

1 VASUDHA TALLA (SBN 316219)  
2 AMERICAN CIVIL LIBERTIES UNION  
3 FOUNDATION OF NORTHERN CALIFORNIA  
4 39 Drumm Street  
5 San Francisco, California 94111  
6 Phone: (415) 621-2493 ext. 308  
7 Facsimile: (415) 255-8437  
8 vtalla@aclunc.org

9 *Attorney for Plaintiffs*

10  
11  
12 **UNITED STATES DISTRICT COURT**  
13 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**  
14 **SAN FRANCISCO-OAKLAND DIVISION**  
15

16 AMERICAN CIVIL LIBERTIES UNION OF  
17 NORTHERN CALIFORNIA; MIJENTE  
18 SUPPORT COMMITTEE; JUST FUTURES  
19 LAW; and IMMIGRANT DEFENSE  
20 PROJECT,

21 *Plaintiffs,*

22 v.

23 U.S. IMMIGRATION AND CUSTOMS  
24 ENFORCEMENT; U.S. CUSTOMS AND  
25 BORDER PROTECTION; and U.S.  
26 DEPARTMENT OF HOMELAND  
27 SECURITY,

28 *Defendants.*

**COMPLAINT FOR  
DECLARATORY AND  
INJUNCTIVE RELIEF FOR  
VIOLATION OF THE FREEDOM  
OF INFORMATION ACT,  
5 U.S.C. § 552 ET SEQ.**

**INTRODUCTION**

1  
2 1. This is an action under the Freedom of Information Act (“FOIA”), 5 U.S.C. §552 *et*  
3 *seq.*, to enforce the public’s right to records of U.S. Immigration and Customs Enforcement’s  
4 (“ICE”), U.S. Customs and Border Protection’s (“CBP”), and the U.S. Department of Homeland  
5 Security’s (“DHS”) use of facial recognition surveillance technology to identify, locate, and track  
6 individuals.

7 2. Facial recognition is a biometric technology that uses an automated or semi-  
8 automated process to identify or attempt to identify a person based on the distinguishable  
9 characteristics of their face. The technology is frequently deployed by private companies, local law  
10 enforcement agencies, and other government entities to verify the identity of a known person or  
11 determine the identity of an unknown person.

12 3. Facial recognition affords government and private actors the unprecedented ability to  
13 identify, locate, and track individuals, raising serious civil and human rights and civil liberties  
14 concerns. Use of the technology can lead to unwanted tracking and invasive surveillance, making it  
15 possible to instantly identify individuals at protests, houses of worship, and medical facilities, among  
16 other sensitive locations.

17 4. Facial recognition exacerbates the harms experienced by Black people and other  
18 over-policed communities, drawing them further into the criminal and immigration systems. For  
19 example, in the past year alone, several Black men have been wrongfully arrested due to a faulty  
20 facial recognition match, while ICE has used the technology to mine state driver license databases  
21 and identify immigrants for deportation.

22 5. Clearview AI is a software company that has significantly expanded the reach of  
23 facial recognition by scraping and scanning billions of personal photos from the internet, including  
24 social media sites, to create a massive database. Clearview AI has sold access to this trove of  
25 information to both law enforcement agencies and private businesses.

26 6. Last year, the public learned that ICE had purchased access to Clearview AI services,  
27 after ICE and CBP agents had run thousands of facial recognition searches using Clearview AI  
28 technology through a pilot program.

1 7. Even as people use social media services to maintain vital connections with friends  
2 and family members throughout the world—a form of communication made even more critical  
3 during the COVID-19 pandemic—ICE’s use of facial recognition weaponizes these relationships  
4 into a conduit for arrest and deportation.

5 8. The prospect of CBP—an agency whose abuses have grown increasingly violent and  
6 common—deploying facial recognition technology is equally as disturbing. Not only have CBP  
7 officers engaged in militarized over-policing of border communities for decades, but they have also  
8 expanded into domestic surveillance and secret arrests of individuals protesting police killings in  
9 recent months across the nation.

10 9. Over three months ago, on October 19, 2020, Plaintiffs Mijente Support Committee  
11 (“Mijente”), Just Futures Law (“JFL”), Immigrant Defense Project (“IDP”), and the American Civil  
12 Liberties Union of Northern California (“ACLU-NC”), non-profit civil and human rights  
13 organizations, submitted a FOIA request to Defendants ICE, CBP and DHS seeking records related  
14 to Defendants’ past and present use of Clearview AI facial recognition technology, including  
15 contracts, policies, procedures for verifying results and auditing use of the technology, and related  
16 correspondence between the agencies and Clearview AI (the “FOIA Request”).

17 10. Since that time, neither ICE, CBP, nor DHS have provided Plaintiffs with a  
18 substantive response to the FOIA Request.

19 11. ACLU-NC, IDP, JFL and Mijente now bring this action to obtain the information to  
20 which they are statutorily entitled.

21 **PARTIES**

22 12. Plaintiff ACLU-NC is a non-profit organization and an affiliate of the ACLU, a  
23 national organization that works to protect civil liberties of all people, including the safeguarding of  
24 the basic constitutional rights to privacy, free expression, and due process of law. The ACLU-NC is  
25 established under the laws of the state of California and is headquartered in San Francisco,  
26 California. ACLU-NC has approximately 148,000 members. In support of its mission, ACLU-NC  
27 uses its communications department to disseminate to the public through its website, newsletters, in-  
28 depth reports, and other publications.

1           13. Plaintiff IDP is a non-profit organization whose mission is to promote fundamental  
2 fairness for immigrants accused or convicted of crimes. IDP works to protect and expand the rights  
3 of immigrants who have contact with the criminal legal system, including: 1) working to transform  
4 unjust deportation laws and policies; 2) minimizing the harsh and disproportionate immigration  
5 consequences of contact with the criminal legal system; and 3) educating and advising immigrants,  
6 their criminal defenders, and other advocates. IDP disseminates information about the immigration  
7 system to the public in accessible ways and is a leader in providing training and support for legal  
8 practitioners, community-based organizations, and community members. IDP provides expert  
9 information and community-based education on ICE tactics, including surveillance practices, and  
10 possible legal and policy remedies. IDP is established under the laws of the state of New York and  
11 headquartered in New York City, New York.

12           14. Plaintiff JFL is a non-profit organization that works in partnership with immigrant  
13 and racial justice organizers and base-building groups to develop legal and advocacy strategies  
14 aimed at disrupting criminalization and deportation; file litigation aligned with organizing; and build  
15 a political home for lawyers and legal workers who center directly-impacted communities in the  
16 immigrants' rights movement. JFL disseminates information about the immigration system to the  
17 public in accessible ways and is a leader in providing training and support for legal practitioners,  
18 community-based organizations, and community members. JFL provides expert information and  
19 community-based education on ICE tactics, including surveillance practices, and possible legal and  
20 policy remedies. JFL is established under the laws of Delaware and headquartered in Washington,  
21 D.C.

22           15. Plaintiff Mijente Support Committee is a national organization that coordinates and  
23 organizes with its members in several states to address issues relating to immigration enforcement  
24 and Latinx political participation. Among the campaigns run by Mijente Support Committee is  
25 #NoTechForICE, launched in 2019. Mijente is established under the laws of Arizona and  
26 headquartered in Phoenix, Arizona.

27           16. Defendant DHS is a federal agency within the meaning of 5 U.S.C. § 552(f). The  
28 agency has its headquarters in Washington, D.C.

1 17. Defendant ICE is a component of DHS. ICE is an agency within the meaning of 5  
2 U.S.C. § 552(f). The agency has its headquarters in Washington, D.C., and field offices all over the  
3 country, including San Francisco, California.

4 18. Defendant CBP is a component of DHS. CBP is an agency within the meaning of 5  
5 U.S.C. § 552(f). The agency has its headquarters in Washington, D.C., and field offices all over the  
6 country, including San Francisco, California.

7 **JURISDICTION**

8 19. This Court has subject matter jurisdiction and personal jurisdiction over the parties  
9 pursuant to 5 U.S.C. §§ 552(a)(4)(B), 552(a)(6)(C)(i). This Court also has subject matter jurisdiction  
10 over this action pursuant to 28 U.S.C. §§ 1331, 1346.

11 **VENUE AND INTRADISTRICT ASSIGNMENT**

12 20. Venue is proper in this district pursuant to 5 U.S.C. §§552(a)(4)(B) and 28 U.S.C.  
13 §§1391(e) and 1402. Plaintiff ACLU-NC has its principal place of business in this district.

14 21. Pursuant to Local Rule 3-2 (c) and (d), assignment to the San Francisco division is  
15 proper because Plaintiff ACLU-NC is headquartered in San Francisco.

16 **FACTUAL ALLEGATIONS**

17 **The Federal Government's Use of Clearview AI Facial Recognition Technology to Identify,**  
18 **Track, and Locate Individuals is a Matter of Significant Public Interest**

19 22. Now more than ever, Americans rely heavily on social media websites and  
20 applications to connect with family and friends, engage in professional networking, participate in  
21 distance learning, and work from home, among other activities. In order to use these services, most  
22 social media websites and applications require that users share a profile picture so that others in their  
23 network can accurately identify them.

24 23. For the minority of persons whose photo is not displayed on a social media site or  
25 other website, their identity can be ascertained through other publicly available photos, such as those  
26 displayed on government IDs, driver licenses, and passports.

27 24. In January 2020, a *New York Times* investigative report revealed that Clearview AI, a  
28 secretive facial recognition technology startup, had quietly created a massive database of more than

1 3 billion photos that the startup scraped from internet sites such as Facebook, Twitter, LinkedIn, and  
2 Venmo and collected from government databases.<sup>1</sup> Clearview AI's database is now comprised of  
3 face prints captured from photos scraped from social media sites that are publicly available,  
4 including the profile photos that many users must share as a condition of utilizing social media  
5 services. It is likely that the face prints were captured and enrolled in Clearview AI's database  
6 without the knowledge or consent of those pictured.

7 25. The *New York Times* report alarmed the public and privacy advocates alike, who  
8 expressed concerns about Clearview AI's ability to instantly identify people, enabling covert and  
9 remote surveillance of Americans on a massive scale and threatening to "end privacy as we know  
10 it."<sup>2</sup> Subsequent reports indicated that Clearview AI had provided thousands of entities and  
11 individuals access to its database, including companies like Walmart, Kohls, and Bank of America,  
12 and local and federal government entities.<sup>3</sup> ICE and CBP agents alone were reported to have run  
13 thousands of searches by February 2020 using a purported paid pilot of Clearview AI technology.<sup>4</sup>

14 26. Reports that Clearview AI had significantly expanded the reach of facial recognition  
15 technology exacerbated fears about the technology's ability to cause harm. Facial recognition  
16 technology affords government and private actors the unprecedented ability to identify, locate, and  
17 track individuals, raising serious civil and human rights and civil liberties concerns.

18 27. The risks posed by facial recognition are particularly consequential for Black and  
19 Brown people, who are more likely to be stopped by police without just cause and are  
20 disproportionately impacted by police brutality.<sup>5</sup> As a tool that can further streamline racial  
21 profiling, facial recognition increases the risks of such wrongful detentions, arrests, and violent  
22 police encounters.

23 <sup>1</sup> Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, THE NEW YORK  
24 TIMES (Jan. 18, 2020), [https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-  
recognition.html](https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html).

25 <sup>2</sup> *Id.*

26 <sup>3</sup> 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 (Feb. 27, 2020),  
27 <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>.

28 <sup>4</sup> *Id.*

<sup>5</sup> NAACP, *Criminal Justice Fact Sheet*, (Last accessed Jan. 26, 2021)  
<https://www.naacp.org/criminal-justice-fact-sheet>.

1           28. Facial recognition has also been repeatedly demonstrated to be less accurate when  
 2 used to identify Black people, people of Asian descent, and women.<sup>6</sup> In December 2019, the  
 3 National Institute of Standards and Technology released results for a comprehensive study of facial  
 4 recognition systems finding that African American and Asian people were up to 100 more times  
 5 likely to be misidentified than white men, depending on the algorithm and use case.<sup>7</sup> These findings  
 6 built on an earlier ACLU study, in which 1 in 5 California legislators were erroneously matched to a  
 7 mugshot of persons who have been arrested, with facial recognition disproportionately  
 8 misidentifying lawmakers of color.<sup>8</sup> Many face recognition algorithms also misgender transgender  
 9 and gender nonconforming people, while others purport to identify a person's sexual orientation by  
 10 relying on and perpetuating harmful stereotypes about physical appearance.<sup>9</sup> These inaccuracies  
 11 have led to wrongful detentions for crimes people did not commit, such as the false arrest of Robert  
 12 Julian-Borchak Williams recently documented in the *New York Times*,<sup>10</sup> and the false arrest of  
 13 Nijeer Parks recently reported in the *Wall Street Journal*.<sup>11</sup>

14           29. Around August 2020, ICE purchased access to Clearview AI technology and services  
 15 under Contract ID 70CMSD20P00000130. The existence of this contract has generated significant  
 16 public interest and concerns over the use of facial recognition technology to target immigrants for

17 \_\_\_\_\_  
 18 <sup>6</sup> Black and Brown people, especially women and young people, are more likely to be misidentified  
 19 by discriminatory algorithms like facial recognition systems that are built using biased data. See Joy  
 20 Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial*  
 21 *Gender Classification*, PROCEEDINGS OF MACHINE LEARNING RESEARCH, (2018)

22 <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.  
 23 <sup>7</sup> See Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts*  
 24 *doubt on their expanding use*, WASHINGTON POST, (Dec. 19, 2019),  
 25 [https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-](https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-manyfacial-recognition-systems-casts-doubt-their-expanding-use/)  
 26 [manyfacial-recognition-systems-casts-doubt-their-expanding-use/](https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-manyfacial-recognition-systems-casts-doubt-their-expanding-use/).

27 <sup>8</sup> ACLU of Northern California, *Facial Recognition Technology Falsely Identifies 26 California*  
 28 *Legislators with Mugshots*, ACLU NORCAL, (Aug. 13, 2019), [https://www.aclunc.org/news/facial-](https://www.aclunc.org/news/facial-recognition-technology-falsely-identifies-26-californialegislators-mugshots)  
 29 [recognition-technology-falsely-identifies-26-californialegislators-mugshots](https://www.aclunc.org/news/facial-recognition-technology-falsely-identifies-26-californialegislators-mugshots).

30 <sup>9</sup> Vanessa Taylor, *Facial recognition misclassifies transgender and non-binary people, study finds*,  
 31 MIC, (Oct. 30, 2019), [https://www.mic.com/p/facial-recognition-misclassifies-transgender-non-](https://www.mic.com/p/facial-recognition-misclassifies-transgender-non-binary-people-study-finds-19281490)  
 32 [binary-people-study-finds-19281490](https://www.mic.com/p/facial-recognition-misclassifies-transgender-non-binary-people-study-finds-19281490).

33 <sup>10</sup> Kashmir Hill, *Wrongfully Accused by an Algorithm*, NEW YORK TIMES, (Jun. 24, 2020),  
 34 <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>.

35 <sup>11</sup> Asa Fitch, *Facial-Recognition Tools in Spotlight in New Jersey False-Arrest Case*, WALL STREET  
 36 JOURNAL, [https://www.wsj.com/articles/facial-recognition-tools-in-spotlight-in-new-jersey-false-](https://www.wsj.com/articles/facial-recognition-tools-in-spotlight-in-new-jersey-false-arrest-case-11609269719)  
 37 [arrest-case-11609269719](https://www.wsj.com/articles/facial-recognition-tools-in-spotlight-in-new-jersey-false-arrest-case-11609269719) (Dec. 29, 2020).

1 arrest and deportation. Immigrant communities and the broader public have an urgent need to know  
 2 whether the social media services they rely on to connect with family and friends are being exploited  
 3 for facial recognition to facilitate deportations.

4 30. CBP's use of facial recognition surveillance is a matter of grave concern—doubly so  
 5 given confirmed reports that CBP has been unable to protect highly-sensitive location tracking data  
 6 from malicious cyberattacks and other data breaches.<sup>12</sup> And these concerns have taken on a new  
 7 urgency because of CBP's recent involvement in the monitoring, surveilling, and suppression of  
 8 First Amendment-protected protest activity following the murder of George Floyd.<sup>13</sup> Given CBP's  
 9 well-documented history of civil and human rights abuses, which have gone largely unchecked,  
 10 CBP's expanded domestic law enforcement activities are alarming.<sup>14</sup>

11 31. DHS has several offices that play a role in biometrics policy and/or coordination,  
 12 including the DHS Management Directorate, the DHS Office of Policy, DHS Science and  
 13 Technology Directorate (S&T), the DHS Privacy Office, and the DHS Office of Civil Rights and  
 14

15 <sup>12</sup> Zack Whittaker, *CBP Says Traveler Photos and License Plate Images Stolen in Data Breach*,  
 16 TECH CRUNCH, June 10, 2019, <https://techcrunch.com/2019/06/10/cbp-data-breach/>.

17 <sup>13</sup> See, e.g., Josh Gerstein, *Feds Assemble 'Operation Diligent Valor' Force to Battle Portland*  
 18 *Unrest*, POLITICO (July 22, 2020, 9:37 AM ET), [https://www.politico.com/news/2020/07/22/federal-](https://www.politico.com/news/2020/07/22/federal-government-assembles-force-portland-unrest-377785)  
 19 [government-assembles-force-portland-unrest-377785](https://www.politico.com/news/2020/07/22/federal-government-assembles-force-portland-unrest-377785) (describing DHS Rapid Deployment Force in  
 20 Portland as “Operation Diligent Valor”); Caitlin Oprysko, *Trump Announces Plan to Send Federal*  
 21 *Law Enforcement to Chicago, Albuquerque*, POLITICO (July 22, 2020, 6:28 PM ET),  
 22 <https://www.politico.com/news/2020/07/22/trump-law-enforcement-chicago-albuquerque-378692>  
 23 (describing deployments to additional U.S. cities under rubric of “Operation Legend”); Gregory Pratt  
 24 & Jeremy Gerner, *Trump Expected to Send New Federal Force to Chicago This Week to Battle*  
 25 *Violence, but Plan's Full Scope Is a Question Mark*, CHICAGO TRIBUNE, July 20, 2020,  
 26 [https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-dhs-deployment-](https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-dhs-deployment-20200720-dftu5ychwbcxtg4ltarh5qnwma-story.html)  
 27 [20200720-dftu5ychwbcxtg4ltarh5qnwma-story.html](https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-dhs-deployment-20200720-dftu5ychwbcxtg4ltarh5qnwma-story.html); Sergio Olmos, *et al.*, *Federal Officers*  
 28 *Deployed in Portland Didn't Have Proper Training, D.H.S. Memo Said*, N.Y. TIMES, July 21, 2020,  
<https://www.nytimes.com/2020/07/18/us/portland-protests.html>; Ken Klippenstein, *The Border*  
*Patrol Was Responsible for an Arrest in Portland*, THE NATION, July 17, 2020,  
<https://www.thenation.com/article/society/border-patrol-portland-arrest/>.

<sup>14</sup> See, e.g., John Washington, “*Kick Ass, Ask Questions Later*”: *A Border Patrol Whistleblower*  
*Speaks Out About Culture of Abuse Against Migrants*, THE INTERCEPT, Sept. 20, 2018,  
<https://theintercept.com/2018/09/20/border-patrol-agent-immigrant-abuse/>; GUILLERMO CANTOR &  
 WALTER EWING, AM. IMMIGRATION COUNCIL, STILL NO ACTION TAKEN: COMPLAINTS AGAINST  
 BORDER PATROL AGENTS CONTINUE TO GO UNANSWERED (Aug. 2017),  
[http://bit.ly/Council\\_StillNoActionTaken](http://bit.ly/Council_StillNoActionTaken) (examining records of alleged misconduct by Border  
 Patrol employees).



1 Civil Liberties.<sup>15</sup> DHS also recently established its Biometric Capabilities-Executive Steering  
2 Committee (“BS-ESC”), a DHS-wide body that provides “governance, oversight, coordination, and  
3 guidance to all DHS and Component-level programs that are developing or providing biometric  
4 capabilities.”<sup>16</sup>

5 32. To date, neither ICE, CBP, nor DHS have publicly disclosed the terms of any  
6 contractual relationships with Clearview AI or the circumstances under which their personnel are  
7 able to access the technology. Further, neither ICE, CBP, nor DHS have made publicly available the  
8 internal privacy guidelines or training materials governing their personnel’s access and use of  
9 Clearview AI facial recognition technology. Accordingly, the public remains largely unaware of the  
10 extent and purposes to which their face prints are being shared among ICE, CBP, DHS, state and  
11 local agencies, and third parties.

12 33. The information sought in ACLU-NC, IDP, JFL, and Mijente’s FOIA request would  
13 reveal critical information concerning ICE, CBP, and DHS’s use, maintenance, and handling of  
14 people’s images, and would allow members of the public a meaningful opportunity to vet the federal  
15 government’s surveillance of their faces via social media and other websites. This information would  
16 shed light on important and ongoing public debates about facial recognition technology in  
17 communities across the country.

18 **Defendants Have Failed to Produce Any Records in Response to Plaintiffs’ FOIA Request**

19 34. On October 19, 2020, Plaintiffs submitted a FOIA request to ICE headquarters, CBP  
20 headquarters, and DHS headquarters, all located in Washington, District of Columbia, seeking  
21 information relating to contracts by and between ICE, CBP, and DHS and Clearview AI. A copy of  
22 Plaintiffs’ request is appended hereto as Exhibit 1.

23 35. Specifically, the request seeks records containing the following information:

- 24 1. The purchase order or contract entered into between ICE and Clearview AI under Contract  
25

26 <sup>15</sup> See U.S. Department of Homeland Security, Homeland Security Advisory Council, *Final Report*  
27 *of the Biometrics Subcommittee* (Nov. 12, 2020) available at  
28 [https://www.dhs.gov/sites/default/files/publications/final\\_hsac\\_biometrics\\_subcommittee\\_report\\_11-12-2020.pdf](https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf).

<sup>16</sup> *Id.*

1 Award ID 70CMSD20P00000130 (the “Contract”), along with any purchase records, purchase  
2 orders, invoices, sole source letters or justifications, budget request, and grant applications.

- 3 2. All requests for quotations or proposals issued by ICE that led to the award of the Contract.
- 4 3. All records identifying the companies, individuals, or vendors that submitted quotations,  
5 proposals, or submissions in connection with the Contract.
- 6 4. All records identifying the list(s) of facial recognition technology vendors approved for  
7 acquisition and/or use by DHS and any of its offices, components and/or directorates, including  
8 but not limited to all Facial Recognition Services (“FRS”) used by ICE as specified in Privacy  
9 Impact Assessment DHS/ICE/PIA-054 (May 2020).<sup>13</sup> This includes FRS classified under  
10 several types, namely: "State and Local Facial Recognition Services," "Regional and subject  
11 matter-specific intelligence fusion centers," "Federal Agency Facial Recognition Services," and  
12 "Commercial Vendors," the last of which includes Clearview AI facial recognition technology.
- 13 5. Purchase records related to Clearview AI facial recognition technology, including but not limited  
14 to requests for proposal, purchase orders, invoices, sole source letters or justifications, budget  
15 requests, and grant applications, that were created or operative on or after September 1, 2017.
- 16 6. Draft or finalized agreements related to Clearview AI facial recognition software and the above  
17 transactions, including but not limited to e-mail negotiations, contracts, memoranda of  
18 understanding, terms of service, and master services agreements, that were created or operative  
19 on or after September 1, 2017.
- 20 7. Correspondence among or between DHS, CBP and ICE personnel and/or an individual or agency  
21 acting on behalf of DHS, CBP, and ICE, regarding Clearview AI facial recognition technology,  
22 including but not limited to e-mails, internal reports or dossiers, and instant messages<sup>14</sup>, that  
23 were created on or after September 1, 2017.
- 24 8. Correspondence between DHS, CBP and ICE personnel and/or an individual or agency acting on  
25 behalf of DHS, CBP, and ICE, and any employee of Clearview AI, that was created on or after  
26 September 1, 2017. Please search for all email communications to and from help@clearview.ai;  
27 and all email communications to and from email accounts utilizing the “clearview.ai” email  
28 domain.

- 1 9. All records relating to how the Clearview AI facial recognition product or service functions (or  
2 malfunctions), including manuals, instructions, training materials, e-mails, handouts, PowerPoint  
3 presentations, advertisements, or specification documents, that were created on or after  
4 September 1, 2017. Please include all records that describe validation, accuracy, reliability, and  
5 policy compliance of Clearview AI technology.
- 6 10. All manuals, policies, procedures, and practices governing the use or monitoring of Clearview AI  
7 facial-recognition products or services or related information or databases, that were created on  
8 or after September 1, 2017. This request includes, but is not limited to:
- 9 a. Procedures for and restrictions on using, minimizing, deleting, or retaining photos of subjects  
10 to be identified;
  - 11 b. Records identifying any sources of such photos, such as mobile devices, body cameras,  
12 surveillance videos, social media photos, identification photos, or arrest photos;
  - 13 c. Policies or procedures relating to the legal standard, if any, (e.g. probable cause, court order,  
14 relevance, consent) that is required before using Clearview AI's facial recognition product or  
15 service;
  - 16 d. Procedures ICE, CBP and DHS follow after a positive result generated by Clearview AI,  
17 such as requiring independent or in-person verification; and
  - 18 e. Permitted uses of the information created from a positive match.
- 19 11. Training materials related to any Clearview AI products or services by employees of ICE, CBP  
20 and DHS, that were created on or after September 1, 2017.
- 21 12. All records indicating the number of DHS personnel and/or individuals acting on behalf of DHS,  
22 including personnel and individuals working for or acting on behalf of HSI or Enforcement and  
23 Removal Operations divisions, that possess accounts that provide access to any Clearview AI  
24 product, service, or technology.
- 25 13. All records indicating the number of ICE personnel and/or individuals acting on behalf of ICE,  
26 including personnel and individuals working for or acting on behalf of HSI or Enforcement and  
27 Removal Operations divisions, that possess accounts that provide access to any Clearview AI  
28 product, service, or technology.

- 1 14. All records indicating the number of CBP personnel and/or individuals acting on behalf of CBP,  
2 that possess accounts that provide access to any Clearview AI product, service, or technology.
- 3 15. All records indicating the number of facial recognition scans or queries initiated by ICE, CBP  
4 and DHS personnel utilizing Clearview AI products or services on or after September 1, 2017,  
5 including but not limited to daily, weekly, monthly, and/or annual datasets, logs, and/or reports.  
6 Please include the “audit log” Clearview AI makes available to the designated agency  
7 administrator(s).
- 8 16. All records indicating the number of positive and negative facial recognition results generated  
9 via Clearview AI facial recognition software on or after September 1, 2017, including but not  
10 limited to daily, weekly, monthly, and/or annual datasets, logs, and/or reports. Please include the  
11 “audit log” Clearview AI makes available to the designated agency administrator(s).
- 12 17. All records identifying any sources of photos utilized by ICE, CBP and DHS for purposes of  
13 initiating or conducting Clearview AI facial recognition scans or queries, including but not  
14 limited to sources such as mobile devices, body cameras, surveillance videos, social media sites,  
15 traditional newspapers and/or magazines, digital newspapers and/or magazines, aerial  
16 surveillance, identification photos, arrest photos, and/or photos collected or stored by other  
17 federal, state, or local agencies.
- 18 18. All records indicating the number of warrant applications, warrants, arrests and/or prosecutions  
19 associated with a facial recognition scan or query utilizing Clearview AI conducted on or after  
20 September 1, 2017, including warrant applications, warrants, arrests or prosecutions where a  
21 facial recognition scan or query was not cited as a basis for a warrant application, the issuance of  
22 a warrant, an arrest, or a prosecution.
- 23 19. All manuals, policies, procedures, and practices that were created or operative on or after  
24 September 1, 2017 regarding the use or monitoring of Clearview AI facial-recognition products  
25 or services or related information or databases. This request includes, but is not limited to:  
26 a. Any Privacy Impact Assessments;  
27 b. Procedures for and restrictions on using, minimizing, deleting, or retaining photos of  
28 subjects to be identified;

- 1 c. Records identifying any sources of such photos, such as mobile devices, body cameras,
- 2 surveillance videos, social media photos, identification photos, or arrest photos;
- 3 d. Policies or procedures relating to the legal standard, if any, (e.g. probable cause, court order,
- 4 relevance, consent) that is required before using Clearview AI's facial recognition product or
- 5 service;
- 6 e. Procedures ICE, CBP and DHS follow after a positive result generated by Clearview AI,
- 7 such as requiring independent or in-person verification; and
- 8 f. Permitted uses of the information created from a positive match.

9 36. CBP acknowledged receipt of the request on October 20, 2020, assigning tracking  
10 number CBP-2021-008288 to the request, and invoking a 10-day extension to the 20 working-day  
11 deadline for CBP to provide a substantive response to the FOIA request.

12 37. More than 30 working days have passed since CBP acknowledged receipt of the  
13 FOIA request.

14 38. As of the date of the filing of this Complaint, Plaintiffs have not received a  
15 determination from CBP as to whether CBP will comply with the request.

16 39. As of the date of the filing of this Complaint, Plaintiffs have not received any  
17 documents from CBP that are responsive to the request or any correspondence indicating when they  
18 might provide any documents.

19 40. ICE acknowledged the request on December 1, 2020, assigning tracking number  
20 2021-ICFO-12708 to the request, and invoking a 10-day extension to the 20 working-day deadline  
21 for ICE to provide a substantive response to the FOIA request.

22 41. More than 30 working days have passed since ICE acknowledged receipt of the FOIA  
23 request.

24 42. As of the date of the filing of this Complaint, Plaintiffs have not received a  
25 determination from ICE as to whether they will comply with the request.

26 43. As of the date of the filing of this Complaint, Plaintiffs have not received any  
27 documents from ICE that are responsive to the request or any correspondence indicating when they  
28 might provide any documents.

1 44. DHS issued a Final Response to the request on October 29, 2020, assigning tracking  
2 number 2021-HQFO-00091, and stating that the request had been transferred to the FOIA officers  
3 for ICE and CBP due to the subject matter of the request.

4 45. On January 13, 2021, Plaintiffs submitted an administrative appeal to DHS. The  
5 appeal stated that DHS possessed records responsive to the request, that DHS's referral of the  
6 request to ICE and CBP was inappropriate, and that the agency conduct its own search for records.  
7 DHS acknowledged receipt of the appeal on January 22, 2021, assigning DHS Appeal Number  
8 2021-HQAP-00039.

9 46. More than 20 working days have passed since DHS acknowledged receipt of the  
10 administrative appeal.

11 47. Plaintiffs have not received a response to the administrative appeal or a determination  
12 from DHS as to whether they will grant the appeal and comply with the request.

13 48. As of the date of the filing of this Complaint, Plaintiffs have not received any  
14 documents from DHS that are responsive to the request or any correspondence indicating when they  
15 might provide any documents.

16 49. Plaintiffs have exhausted all applicable administrative remedies.

17 50. ICE, CBP, and DHS have wrongfully withheld records from Plaintiffs.

### 18 **FIRST CLAIM FOR RELIEF**

#### 19 **Violation of the Freedom of Information Act for Wrongful Withholding of Agency Records**

20 51. Plaintiffs incorporate the above paragraphs as if fully set forth herein.

21 52. ICE, CBP, and DHS have wrongfully withheld agency records requested by Plaintiffs  
22 under FOIA and have failed to comply with the statutory time for processing of FOIA requests under  
23 5 U.S.C. §§ 552(a)(6)(A), 552(a)(3) and corresponding regulations.

24 53. Plaintiff has exhausted the applicable administrative remedies with respect to ICE,  
25 CBP, and DHS's wrongful withholding of the requested records.

26 54. Plaintiffs are entitled to injunctive relief with respect to the release and disclosure of  
27 the requested documents because ICE, CBP, and DHS continue to improperly withhold agency  
28 records in violation of FOIA. Plaintiffs will suffer irreparable injury from, and have no adequate

1 legal remedy for, ICE, CBP, and DHS's illegal withholding of government documents pertaining to  
2 the subject of Plaintiffs' FOIA request.

3 **PRAYER FOR RELIEF**

4 Plaintiff respectfully requests that this Court:

5 A. Order Defendants ICE, CBP, and DHS to promptly conduct a thorough search for all  
6 responsive records;

7 B. Order Defendants to immediately process and release all responsive records to  
8 Plaintiffs, and enjoin Defendant from improperly withholding records;

9 C. Declare that Defendants ICE, CBP, and DHS's failure to disclose the records  
10 requested by Plaintiffs is unlawful;

11 D. Award Plaintiffs their litigation costs and reasonable attorneys' fees incurred in this  
12 action pursuant to 5 U.S.C. § 552(a)(4)(E); and

13 E. Grant such other relief as the Court may deem just and proper.

14 Dated: April 13, 2021

Respectfully Submitted,

15 /s/ Vasudha Talla  
16 Vasudha Talla (SBN 316219)  
17 AMERICA CIVIL LIBERTIES UNION  
18 FOUNDATION  
19 OF NORTHERN CALIFORNIA  
20 39 Drumm Street  
21 San Francisco, California 94111  
22 Phone: (415) 621-2493  
23 Facsimile: (415) 255-8437  
24 vtalla@aclunc.org

*Attorney for Plaintiffs*

# **EXHIBIT 1**





JUST  
FUTURES  
LAW



IMMIGRANT  
DEFENSE  
PROJECT



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](mailto: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](mailto: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.<sup>1</sup>

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.<sup>2</sup> 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.<sup>3</sup> 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.<sup>4</sup> 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

---

<sup>1</sup> Publicly available documents indicate that Homeland Security Investigations funded a recent contract between ICE and Clearview AI. See Taylor Hatmaker, *Clearview AI landed a new facial recognition contract with ICE*, TECH CRUNCH, (Aug. 14, 2020), <https://techcrunch.com/2020/08/14/clearview-ai-ice-hsi-contract-2020/>.

<sup>2</sup> 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.

<sup>3</sup> 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>.

<sup>4</sup> See Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, Washington Post, (Dec. 19, 2019), <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>.

arrested, with facial recognition disproportionately misidentifying lawmakers of color.<sup>5</sup> 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.<sup>6</sup> 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*.<sup>7</sup>

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.<sup>8</sup> 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.<sup>9</sup> 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.<sup>10</sup> 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.<sup>11</sup> Most recently, ICE purchased access to the Clearview AI technology and services under Contract ID 70CMSD20P00000130. These agencies have amassed a horrifying record of medical abuse, forced

---

<sup>5</sup> ACLU of Northern California, *Facial Recognition Technology Falsely Identifies 26 California Legislators with Mugshots*, ACLU NORCAL, (Aug. 13, 2019), <https://www.aclunc.org/news/facial-recognition-technology-falsely-identifies-26-california-legislators-mugshots>.

<sup>6</sup> Vanessa Taylor, *Facial recognition misclassifies transgender and non-binary people, study finds*, Mic, (Oct. 30, 2019), <https://www.mic.com/p/facial-recognition-misclassifies-transgender-non-binary-people-study-finds-19281490>.

<sup>7</sup> Kashmir Hill, *Wrongfully Accused by an Algorithm*, NEW YORK TIMES, (Jun. 24, 2020), <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>.

<sup>8</sup> Catie Edmundson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, New York Times, (Jul. 7, 2019), <https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html>; Russell Brandom, *Facebook, Twitter, and Instagram surveillance tool was used to arrest Baltimore protestors*, Verge, (Oct. 11, 2016), <https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api>; Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, New York Times, (Apr. 11, 2019), <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>.

<sup>9</sup> *Id.*

<sup>10</sup> 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, (Feb. 27, 2020), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>.

<sup>11</sup> *Id.*

family separation, discrimination and psychological torture.<sup>12</sup> 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).<sup>13</sup> 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.

---

<sup>12</sup> See Amnesty International, *ICE Raids Encourage Hate and Discrimination Toward Immigrants and Communities of Color*, (July 11, 2019), <https://www.amnestyusa.org/press-releases/ice-raids-encouragehate-and-discrimination-toward-immigrants-and-communities-of-color/>; See Amnesty International, USA *'You Don't Have Any Rights Here': Illegal Pushbacks, Arbitrary Detention & Ill Treatment of Asylum-Seekers in the United States* (2018), <https://www.amnesty.org/download/Documents/AMR5191012018ENGLISH.PDF>; Jasmine Aguilera, "Here's What to Know About the Status of Family Separation at the U.S. Border, Which Isn't Nearly Over," *Time*, (Oct. 25, 2019), <https://time.com/5678313/trump-administration-familyseparation-lawsuit>; Carmen Molina Acosta, *Psychological Torture: ICE Responds to COVID-19 With Solitary Confinement*, *The Intercept*, (Aug. 24, 2020), <https://theintercept.com/2020/08/24/ice-detention-coronavirus-solitary-confinement/>; Rachel Treisman, *Whistleblower Alleges 'Medical Neglect,' Questionable Hysterectomies Of ICE Detainees*, *NPR*, (Sep. 16, 2020), <https://www.npr.org/2020/09/16/913398383/whistleblower-alleges-medical-neglect-questionable-hysterectomies-of-ice-detaine>.

<sup>13</sup> Privacy Impact Assessment DHS/ICE/PIA-054, (May 14, 2020), [www.dhs.gov/publication/dhsicepia-054-ice-use-facial-recognition-services](http://www.dhs.gov/publication/dhsicepia-054-ice-use-facial-recognition-services).

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<sup>14</sup>, 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](mailto: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

---

<sup>14</sup> 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.<sup>15</sup> They have also garnered coverage by other news media.<sup>16</sup> ACLU-

---

<sup>15</sup> See, e.g., <https://www.aclunc.org/news/aclu-northern-california-files-demands-documents-implementation-trump-s-muslim-ban> (FOIA request for CBP detention and deportation records); <https://www.aclunc.org/news/aclu-northern-california-files-lawsuit-demanding-documents-implementation-trumps-muslim-ban> (lawsuit challenging government's response to FOIA request for CBP records) <https://www.aclunc.org/news/aclu-seeks-records-immigration-enforcement-actions-northern-california> (FOIA request for ICE enforcement action records); <https://www.aclunc.org/news/lawsuit-seeks-documents-regarding-ice-raids> (lawsuit challenging government's response to FOIA request for ICE enforcement action records);

<sup>16</sup> See, e.g., Eric Tucker, *5 Men Sue Over Anti-Terror Info-Sharing Program*, Associated Press, (July 9, 2014), <https://katu.com/news/nation-world/5-men-sue-over-anti-terror-info-sharing-program-11-20-2015>; Hameed Aleaziz, *Lawsuit Against ICE Seeks Information on Asylum Seekers*, SFGate.com, (Oct. 20, 2016), <https://www.sfgate.com/bayarea/article/Lawsuit-against-ICE-seeks-information-on-asylum-10001076.php>; Luke Darby, *What Surveillance Looks Like Under the Trump Administration*, GQ Magazine, (May 1, 2017), <https://www.gq.com/story/trump-surveillance>; Daisy Alioto, *How Taking a Photograph Can Land You a Visit from the FBI*, Artsy.com, (June 20, 2017), <https://www.artsy.net/article/artsy-editorial-photograph-land-visit-fbi>; Nicole Narea, *ICE To Hand Over Asylum Seeker*



FOIA Request to ICE and DHS re Clearview AI Facial Recognition Technology  
October 19, 2020  
Page 9

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”).

*Second*, there is urgency to inform the public concerning actual or alleged federal government activity. Recent news articles reflect the significant media and public interest in the use of Clearview AI facial recognition technology by governments. *See* 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, (Feb. 27, 2020), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>; Taylor Hatmaker, *Clearview AI landed a new facial recognition contract with ICE*, TechCrunch, (Aug. 14, 2020), <https://techcrunch.com/2020/08/14/clearview-ai-ice-hsi-contract-2020/>; Alyse Stanley, *Controversial Face Recognition Firm Clearview AI Is Teaming Up With ICE*, MSN News, (Aug. 15, 2020), <https://www.msn.com/en-us/news/technology/controversial-face-recognition-firm-clearview-ai-is-teaming-up-with-ice/ar-BB17Z982>.

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.

---

*Detention Policy Data*, Law360.com, (Aug. 9, 2017), <https://www.law360.com/articles/952536/ice-to-hand-over-asylum-seeker-detention-policy-data>.

#### 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 non-profit 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).

FOIA Request to ICE and DHS re Clearview AI Facial Recognition Technology  
October 19, 2020  
Page 11

**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](mailto: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,



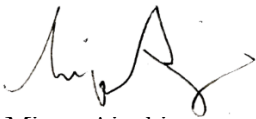
Vasudha Talla  
Immigrants' Rights Program Director  
ACLU Foundation of Northern California



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