epic.org

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

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

VIA EMAIL

March 6, 2020

Dr. James V.M.L. Holzer
Deputy Chief FOIA Officer
Privacy Office, Mail Stop 0655
Department of Homeland Security
2707 Martin Luther King Jr. AVE SE
Washington, DC 20528-065
Email: foia@hq.dhs.gov

Dear Dr. Holzer:

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

EPIC seeks records related to the agency's use of Clearview AI technology.[1]

Documents Requested

1. Emails and communications about Clearview AI, Inc., including but not limited to the following individuals and search terms:
    a. Clearview
    b. Clearview AI
    c. Hoan Ton-That
    d. Tor Ekeland
    e. Third parties with an email address ending in "@clearview.ai"
2. All contracts or agreements between the DHS and Clearview AI, Inc.;
3. All presentations mentioning Clearview;
4. All Clearview sales materials;
5. All privacy assessments, including but not limited to Privacy Threshold Analysis and/or Privacy Impact Assessments, that discuss the use of Clearview AI technology.

Background

A recent *New York Times* investigation revealed that a secretive New York-based company, Clearview AI, Inc., has developed an application that allows law enforcement agencies to identify people in public spaces without actually requesting identity documents or without a legal basis to

[1] Clearview AI, Inc., https://clearview.ai/.

determine the person's identity.[2] Clearview AI uses a secret algorithm and billions of facial images collected without consent.[3] Clearview conducts matches surreptitiously.[4] Whenever an image is uploaded onto the app, the company also stores the image in its servers.[5] Clearview has scraped more than 3 billion images from websites and social media platforms such as Facebook, YouTube, Venmo, and Twitter.[6] Within the past year, more than 600 law enforcement agencies have started using the Clearview AI app.[7]

Several major technology companies including Twitter, LinkedIn, Venmo, Facebook, YouTube, and Google have issued cease and desist notices asking the company to stop its data scraping practices.[8] New Jersey recently banned statewide law enforcement agencies from using Clearview AI services and are looking into how the state's law enforcement agencies have used the app.[9] Apple has also suspended the app from its developer program for violating its policies.[10]

On February 26, 2020, *The Daily Beast* reported that Clearview AI suffered a massive data breach that revealed its client list, number of user accounts its clients set up, and the total number of searches its clients have conducted.[11] Clearview stated that it fixed the vulnerability and that law enforcement agencies' search history was not compromised.[12] But government officials remain skeptical that Clearview can safeguard the information it has gathered.[13]

While the company stated that its technology is strictly used for law enforcement purposes in the United States and Canada, a subsequent report reveals that its clients include companies, educational institutions, banking institutions, and individuals around the world.[14] According to

---

[2] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[3] *Id*.
[4] *Id*.
[5] *Id*.
[6] *Id*.
[7] *Id*.
[8] Gisela Perez & Hilary Cook, *Google, YouTube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App that Helps Law Enforcement*, CBS News (Feb. 5, 2020), https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/.
[9] Kashmir Hill, *New Jersey Bars Police From Using Clearview Facial Recognition App*, N.Y. Times (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html.
[10] Rishi Iyengar, *Apple Suspends Controversial Facial Recognition App Clearview AI From Its Developer Program*, CNN (Feb. 28, 2020), https://www.cnn.com/2020/02/28/tech/clearview-ai-apple-account-disabled/index.html.
[11] Betsy Swan, *Facial-Recognition Company that Works with Law Enforcement Says Entire Client List was Stolen*, Daily Beast (Feb. 26, 2020), https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen.
[12] *Id*.
[13] Dell Cameron, *Data Breach at Controversial Face Recognition Firm Shows Company Can't Be Trusted, Officials Say*, Gizmodo (Feb. 26, 2020), https://gizmodo.com/data-breach-at-controversial-face-recognition-firm-show-1841938311.
[14] Ryan Mac, Caroline Haskins, & Logan McDonald, *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, Buzzfeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

documents reviewed by *Buzzfeed News*, Clearview has already shared and or sold its technology to more than "2,200 law enforcement departments, government agencies, and companies across 27 countries."[15] These clients include:

- U.S. Immigration and Customs Enforcement ("ICE")
- U.S. Attorney General's Office for the Southern District of New York
- Federal Bureau of Investigations
- U.S. Department of Homeland Security ("DHS")
- U.S. Customs and Border Protection ("CBP")
- U.S. Department of Justice ("DOJ")
- U.S. Secret Service
- Drug Enforcement Administration ("DEA")
- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- U.S. Marshals
- Interpol
- Hundreds of local police departments[16]

There is now support for a ban on facial recognition in the United States. Members of Congress of both parties, technical experts, scholars, advocates, and the public have expressed concern at the use of this secretive technology is intrusive, unreliable, and a threat to civil liberties. A recent federal study found that a majority of face surveillance software exhibits racial bias.[17] Currently, there are state or local level facial recognition bans in Massachusetts, Oregon, and in California.[18]

Request for Expedited Processing

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

First, there is "urgency to inform the public concerning actual or alleged federal government activity." 6 C.F.R. § 5.5(e)(1)(ii). The DHS's use of Clearview's facial recognition technology for law enforcement purposes constitutes an "actual . . . federal government activity."

There is "clear urgency" to release the requested information because the federal government's use of Clearview's controversial facial recognition app has been the subject of intense scrutiny from the media, lawmakers, and the public. On January 23, 2020, Senator Markey sent a

[15] *Id*.
[16] *Id*.
[17] Patrick Grother, Mei Ngan, & Kayee Hanaoka, Nat'l Inst. of Standards and Tech., U.S. Dep't of Commerce, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[18] *See* EPIC, *Face Surveillance By Country: United States*, https://epic.org/banfacesurveillance/index.php?c=United%2BStates#country.

letter to Clearview stating that "Clearview's products appears to pose particularly chilling privacy risks, and I am deeply concerned that it is capable of fundamentally dismantling Americans' expectation that they can move, assemble, or simply appear in public without being identified."[19] Moreover, the company currently faces several class action lawsuits alleging violation of both Illinois and California privacy laws.[20] Clearview has been secretive about how its proprietary algorithm works and who its clients are until leaked information recently revealed the extent of its relationship with not only law enforcement but also companies and international entities. To date, these relationships continue to exist and government agencies will continue to use this controversial, potentially privacy invasive facial recognition app to carry out government activities.

Second, EPIC is an organization "primarily engaged in disseminating information." 6 C.F.R. § 5.5(e)(1)(ii). As the Court explained in *EPIC v. DOD,* "EPIC satisfies the definition of 'representative of the news media'" entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003). EPIC is a non-profit organization committed to privacy, open government, and civil liberties that consistently discloses documents obtained through FOIA on its website, EPIC.org, and its online newsletter, the *EPIC Alert*.[21]

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

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. DOD*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II); 6 C.F.R. § 5.11(d)(1)–(2).

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

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

Disclosure of the requested documents is "in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government." 6

[19] Letter from Senator Edward J. Markey to Hoan Ton-That, Chief Exec. Officer, Clearview AI (Jan. 23, 2020), https://www.markey.senate.gov/imo/media/doc/Clearview%20letter%202020.pdf.
[20] *See* Daniel R. Stoller & Sara Merken, *Clearview AI Faces California, Illinois Lawsuit After Breach*, Bloomberg Law (Feb. 28, 2020), https://news.bloomberglaw.com/privacy-and-data-security/clearview-ai-faces-california-illinois-lawsuit-after-breach; Devin Coldewey, *Class Action Suit Against Clearview AI Cites Illinois Law that Cost Facebook $550M*, TechCrunch (Feb. 14, 2020), https://techcrunch.com/2020/02/14/class-action-suit-against-clearview-ai-cites-illinois-law-that-cost-facebook-550m/.
[21] EPIC, *About EPIC*, https://epic.org/epic/about.html.

C.F.R. § 5.11(k)(2). The DHS evaluates four factors to determine whether the "public interest" condition is met: (i) the "subject of the request must concern identifiable operations or activities of the federal government"; (ii) disclosure must be "meaningfully informative about government operations or activities"; (iii) disclosure "must contribute to the understanding of a reasonably broad audience of persons interested in the subject"; and (iv) "[t]he public's understanding of the subject in question must be enhanced by the disclosure to a significant extent." *Id*. EPIC's request satisfies all four factors.

First, the requested records clearly "concern identifiable operations or activities of the Federal Government," namely: the DHS's implementation and use of Clearview's software for law enforcement purposes. 6 C.F.R. § 5.11(k)(2)(i). It has been reported that Clearview has credentialed individual users at the DHS to access the company's database of more than 3 billion photos.[22]

Second, disclosure of the requested records is "'likely to contribute' to an increased public understanding of those operations or activities." 6 C.F.R. § 5.11(k)(2)(ii). Disclosure would "be meaningfully informative about government operations or activities" because little new information has been released about the DHS's relationship with Clearview and how the agency is implementing Clearview's software. *Id.* The records requested will help inform the public on the extent of the DHS's use of this facial recognition software.

Third, disclosure will "contribute to the understanding of a reasonably broad audience of persons interested in the subject," because DHS components must "presume[] that a representative of the news media," such as EPIC, "will satisfy this consideration." 6 C.F.R. § 5.11(k)(2)(iii). The requested records will reach a large audience through EPIC's widely read website, https://epic.org, where EPIC routinely posts and interprets privacy-related government documents obtained under the FOIA. EPIC's FOIA work is also frequently covered through major media outlets.[23]

Fourth, "[t]he public's understanding of the subject in question [will] be enhanced by the disclosure to a significant extent." 6 C.F.R § 5.11(k)(2)(iv). The precise extent of the DHS's use of Clearview technology is unknown. Further, it is unclear whether the agency considered potential privacy implications when implementing Clearview's technology. Disclosure of the requested records will provide exactly this information.

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

The "[d]isclosure of the information is not primarily in the commercial interest" of EPIC. 6 C.F.R. § 5.11(k)(3). The DHS components evaluate two considerations in assessing this requirement: (i) whether there are "any commercial interest of the requester . . . that would be furthered by the requested disclosure"; and/or (ii) whether "the public interest is greater than any identified commercial interest in disclosure" and "[c]omponents ordinarily shall presume that where a news media requester has satisfied the public interest standard, the public interest will be the interest primarily served by disclosure to that requester." *Id.*

[22] Mac et al, *supra* note 14.
[23] *See* EPIC, *EPIC in the News*, https://epic.org/news/epic_in_news.php/.

First, there is no "commercial interest of the requester . . . that would be furthered by the requested disclosure." 6 C.F.R. § 5.11(k)(3)(i). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[24] EPIC has no commercial interest in the requested records.

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

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

Conclusion

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

Respectfully submitted,

/s/ Enid Zhou
Enid Zhou
EPIC Open Government Counsel

/s/ Jeramie Scott
Jeramie Scott
EPIC Senior Counsel

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