Records Provide More Insight into ICE Use of Clearview AI, Suggesting Broader Use, Lack of Oversight, and Internal Concerns

In October 2020, Immigrant Defense Project, Just Futures Law, Mijente, and ACLU Northern California filed a Freedom of Information Act request to demand information related to federal immigration authorities' use of Clearview AI, Inc.'s facial recognition technology. We were concerned that the social media services on which immigrants and others rely to connect with family and friends were being exploited to track, identify, and deport immigrants. Following litigation by ACLU Northern California, we are receiving relevant records from the Department of Homeland Security (DHS), Immigration Customs and Enforcement (ICE), and Customs and Border Patrol (CBP). The records we have so far obtained are concerning on several fronts and raise many questions as explained below.

Clearview AI is a software company that has created a massive facial recognition database by scraping and scanning billions of personal photos from the internet, including social media platforms. These practices violate the terms of service of many social media platforms. Clearview AI sells access to this trove of information to thousands of law enforcement agencies, including ICE, and makes it possible to find people's names and social media accounts and identify them as they protest, shop, and seek essential and sensitive government services.

Key takeaways from the documents received so far include:

1 ICE's Use of Clearview AI is Broader than Originally Claimed

First, the records call into question ICE and Clearview's public claims that ICE's use of Clearview was primarily for investigating child exploitation or cybercrime. Records indicate that ICE use of the Clearview surveillance system was soon implicated in unrelated offenses, including identity theft crimes.[1]

- When ICE purchased three Clearview accounts on June 21, 2019, the agency had already envisioned expanding Clearview's use into "any other criminal or person-of-interest categories [they] wish[ed] to pursue."[2]

[1] See Homeland Security Investigations, Harrisburg/York PowerPoint Presentation.

[2] See internal ICE e-mail thread regarding Clearview AI contract proposal, dated June 20, 2019.

- ICE consulted with Clearview before considering additional language to the contract proposal that would justify Clearview's broader use.[3]
- National Lead Development Center, an agency that investigates fraud related to immigration benefits, used Clearview in the course of its investigations.[4] This raises the question as to whether the Trump Administration/ICE was using Clearview to investigate individuals who apply for immigration benefits.
- ICE used "Darkweb Analytics funding" for the purchase of Clearview licenses.[5] What precisely this means is unclear.
- Meanwhile, ICE referenced that it was broadening its sharing of biometric facial information with local and federal agencies, including the State Department, for purposes of immigration and visa determinations.[6]

[3] See internal ICE e-mail thread regarding Clearview AI contract proposal, dated June 20, 2019.

[4] See memo on "Use of Facial Recognition" from National Lead Development Center.

[5] See internal e-mail from the Unit Chief for the HSI Cyber Crimes Unit, dated June 19, 2019.

[6] See June 27, 2019 Privacy Threshold Analysis from the HSI Cyber Crimes Center, for Clearview AI, which references "forthcoming" updates to the System of Record Notice DHS/ICE-009 that would "provide further transparency on HSI's use of facial photographs." That notice discusses among changes made to "Allow sharing between ICE and the Department of State (DOS) in order to support DOS in making accurate passport and visa issuance, reissuance or revocation determinations" as well as "Allow data sharing between ICE and federal, state, local, tribal, territorial, international, or foreign government agencies…"

2 There Was a Lack of Oversight As ICE Agents Used Clearview.

The records also reveal a troubling lack of agency oversight of ICE employees' acquisition and deployment of Clearview's face surveillance system. There are limited oversight mechanisms regarding ICE's use of surveillance technology. The few mechanisms that do exist matter because of the potential for abuse of this technology, especially technology like Clearview, which can be used to track and identify individuals in real time while they attend political demonstrations, pray at the mosque, or go to the hospital. ICE itself even described Clearview as "privacy sensitive."[7]

[7] See June 27, 2019 Privacy Threshold Analysis from the HSI Cyber Crimes Center, for Clearview AI.

One of these oversight mechanisms—a Privacy Impact Assessment—requires ICE to check if use of Clearview complies with privacy laws and regulations and to mitigate any privacy risks.

In the records, some highlights of what we learned include the following:

- ICE's Child Exploitation Investigations Unit (CEIU) began piloting Clearview for almost a year without conducting a Privacy Impact Assessment.[8]
- During this time period, CEIU relied solely on "interim" privacy safeguards.[9] Meanwhile, the agency continued to buy and pilot Clearview licenses, even in absence of established safeguards.[10]
- A CEIU Section Chief admitted that CEIU did not know the extent of who in ICE was using Clearview, and only "recently became aware that agents and analysts in the field were using the tool." The section belatedly sent out inquiries to identify all users, licenses, and free trials within the department.[11]

[8] See June 27, 2019 Privacy Threshold Analysis from the HSI Cyber Crimes Center, for Clearview AI.

[9] See June 27, 2019 Privacy Threshold Analysis from the HSI Cyber Crimes Center, for Clearview AI.

[10] See receipt for purchase of additional Clearview AI licenses on September 5, 2019.

[11] See internal e-mail thread, February 28, 2020, among staff of the CEIU.

Other concerning revelations

The records also show that ICE adopted other aggressive positions around social media and information that it considers to be publicly available. For example, ICE adopted a practice of recommending its agents use "unattributable browsers," in part to evade websites that are "averse to law enforcement" and that make it more difficult for law enforcement to obtain "advertising data, location data, and search habits."[12] But the audit logs for use of those browsers are maintained for only ninety days. It is unclear whether Clearview searches—which ICE takes the view are just referencing public social media content—fall under the scope of these unattributable searches, and are thus further removed from meaningful oversight.

[12] See Enforcement and Removal operations, Combined Intelligence Unit Memo on "Unattributable Online Browser Licenses."

3 DHS Monitored Public Scrutiny of Agency Use of Clearview

The Department of Homeland Security has kept a close eye on public scrutiny of Clearview from the press and civil and human rights groups. We obtained numerous internal e-mails and other documents in our FOIA advocacy where DHS was either circulating or logging such scrutiny. Some of that coverage has included the following:

- DHS internally tracked prominent press coverage, including in Vox, that raised serious constitutional concerns with the use of Clearview.[13]
- DHS circulated an April 19, 2021 sign-on letter to Homeland Security Secretary Alejandro Mayorkas drafted by Mijente, Just Futures Law, Immigrant Defense Project, ACLU of Northern California and other groups calling for transparency regarding DHS practices and the immediate end of Clearview's use.[14]
- DHS acknowledged that biometric facial images were vulnerable to being reverse engineered.[15]
- DHS tracked state laws restricting the collection of DMV vehicle records.[16]

This tracking, coupled with DHS' internal acknowledgment of the privacy risks inherent in using Clearview, indicates that DHS remains on notice of the serious rights implications of the technologies.

Conclusions

These documents leave many concerning open questions about the nature and extent of use of Clearview and facial recognition technologies which have huge implications for fundamental rights. In addition, they raise serious doubts as to the effectiveness of existing oversight safeguards, which appear to have been delayed or outright ineffective at providing appropriate transparency. We continue to call on DHS to end its use of Clearview technologies.

[13] See internal complaints production spreadsheet indicating that "On February 11, 2020, CRCL reviewed an article published by Vox regarding the DHS-Clearview collaboration, titled 'The world's scariest facial recognition software, explained.'" The note is flagged "First Amendment" and "Fourth Amendment" and indicates that DHS did not respond to a request for comment.

[14] See internal e-mail thread, June 30, 2021, among staff of the DHS Office for Civil Rights and Civil Liberties (CRCL).

[15] See internal CRCL e-mail thread of May 24, 2021, referencing vulnerability of facial recognition technology to reverse engineering.

[16] See internal e-mail thread of January 30, 2020 referencing "Memo re: Assessments of State Laws Restricting the Sharing of DMV Data with DHS."

Key Timeline Dates Providing Context on Lack of Oversight

June 27, 2019

In an internal review, ICE states "*ICE's use of Clearview AI is privacy sensitive, requiring PIA [Privacy Impact Assessment] coverage*." The PIA is not issued until nearly a year later.

Feb 28, 2020

Internal memos state that: "*We recently became aware that agents and analysts in the field were using the [Clearview] tool. We sent a tasking to the field to identify all of the users…*"

March 4, 2021

DHS uses Clearview not only in child exploitation investigations but in "*certain types of criminal investigations that meet specific, defined parameters*."[17]

Sept 5, 2019

ICE purchases additional Clearview licenses.

June 2020

Arrests are internally discussed in an identity theft investigation which an ICE presentation explicitly connects to Clearview.

June 21, 2019

ICE purchases three Clearview AI user accounts for the CEIU.

March 2, 2020

An internal memo states that ICE is *"completing a thorough privacy impact assessment process with the ICE Office of Privacy to ensure the product complies with ICE and HSI policies."*

[17] See internal memo dated March 4, 2021, from the AD of Operational Technology and Cyber Division, HSI, to all personnel.

Primary authors: Carey Shenkman, consulting attorney for Just Futures Law, and Sejal Zota, Legal Director of Just Futures Law.