EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:
ENVIRONMENT AND PUBLIC WORKS
CHAIR:
SUBCOMMITTEE ON CLEAN AIR, CLIMATE, AND NUCLEAR SAFETY
HEALTH, EDUCATION, LABOR, AND PENSIONS
CHAIR:
SUBCOMMITTEE ON PRIMARY HEALTH AND RETIREMENT SECURITY
COMMERCE, SCIENCE, AND TRANSPORTATION
SMALL BUSINESS AND ENTREPRENEURSHIP
CHAIR:
U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

SUITE SD-255
DIRKSEN BUILDING
WASHINGTON, DC 20510-2107
202-224-2742

975 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
617-565-8519

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

November 20, 2023

Mr. Hoan Ton-That
Founder & Chief Executive Officer
Clearview AI
99 Wall St. #5730
New York, NY 10005

Dear Mr. Ton-That:

I write with serious concerns about Clearview AI's continued development of facial recognition technology through the mass collection of the public's biometric information. Facial recognition technologies — and Clearview AI's system, in particular — pose a serious threat to privacy rights and civil liberties. Particularly in the context of law enforcement use of your product, the American people should not have to forgo personal privacy for public safety. If Clearview AI is serious about participating in Congress' work to regulate artificial intelligence, I urge your company to consider the privacy risks of facial recognition technology and be transparent about your company's development and use of its facial recognition system.

Despite accuracy improvements in recent years, facial recognition technologies remain biased against communities of color. For example, one study found that algorithms for one-to-many identification — in which a photo of an individual's face is compared against a database of photos — had higher rates of false positive identifications for people of color and women.[1] This bias is already evident in the real world. Based on public reporting, law enforcement agencies nationwide already have made at least six false arrests based on an inaccurate facial recognition match.[2] The true number is surely higher. These incidents have serious consequences for the impacted individuals. Earlier this year, based on a false facial recognition match, Detroit police officers wrongfully arrested a Black woman — who was eight months pregnant — for robbery and carjacking.[3] The woman experienced contractions in the holding cell; her daughters were traumatized. That is unacceptable. The use of facial recognition systems trained off biased

[1] 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/.

[2] Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, The New York Times (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

[3] *Id.*

datasets, that produce biased results, and that impose serious harms on marginalized communities must end.

Facial recognition technologies are also likely to be disproportionally deployed against Black, Brown, and immigrant individuals, leading to additional over-policing and increased surveillance in these communities.[4] For example, in New Orleans, the police used a facial recognition system against 15 suspects in the last year — 14 of which were Black.[5] Of those 15 facial recognition requests, the system returned a match just six times and half of those six matches were inaccurate.[6] In Detroit, 100 percent of the 129 facial recognition searches in 2020 were conducted on Black people.[7] Although the New Orleans and Detroit police departments did not use Clearview AI's system, these results raise significant concerns about law enforcement's use of facial recognition tools and its impact on communities of color. Indeed, one recent academic study showed that law enforcement use of facial recognition technology contributes to greater racial disparity in arrests.[8]

Clearview AI's facial recognition system is particularly problematic. Clearview reportedly developed its database by scraping tens of billions of photos online and extracting people's unique biometric face prints from them — without either providing a notice to the individual photographed or obtaining their consent,[9] raising serious questions about Clearview AI's compliance with domestic and international privacy laws.[10] If Clearview AI's reported number of face prints in its database is accurate, it may have collected facial images on billions of people without their knowledge or consent. Moreover, by aggregating this sensitive data in a single location, Clearview AI created a prime target for cyber criminals. Although that database has not, as far as the public knows, been hacked, Clearview AI did suffer a cyberattack in 2020 in which its client list was stolen, raising serious concerns about the security of its facial recognition database.[11]

---

[4] Nicol Turner Lee and Caitlin Chin-Rothmann, *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*, Brookings Institute (Apr. 12, 2022), https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

[5] Alfred Ng, *'Wholly ineffective and pretty obviously racist': Inside New Orleans' struggle with facial-recognition policing*, Politico (Sept. 31, 2023), https://www.politico.com/news/2023/10/31/new-orleans-police-facial-recognition-00121427.

[6] *Id.*

[7] Detroit Police Department, *Annual Report on Facial Recognition*, 2020, City of Detroit (Jan. 27, 2021), https://detroitmi.gov/sites/detroitmi.localhost/files/2021-02/Facial%20Recognition%202020%20Annual%20Report.pdf .

[8] Thomas L. Johnson, et. al., *Facial recognition systems in policing and racial disparities in arrests*, Science Direct (Oct. 2022), https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000892.

[9] Kashmir Hill, *The Secretative Company That Might End Privacy as We Know It*, The New York Times ((Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[10] https://techcrunch.com/2023/05/10/clearview-ai-another-cnil-gspr-fine/; https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html.

[11] Kate O'Flaherty, *Clearview AI, The Company Whose Database Has Amassed 3 Billion Photos, Hacked*, Forbes (Feb. 26, 2020), https://www.forbes.com/sites/kateoflahertyuk/2020/02/26/clearview-ai-the-company-whose-database-has-amassed-3-billion-photos-hacked/?sh=1f419de57606.

Finally, although Clearview AI has promoted incidents in which its facial recognition system was supposedly used for public benefit, the company has not addressed the very real harms from the use of its facial recognition technologies. In at least one case, in 2019, Clearview misled the public that its technology was used to identify a terrorism suspect.[12] Furthermore, in 2020, the Minneapolis Police Department used Clearview to target and surveil Black Lives Matter protestors.[13] And in 2022, reports indicate that a sheriff's office in Louisiana investigating retail fraud relied on incorrect Clearview results to obtain an arrest warrant, leading to the wrongful arrest of a Black Georgia resident who had never even been to Louisiana.[14] Police in Indiana have similarly relied solely on Clearview results to obtain arrest warrants.[15] Although Clearview AI publicly warns law enforcement officers against relying solely on a facial recognition match to make an arrest, the company appears to lack compliance mechanisms, and in past marketing materials, has suggested police officers "run wild" with their searches.[16] These reports raise serious questions about the true benefits and potential vast privacy and civil liberties harms of Clearview AI's photo database and facial recognition algorithm.

During a recent Senate AI Insight Forum, you stated your openness to regulation and oversight and that you looked forward to "being part of the conversation."[17] I appreciate this willingness and look forward to receiving your detailed written responses to the following questions by December 11, 2023:

1. Please describe Clearview AI's process for storing the photos that it scrapes from the Internet and the face prints (or facial vectors) that it detects in those photos.

    a. Does Clearview AI keep a database of photos that it scrapes from the Internet? If so, how many photos are in the database?

---

[12] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview AI Says Its Facial Recognition Software Identified A Terrorism Suspect. The Cops Say That's Not True.,* BuzzFeed News (Jan 23, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-nypd-facial-recognition.

[13] Caroline Haskins and Ryan Mac, *Here Are The Minneapolis Police's Tools To Identify Protesters*, BuzzFeed News (May 29, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/george-floyd-protests-surveillance-technology.

[14] Kashmir Hill and Ryan Mac, *'Thousands of Dollars for Something I Didn't Do'*, The New York Times (Mar. 31, 2023), https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.

[15] Houston Harwood, *Company says facial recognition can't be used in arrest, but it's happening in Evansville*, Courier & Press (Oct. 19, 2023), https://www.courierpress.com/story/news/local/2023/10/19/evansville-police-using-clearview-ai-facial-recognition-to-make-arrests/70963350007/.

[16] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview AI Once Told Cops to "Run Wild" With Its Facial Recognition Tool. It's Now Facing Legal Challenges.*, BuzzFeed News (Jan. 28, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-cops-run-wild-facial-recognition-lawsuits.

[17] Press Release, Clearview AI, AI Insight Forum: Statement From Hoan Ton-That, CEO Clearview AI (Nov. 1, 2023).

b. Does Clearview AI keep a database of unique facial vectors? If so, how many facial vectors does Clearview AI have in that database? How many of those facial vectors are U.S. citizens? How many are U.S. children?

c. Does Clearview AI collect or scrape any metadata or additional data, outside of photos or links, from websites?

d. Does Clearview AI supplement the data its scrapes from the Internet with additional data, such as from commercial vendors or governmental databases?

e. Please describe how Clearview AI treats the scraping and storage of photos of children.

f. Does Clearview AI estimate the age of individuals whose face prints it has processed from photos?

2. Please identify the data that Clearview AI has used to train its facial recognition algorithm(s).

   a. Has Clearview AI in the past, or does Clearview AI now, train its algorithms on photos scraped from the internet without individuals' consent?

   b. Has Clearview AI used photos of U.S. children to train its facial recognition algorithm?

3. Does Clearview AI track the race, gender, ethnicity, age, and other demographic indicators of individuals in images submitted for and generated by its clients' searches?

   a. If so, please provide the demographic breakdowns of the searches made over the past three years.

   b. Does Clearview AI audit disparities among the results of its facial recognition technology, including by race, sex, age, and other demographics? If so, please provide documentation of those audits.

4. Although Clearview AI has submitted algorithms to testing by the National Institute of Standards and Technology, that testing is not designed to replicate real-world conditions. Has Clearview AI tested the accuracy and reliability of its system in conditions equivalent to real-world uses by law enforcement, including use on low-quality probe images and use by poorly trained or untrained law enforcement personnel? If so, was that testing conducted by an independent auditor? If so, please provide the results of this test.

5. Please identify all Clearview AI's public and private sector clients that have access to Clearview AI's database, including federal government entities such as intelligence and law enforcement agencies and state and local government entities such as public schools.

    a. How much does Clearview AI charge for access to its algorithm and database?

    b. How many free trials has Clearview AI provided to government and law enforcement entities in the last three years?

    c. Clearview AI is under a binding obligation to end its prior practice of offering free trials to law enforcement personnel without the knowledge or approval of the law enforcement agency that employs them.[18] How does Clearview AI ensure compliance with this obligation?

6. Please identify all Clearview AI's public and private clients that have purchased licenses to use Clearview AI's facial recognition algorithm.

    a. How much does Clearview AI charge for a license to use its facial recognition algorithm?

    b. Please describe Clearview AI's process for agreeing to license its facial recognition algorithm to a new client. What vetting does Clearview AI conduct before granting an entity access to its algorithm?

    c. Does Clearview AI require clients to establish procedures for overseeing use of Clearview's algorithm by its employees?

7. Has Clearview AI ever revoked access to its facial recognition algorithm from a law enforcement agency?

    a. If so, please identify the agencies and the reason for revoking access.

    b. Will Clearview AI commit to not selling its product to law enforcement agencies that have a record of discrimination?

    c. Will Clearview AI commit to revoking access to its photo database for law enforcement and government entities that use its product to surveil peaceful protestors or disproportionally target communities of color? If not, why not?

8. Please describe the process an individual must undergo to remove their face prints (or facial vectors) and photos from Clearview AI's database.

[18] Ryan Mac and Kashmir Hill, *Clearview AI settles suit and agrees to limit sales of facial recognition database*, The New York Times (May 9, 2022), https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html.

a. If an individual requests that Clearview AI delete their information, does that include their face print and all photos that match that face print?

b. In processing deletion requests, what level of similarity does Clearview AI require to determine that the face print and photo are matches?

c. How long, on average, does Clearview AI take to process a deletion request?

d. When individuals request that Clearview AI remove their images from its database, do they need to continue to make deletion requests if additional photos are posted publicly?

i. If so, why does Clearview AI require users to continuously make deletion requests to exclude themselves from its database?

ii. If not, how does Clearview AI ensure photos that have been deleted are permanently removed from Clearview AI's database?

e. Will Clearview AI commit to providing all individuals with the right to request the deletion of their information from Clearview AI's database? If not, why not?

9. Has Clearview AI changed its cybersecurity practices following the 2020 hack? If so, please describe the changes.[19] If not, why not?

a. Has Clearview AI experienced any successful hacks since 2020? If so, please describe the incident, including identifying the information accessed during the security breach.

b. Was Clearview AI able to identify the 2020 hackers or their motive? If so, please provide that information.

10. Has Clearview AI developed any product that would permit real-time identification of individuals using its facial recognition technologies?

a. If so, please describe the product and identify any entities to which Clearview AI has sold, licensed, or otherwise provided access to that product.

b. Is Clearview AI working with any entities, including schools, on real-time facial recognition technologies integrated in existing camera networks?

[19] Kate O'Flaherty, *Clearview AI, The Company Whose Database Has Amassed 3 Billion Photos, Hacked*, Forbes (Feb. 26, 2020), https://www.forbes.com/sites/kateoflahertyuk/2020/02/26/clearview-ai-the-company-whose-database-has-amassed-3-billion-photos-hacked/?sh=1f419de57606.

c. Is Clearview AI working with any entities on real-time facial recognition technologies integrated into smart glasses or a similar product?

d. Will Clearview AI commit to not allowing its photo database, facial vector database, or facial recognition algorithm to be used for real-time identification? If not, why not?

e. Is Clearview AI working with any entities to using its photo database, facial vector database, or facial recognition algorithm to be used to identify individuals on recorded video footage?

f. Will Clearview AI commit to not allow its photo database, facial vector database, or facial recognition algorithm to identify individuals on recorded video footage? If not, why not?

11. Does Clearview AI attempt to obtain consent or identify another legal basis to collect, maintain, or use personal information where required by law?

    a. Is Clearview AI in compliance with Illinois' Biometric Information Privacy Act?

    b. Is Clearview AI in compliance with the Children's Online Privacy Protection Act?

Thank you for your attention to these important issues.

Sincerely,

Edward J. Markey
United States Senator