a)(4)(A)(iii); 6 C.F.R. § 5.11(k).

As discussed above, numerous news accounts reflect the considerable public interest in the requested records. Given the ongoing and widespread media attention to this issue, the records sought by the Request will significantly contribute to the public understanding of the operations and activities of DHS, CBP and ICE, and will be of interest to a broad interest. See 6 C.F.R. § 5.11(k)(1)(i), (k)(2)(iii). In addition, disclosure is not in the Requesters’ commercial interests. As described above, any information disclosed as a part of this FOIA Request will be available to the public at no cost. Thus, a fee waiver would fulfill Congress’s legislative intent in amending FOIA. See Judicial Watch Inc. v. Rossotti, 326 F.3d 1309, 1312 (D.C. Cir. 2003) (“Congress amended FOIA to ensure that it be 'liberally construed in favor of waivers for noncommercial requesters.’”) (citation omitted); OPEN Government Act of 2007, Pub. L. No. 110-175, § 2, 121 Stat. 2524 (finding that “disclosure, not secrecy, is the dominant objective of the Act,” quoting Dep’t of Air Force v. Rose, 425 U.S. 352, 361 (1992)).

B. Requesters qualify as representatives of the news media.

A waiver of search and review fees is warranted because Requesters qualify as “representative[s] of the news media” and the requested records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii); see also 6 C.F.R. §§ 5.11(b)(6), (k)(2)(iii). Accordingly, fees associated with the processing of this request should be “limited to reasonable standard charges for document duplication.” Requesters meets the statutory and regulatory definitions of “representative[s] of the news media” because they are “entit[ies] that gather[] information of potential interest to a segment of the public, use[] [their] editorial skills to turn the raw materials into a distinct work, and distribute[] that work to an audience.” 5 U.S.C. § 552(a)(4)(A)(ii)(II); see also Nat’l Sec. Archive v. Dep’t of Def., 880 F.2d 1381, 1387 (D.C. Cir. 1989); cf. ACLU v. Dep’t of Justice, 321 F. Supp. 2d 24, 30 n.5 (D.D.C. 2004) (finding nonprofit public interest group to be “primarily engaged in disseminating information”). Requesters are “representative[s] of the news media” for the same reasons that they are “primarily engaged in the dissemination of information.” See Elec. Privacy Info.Ctr. v. Dep’t of Def., 241 F. Supp. 2d 5, 10–15 (D.D.C. 2003) (finding nonprofit public interest group that disseminated an electronic newsletter and published books was a “representative of the news media” for FOIA purposes). The ACLU-NC recently was held to be a “representative of the news media.” Serv. Women’s Action Network v. Dep’t of Def., No. 3:11CV1534 (MRK), 2012 WL 3683399, at *3 (D. Conn. May 14, 2012); see also ACLU of Wash. v. Dep’t of Justice, No. C09-0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding ACLU of Washington to be a “representative of the news media”), reconsidered in part on other grounds, 2011 WL 1900140 (W.D. Wash. May 19, 2011).
V. Conclusion

Pursuant to the applicable statute and regulations, we expect a determination regarding expedited processing within ten (10) calendar days. See 5 U.S.C. § 552(a)(6)(E)(ii)(I); 6 C.F.R. § 5.5(e)(4).

If this request for information is denied in whole or in part, we ask that you justify all deletions by reference to specific exemptions to the Freedom of Information Act. We expect you to release all segregable portions of otherwise exempt material in accordance with 5 U.S.C. § 552(b). We reserve the right to appeal a decision to withhold any information.

Thank you for your prompt attention to this matter. If we can provide any clarification that will help expedite your attention to our request, please contact us at (415) 621-2493. Please furnish all applicable records to jjones@aclunc.org if in electronic format, or, if in physical form, at 39 Drumm St. San Francisco, CA 94111.

I affirm that the information provided supporting the request for expedited processing is true and correct to the best of my knowledge and belief.

Executed on the 19th day of October 2020.

Sincerely,

Vasudha Talla
Immigrants’ Rights Program Director
ACLU Foundation of Northern California

Jennifer Jones
Technology & Civil Liberties Fellow
ACLU Foundation of Northern California

Sejal Zota
Legal Director
Just Futures Law

Mizue Aizeki
Interim Executive Director
Immigrant Defense Project