COMMENT TO OFFICE OF SCIENCE AND TECHNOLOGY POLICY (OSTP)
Docket No. 2021-21975
Submission by Clearview AI, Private Company

United States Office of Science and Technology Policy (OSTP) **January 15, 2022**
725 17th Street NW
Washington, D.C. 20528

RE: Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

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 biometric technologies, including facial recognition technology.

Facial recognition technology is a critical tool to ensure public safety, provided that proper safeguards are established. It is also a tool that is often characterized with inaccurate information. As stated by James Andrew Lewis, Senior Vice President at the Center for Strategic and International Studies, "[t]he level of confusion and misinformation in the FRT discussion is astounding. . . FRT is improving rapidly, and any critique based on data from even a few years ago runs the risk of being entirely wrong."[1]

Reasonable and effective policies eliminate many of the concerns surrounding the technology, including, but not limited to, discrimination, privacy concerns, and security breaches (such as access breaches).

Proper and reasonable safeguards include:

1) Accuracy requirements and non-discrimination;
2) Privacy protections by excluding and/or redacting explicit images;
3) Records to enable an audit or review of each use;
4) Match verification and secondary review of result;
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 any use of the technology to target persons engaged in protected activities.

[1] James Andrew Lewis, *Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (Sept. 29, 2021), available at https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape.

ACCURACY & TRANSPARENCY IN FACIAL RECOGNITION TECHNOLOGY

Procedures for and results of data-driven and scientific validation of biometric technologies

- Accuracy

Concerns over the use of facial recognition technology related to discrimination and bias can be eliminated by setting a 99% accuracy requirement. High-performing algorithms, as determined by the National Institute of Standards and Technology ("NIST"), do not contain racial bias and are at least 99% accurate in matching images. The Director of the Information Technology Laboratory for 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.[2]

Stringent standards for non-discrimination can be met by existing facial recognition technology. For example, NIST's October 2021 evaluation of Clearview AI's facial recognition algorithm found greater than 99% accuracy for all demographics – highlighting the dependability and accuracy in advanced algorithms.[3] In the same report, NIST also ranked Clearview's algorithm #1 in the United States and #2 in the world (most difficult-to-score category WILD photos, as well as average ranking). Subsequently in November 2021, in the most representative one-to-many investigation testing track, NIST once again ranked Clearview AI's algorithm #1 in the United States and #2 in the world (most difficult-to-score category VISA/Kiosk, as well as average ranking).[4]

While Clearview AI has achieved these very high scores in accuracy, the accuracy of facial recognition technology continues to increase generally. As noted by the U.S. Government Accountability Office ("GAO"), "[r]ecent advancements in facial recognition technology have

[2] *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.

[3] *Face Recognition Vendor Test (Part 1: Verification),* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Oct. 28, 2021), available at
https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf and
https://github.com/usnistgov/frvt/tree/nist-pages/reports/11 (past reports).

[4] *Face Recognition Vendor Test (Part 2: Identification)*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Nov. 22, 2021), available at
https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf and
https://github.com/usnistgov/frvt/tree/nist-pages/reports/1N (past reports).

increased its accuracy and its usage."[5] In fact, unlike older algorithms which use manual measurements, advanced and high-performing algorithms use a form of artificial intelligence called a "neural network".[6] These artificial neural networks operate similar to a biological brain, transmitting various signals to other neurons to map out the image. For example, Clearview AI'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.

Another means of maintaining accuracy is for the provider of a facial recognition technology to regularly update its image search engine with public images obtained by its search engine accessing information available to the general public on the internet, so that the data obtained is highly accurate and up-to-date. Data available to the public from the internet is valuable because, unlike traditional government databases, it can capture persons who are not previously known to authorities. A search engine that relies on a very large library of photographs, enhances the probability that the true match is covered in it and returned to the investigator. This reduces the likelihood of search misses, and the chances of investigators arriving at a false positive match derived from a limited search space and an early conclusion.

Therefore, with facial recognition technology, investigative effectiveness increases with the size and integrity of the underlying database. Larger databases are more likely to provide key information to protect the public than are smaller ones. The use of large public datasets for facial recognition also substantially mitigates the impact of historical inequalities and reduces the likelihood of discrimination, because large public reference databases, such as that developed by Clearview AI, are demographically rich and balanced.

Finally, retrieval rank and threshold are settings whereby an algorithm can be modified to return more results that may not be as accurate. Setting a low retrieval rank or threshold tends to return more false positives. High-performing algorithms should have hardcoded bottom lines for these criteria, 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.

- Transparency

Transparency is another key feature and is promoted by systems that enable the reconstruction of the reason for a search involving facial recognition technology, and the results of that search. This

[5] *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.

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

can be done by a platform requiring users to log on with an associated case number and type, and subsequently made available to the administrative supervisor associated with each particular user agency. This enables user agencies to monitor their individual users and ensure compliance with agency policies. The application can generate statistics for user agencies to show how it is being used and who is using it, to enable administrators to ensure that their agencies policies are being followed and that the technology is only being used for authorized purposes.

AVOIDING HARM – PRIVACY & SURVEILLANCE

Exhibited and potential harms of a particular biometric technology

- Privacy

Facial recognition technology service providers should use public information, with limited exceptions. This largely eliminates any potential privacy concerns related to the individual. Specifically, facial recognition service providers should only use lawfully sourced images including those from the public internet, government databases, or client enrollment services. Government investigators already have lawful access to every public image on the internet. Databases of such public images make the processing of those images faster and more accurate. NIST has found that forensic examiners performed best when supported by facial recognition technology and the most accurate performance resulted when these efforts are combined. "[A] team of scientists from . . . NIST and three universities have 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."[7] Facial recognition technology that maintains these kinds of protections achieves a vital public purpose. It is proportional, because the imposition on individual privacy associated with searching public imagery is small, while the benefits to public safety and to victims of crime are substantial.

- Surveillance

Opponents of facial recognition technology often mischaracterize facial recognition technology making it appear analogous to 24/7 mass surveillance. Some countries whose laws do not protect freedom of expression, freedom of movement and other civil rights can design and use the technology to engage in live monitoring of behavior, activities, or information.[8] But this type of

[7] *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-expertsperform-better-ai-partner.

[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.

use is not inherent in the technology, which can be limited to uses that are consistent with and strengthen human rights by protecting against false identifications as well as providing for accurate ones. The use of facial recognition as an investigative tool to look for information to identify a person after a crime or incident occurs is not surveillance. Indeed, LexisNexis, DMV databases, Google, and other search engines are routinely used to look for information after a crime or incident occurs. This type of use does not constitute surveillance even when such algorithms retrieve images to identify a person, nor does it become surveillance when the information they have is matched with a pilot image of a person to identify them. People identify other people using search engines all over the world, every moment of every day. Facial recognition technologies exist, but need to be used for appropriate purposes consistent with protecting societies, with guidelines to ensure that they are not abused.

- Example: Jan. 2021 Capitol Insurrection

Facial recognition technology was used after the fact to investigate criminal conduct during the incidents occurring on January 6, 2021, at the United States Capitol. Law enforcement entities successfully used facial recognition technology to determine if their partial or fleeting photos of those involved in criminal conduct could be matched with publicly posted photos on the internet, and found that the tool shortened the time required to identify persons involved in the incidents.[9]

Security of Facial Recognition Technology

Security considerations associated with a particular biometric technology.

Facial recognition technologies have the promise of providing tremendous value to law enforcement, and companies serving this market should treat law enforcement data with the appropriate level of protection. This means companies should implement strong security programs and internal controls around customer data. These security programs should include industry standard best practices such as annual penetration tests, bug bounty programs, secure software development techniques, endpoint detection and monitoring, and data loss prevention. Internal controls should limit employee access to customer data as much as possible, and all employee and customer actions should be logged and auditable.

Real Uses of Facial Recognition Technology & Potential Benefits

Descriptions of use of biometric information for recognition and inference & exhibited and potential benefits of a particular biometric technology

[9] Kashmir Hill, *The facial-recognition app Clearview sees a spike in use after Capitol attack*, New York Times (Jan. 9, 2021), available at https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html; Jared Council, *Local Police Force Uses Facial Recognition to Identify Capitol Riot Suspects*, Wall Street Journal (Jan. 8, 2021), available at https://www.wsj.com/articles/local-police-force-uses-facial-recognition-to-identify-capitol-riot-suspects-11610164393.

Responsible use of facial recognition technology is supported by the public for appropriate public uses, such as solving crimes, protecting victims, and rescuing endangered persons. 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;

- 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

[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.

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 ban 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.

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.

[11] Daniel Castro and Michael McLaughlin, S*urvey: 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/.

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 a 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 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

Like any technology, facial recognition can be used properly to help protect people and societies, to speed identification of people to enable them to safely secure access to protected areas, to enable them to efficiently obtain services, such as access to their online accounts. Guidelines that shape how facial recognition technologies are used are an essential element of ensuring that they protect civil liberties while meeting other important objectives consistent with living in a free society. Principles such as accuracy and non-discrimination, protecting privacy, ensuring accountability, and preventing the abuse of the technology to surveil domestic populations engaged in protected or private activity, are all essential elements of making facial recognition technology serve the public interest.

[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.

The chart below provides the essential principles for facial recognition technology's use in the public interest.

CIVIL LIBERTY PROTECTION PRINCIPLES	
Accuracy & 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.
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.
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.
Result Validation.	All facial recognition technology search results must be subjected to a secondary review and verification prior to acting on the investigative lead.
Authorization & Accountability.	A facial recognition technology use policy must be in place prior to utilizing the technology.
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.
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 TECHNOLOGY SERVICE PROVIDER

facial recognition technology to any agency.

#3

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.

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.

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