COMMENT TO SCIENCE & TECHNOLOGY DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY
Docket No. DHS-2021-0015

United States Department of Homeland Security
Science and Technology Directorate
245 Murray Lane, Suite 14
Washington D.C. 20528

December 6, 2021

RE: Public Perceptions of Emerging Technology

Clearview AI, a U.S. based company dedicated to providing the most cutting-edge technology to law enforcement to investigate crimes, enhance public safety and provide justice to victims, is pleased to provide public comment addressing the issue of artificial intelligence ("AI"), including facial recognition.

Facial recognition technology is a critical tool to ensure public safety, provided that proper safeguards are established. Reasonable and effective policies eliminate many of the concerns surrounding the technology, including, but not limited to, discrimination and privacy concerns.

Such protections include:

(1) Accuracy requirements and non-discrimination;
(2) Records to enable an audit or review of each use;
(3) Match verification and secondary review of result;
(4) Privacy protections by excluding and/or redacting explicit images;
(5) Authorization and accountability by implementing a use policy;
(6) Independent verification, the match cannot be used as sole source for positive identification;
(7) Prohibition on use by agency for persons engaged in protected activities.

HIGH-PERFORMING ALGORITHMS (AS DETERMINED BY NIST) DO NOT CONTAIN RACIAL BIAS & ARE AT LEAST 99% ACCURATE

The Director of the Information Technology Laboratory for National Institute of Standards and Technology ("NIST"), Dr. Charles Romine testified in 2020 before the U.S. Homeland Security Committee that with the highest-performing algorithms they saw "undetectable" bias, further noting, that they did not see a "statistical level of

significance" related to bias in these top-performing algorithms.[1] Indeed, NIST's October 2021 evaluation of Clearview's facial recognition algorithm found 99% accuracy for all demographics – highlighting the dependability and accuracy in advanced algorithms.[2]

As noted by the U.S. Government Accountability Office ("GAO") [r]ecent advancements in facial recognition technology have increased its accuracy and its usage."[3] In fact, unlike older algorithms which use manual measurements, advanced and high-performing algorithms use a form of artificial intelligence called a "neural network".[4] These artificial neural networks operate similar to a biological brain, transmitting various signals to other neurons to map out the image. For example, Clearview's high-performing algorithm's neural networks are trained on millions of examples of diverse faces from all ethnicities to ensure there is no racial bias in its algorithm.

A larger database of images further promotes accuracy and eliminates the possibility of racial bias because it is more reflective of a diverse population. It also reduces the likelihood of law enforcement making false positives. A database of 1 billion images that are routinely updated provides a diverse data set that matches diverse populations. Further, retrieval rank is a setting whereby an algorithm can be modified to return more results that may not be as accurate. Setting a low retrieval rank will always return more false positives. High-performing algorithms should be hardcoded to not allow the user to modify the retrieval rank, thereby limiting the return of false positives. The facial recognition algorithm produces a set of potential matches that are then reviewed by human investigators and trained analysts who serve as peers in the review process.

Finally, beyond improving an otherwise manual process, facial recognition contributes to more accurate identification. The National Institute of Science and Technology has found that forensic examiners performed best when supported by facial recognition

---

[1] *Facial Recognition and Biometric Technology*, C-SPAN (Feb. 6, 2020), available at https://www.c-span.org/video/?469047-1/homeland-security-officials-testify-facial-recognition-technology-usage.

[2] *Ongoing Face Recognition Vendor Test*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Oct. 28, 2021), available at https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf.

[3] *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (Aug. 24. 2021), available at https://www.gao.gov/products/gao-21-526.

[4] *Neural Networks*, IBM CLOUD EDUCATION (Aug. 2020), available at https://www.ibm.com/cloud/learn/neural-networks.

technology and the most accurate performance resulted when these efforts are combined. "[A] team of scientists from . . . NIST and three universities has tested the accuracy of professional face identifiers, providing at least one revelation that surprised even the researchers: Trained human beings perform best with a computer as a partner, not another person."[5]

THE DATASET IS CRITICAL TO HELP SOLVE CRIMES AND RESCUE VICTIMS

Any policy that encourages restricting the data set to a facial search against Department of Motor Vehicles ("DMV") records or criminal databases (such as mugshots) is extraordinarily limiting. This will not facilitate the identification of an adolescent victim or a suspect committing crimes within the state that do not exist in these limited data sets.

In actuality, limiting a law enforcement agency to look for perpetrators in criminal data sets such as mug shots could encourage the resolution of crimes that point to repeat offenders and discourage the resolution of investigations involving unknown persons that are not in the typical local data set.

For geographic areas that are highly intertwined, such as New England, where crimes can easily be perpetrated in multiple states, using a DMV dataset causes many challenges for law enforcement. Specifically, in July 2021, a group of 11 heavily armed men with the Rise of the Moors group was stopped by State Police on I-95 in Wakefield, Massachusetts at 1:30 a.m. while traveling from Rhode Island to Maine for "training." The standoff lasted 9 hours with a shelter-in-place order issued for the surrounding area.[6] The men refused to provide identification and officers were unable to use facial recognition technology, which resulted in a delay in the booking process and investigation. And even if they could use the technology and if it were limited to Massachusetts DMV images, there likely would not be matches unless they were Massachusetts residents.

---

[5] *NIST Study Shows Face Recognition Experts Perform Better With AI as Partner*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (May 28, 2018), available at https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner.

[6] Kelly Murray and Elizabeth Joseph, *Massachusetts police standoff with heavily armed men ends in 11 arrests*, CNN (Jul. 3, 2021), available at https://www.cnn.com/2021/07/03/us/shelter-in-place-wakefield-reading-massachusetts/index.html.

Additionally, open-source data has been a game changer for rescuing and identifying victims such as children. Law enforcement has significantly increased the rate of identifying child victims of sexual abuse online using high performing facial recognition technology.

FACIAL RECOGNITION TECHNOLOGY SHOULD USE PUBLIC INFORMATION, WITH LIMITED EXCEPTIONS – ELIMINATING PRIVACY CONCERNS

Facial recognition technology service providers should only use lawfully sourced images including those from the public internet, government databases, or client enrollment services. For example:

- Open Social Media Posts and other online profiles (photos from a publicly available Instagram page (not a private post));
- News articles (photos taken as a part of a news story);
- Personal and professional websites (professional photo from work biography);
- Mug shots and other criminal databases;
- Public records sites and thousands of other open sources.

The U.S. Supreme Court has made it clear – "creation and dissemination of information are speech within the meaning of the First Amendment."[7] Algorithms that collect public information and then compare photographs provided by law enforcement is exactly the type of information dissemination intended by the Supreme Court. By limiting the data to only public information, many of the privacy concerns are alleviated.

NOT ALL FACIAL RECOGNITION TECHNOLOGY ALGORITHMS ARE USED AS SURVEILLANCE – SOME ONLY USE IT AFTER AN EVENT HAS OCCURRED

Software that provides facial recognition technology is not inherently surveillance. While some countries and certain algorithms can, and do, use the technology as surveillance, Clearview AI, for example, does not.[8] Without the surveillance function, the technology is used after an incident necessitates the identification of a person. Surveillance is the live monitoring of behavior, activities, or information. Using an investigative tool, including LexisNexis, a DMV database, Google, or any other search engine to look for information after a crime or incident occurs, is not surveillance.

---

[7] *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011).

[8] Dave Davies, *Facial Recognition And Beyond: Journalist Ventures Inside China's 'Surveillance State'*, NATIONAL PUBLIC RADIO (Jan. 5, 2021), available at https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta

Facial recognition technology is used to generate leads connected to an incident after an event has occurred. The process of uploading an image of a suspect, victim, or person of interest after an incident occurs is not "monitoring" or "surveillance" of an individual. Rather, it is an information gathering step in the investigative process equivalent to having an eyewitness review images to determine if they recognize a face (although the AI will be more accurate than the eyewitness). Facial recognition, allows this process to be advanced and accurate, thus delivering more timely and reliable leads.

Example: Jan. 2021 Capitol Insurrection

Facial recognition technology was not used as surveillance during the incidents occurring on January 6, 2021, at the United States Capitol. It was used after the fact to investigate criminal conduct. Law enforcement entities sought facial recognition technology to determine if their sometimes partial or fleeting photos of those involved in criminal conduct could be matched with publicly posted photos on the internet.[9]

RESPONSIBLE USE OF FACIAL RECOGNITION TECHNOLOGY IS SUPPORTED BY THE PUBLIC & PROVIDES SIGNIFICANT BENEFITS TO THE PUBLIC SAFETY

According to November 2021 research performed by Zogby Analytics, 75% of Massachusetts residents and more than 75% of Virginia residents see the use of facial recognition technology by law enforcement as appropriate and beneficial.[10] Specifically:

- 87% of Massachusetts residents said law enforcement should be able to search publicly available social media photos to help find missing children and to find or prosecute child sex offenders/traffickers;
- 83% of Massachusetts residents said law enforcement should be able to search publicly available photos to help find endangered adults and 82% are in favor of using the technology to positively identify endangered individuals;

---

[9] *The facial-recognition app Clearview sees a spike in use after Capitol attack*, NEW YORK TIMES (Jan. 9, 2021); *Local Police Force Uses Facial Recognition to Identify Capitol Riot Suspects*, WALL STREET JOURNAL (Jan. 8, 2021).

[10] *Three-in-Four Massachusetts Residents See Facial Recognition Technologies as Beneficial*, CISION PR NEWSWIRE (Nov. 30, 2021), available at https://www.prnewswire.com/news-releases/three-in-four-massachusetts-residents-see-facial-recognition-technologies-as-beneficial-301433959.html; *Three-in-Four Virginians See Facial Recognition Technologies as Beneficial*, CISION PR NEWSWIRE (Nov. 30, 2021), available at https://www.prnewswire.com/news-releases/three-in-four-virginians-see-facial-recognition-technologies-as-beneficial-301433955.html.

- 69% of Massachusetts residents think that private facial recognition database that only includes arrest mug shots would have a risk of being discriminatory with 52% saying it was a high or moderate risk;
- 90% of Virginia residents said law enforcement should be able to search publicly available social media photos to help find missing children and to find or prosecute child sex offenders/traffickers;
- 84% of Virginia residents said law enforcement should be able to search publicly available photos to help find endangered adults and 86% are in favor of using the technology to positively identify endangered individuals;
- 70% of Virginia residents think that private facial recognition database that only includes arrest mug shots would have a risk of being discriminatory with 52% saying it was a high or moderate risk.

These results match with a 2019 study by the Center for Data Innovation, which found that only 26 percent of Americans believe the United States government should strictly limit the use of facial recognition technology, and only 18 percent believe the government should strictly limit its use if it comes at the expense of public safety.[11] A 2020 study by NetChoice similarly found that 83 percent of Americans want state and local governments to improve law enforcement use of facial recognition rather than banning it.[12] A majority of individuals polled by NetChoice supported the technology's use for lead generation, keeping child predators off school grounds, finding missing senior citizens, and locating terrorists during an active terrorist attack.

Trafficking and Crimes Against Children

Facial recognition offers unprecedented capabilities to identify stalkers, rapists, child abusers, and other online predators and could facilitate identification of previously unknown child victims depicted in child sexual-abuse material proliferating online.

A Nevada Police Department investigator needed to identify a child that was being sexually exploited before she left the city. While online prostitution ads do not always provide identifying information for the workers, the ads often have high quality pictures that are suitable for facial recognition searches.

---

[11] Daniel Castro and Michael McLaughlin, *Survey: Few Americans Want Government to Limit Use of Facial Recognition Technology, Particularly for Public Safety or Airport Screening*, CENTER FOR DATA INNOVATION (Jan. 7, 2019), available at https://datainnovation.org/2019/01/survey-few-americans-want-government-to-limit-use-of-facial-recognition-technology-particularly-for-public-safety-or-airport-screening/.

[12] *Americans Want Facial Recognition Use By Law Enforcement Improved, But Not Banned*, NETCHOICE (Sept. 24, 2020), available at https://netchoice.org/media-press/americans-want-facial-recognition-use-by-law-enforcement-improved-but-not-banned/.

The investigator submitted one of the images from the ads, and within 10 to 15 seconds facial recognition technology provided a possible lead, including a link to the girl's Instagram page. By researching the contents of the public Instagram profile, the investigator positively identified the victim within two hours of the search – and confirmed that she was a 16-year-old juvenile. After booking an "appointment" for the next day, the investigator recovered the victim and apprehended her trafficker. She had been trafficked and abused since she was 13 years old. Time was of the essence and local law enforcement access to the technology was critical to this victim's safety.

Attempted Child Abduction

A suspicious YouTube video was shared to a Michigan police department Facebook account. The video showed conversations in which an adult male subject attempted to solicit child sexually abusive material from a 14-year-old female, and then attempted to abduct the juvenile victim at a park. A vehicle and partial license plate was visible in the video. A facial recognition search of the profile photo resulted in a match to the suspect's real social media account. Further investigation uncovered the suspect had a vehicle matching the partial plate and vehicle seen in the video. The investigative lead was forwarded to local authorities who continued the investigation and apprehended the suspect.

Identifying a Killer Who Targeted LGBTQ Victims[13]

Three members of the LGBTQ+ community were shot and killed by a man at a local home in Detroit, Michigan, in 2019. The Detroit Police Department used facial recognition – in combination with other investigative tools – to help identify the suspect based on video images from a nearby gas station. The suspect was charged with three counts of murder, in addition to other charges.

Identifying a Serial Armed Robber[14]

In 2018, detectives in Munster, Indiana, tried to identify a suspect who had attempted to rob a local business at gunpoint, after releasing a photo from the location's surveillance system which was shared by local media. No leads were generated until they used facial recognition and found possible match, a man that had skipped parole after serving a prison sentence for nine armed robberies in Illinois. The suspect was identified after the store owner was shown a photo lineup that included the man's

---

[13] Sarah Rahal, *Detroit man charged with triple LGBTQ killings*, THE DETROIT NEWS (Jun. 2019), available at https://www.detroitnews.com/story/news/local/detroit-city/2019/06/06/detroit-man-charged-triple-lgbtq-killings/1373342001/.

[14] Sarah Reese, *U.S. Marshalls Arrest Fugitive in Munster Payday Loan Business*, THE TIMES OF NORTHWEST INDIANA (July 7, 2018), available at https://www.nwitimes.com/news/local/illinois/u-s-marshals-arrest-fugitive-in-munster-payday-loan-business/article_9e538765-53a0-52f7-bc8a-34baa5bbdc54.html.

picture and was arrested several months later. Without facial recognition, the suspect would likely never have been found.

Scam Artist

Detectives in North Carolina were working to identify a scam artist in a fraud case. The detective searched a photo of the fraud suspect using facial recognition technology and was able to identify him from an article in New Jersey. The suspect was wanted in New Jersey for similar crimes.

SAFEGUARDS TO ENSURE THE RESPONSIBLE USE OF FACIAL RECOGNITION TECHNOLOGY

Facial Recognition Technology Civil Liberty Protection Principles

1. ***Accuracy and Non-Discrimination.*** Facial recognition technology must meet a minimum accuracy standard for face matches in all demographic groups to ensure non-discrimination against any demographic group. A facial recognition service shall be deemed to meet the standards by having participated in the business-relevant tracks evaluated by the Face Recognition Vendor Test (FRVT) from NIST and scored well. The algorithm is recommended to have received 99% or better true positive rates across all demographic groups at stringent false positive rates as selected by FRVT, or at high retrieval ranks. We note that FRVT regularly puts out new test datasets and retires old ones, so our recommendations must be put into context. On an absolute scale, algorithms will only get more accurate. Notwithstanding the foregoing, a lower standard of accuracy shall be acceptable to identify a person under the age of 18 in connection with providing the facial recognition service for protecting a minor at risk of abuse, kidnapping, or other threats to a minor's life or safety.

2. ***Privacy.*** The facial recognition technology must be designed so that it protects the privacy of persons by excluding, redacting, blurring, or otherwise obscuring nudity or sexual conduct, involving any identifiable person. This limitation shall not apply to images made available to the facial recognition service provider by an authorized law enforcement agency seeking to protect a minor at risk of abuse, kidnapping, or other threats to a minor's life or safety.

3. ***Records.*** Any facial recognition service provider must ensure there is a mechanism to produce a record that can be used to audit or review the information used to make a match of a person.

4. ***Match Verification.*** All facial recognition technology search results must be subjected to a secondary review and verification prior to acting on the match of a person.

5. ***Authorization and Accountability.*** A facial recognition technology use policy must be in place prior to utilizing the technology.

6. ***Independent Verification of the Lead.*** Information provided by facial recognition technology may be used as lead information to assist in identifying a person for an investigative purpose. A match provided by facial recognition technology cannot be used as the sole source for positive identification of a person.

7. ***Prohibition on Use by Law Enforcement for Persons Engaged in Protected Activities.*** Facial recognition technology may not be used to identify a person participating in constitutionally protected activities in public spaces unless there is an articulable investigative purpose.

Requirements for Facial Recognition Services Provider

1. Undertake reasonable steps to ensure that its facial recognition technology meets the standards of each of the Facial Recognition Safety Principles before it may provide facial recognition technology to any agency.

2. Require each user of its facial recognition technology to agree to abide by Facial Recognition Safety Principles in any use of its technology as a precondition to it providing such technology to the user.

3. Put into place a system of data security controls on any images or biometric information provided to the facial recognition service by any user to protect the security of such images or data, including steps to protect facial recognition technology data transmission, storage, and processing to ensure the privacy and security of such images or data, using commercially reasonable encryption and other cybersecurity and privacy best practices.

4. Notifying to the agency of any security breach or compromise of any data provided to the facial recognition service, as applicable, in the law of the jurisdiction.

5. Providing user training on the use of the facial recognition technology.