HJ48 Study
The Future of Facial Recognition Technology
Economic Affairs Interim Committee's Panel Discussion
February 9, 2022

Comments Submitted by Clearview AI

Clearview AI, a US-based company, is dedicated to providing the most cutting-edge technology to law enforcement to investigate crimes, enhance public safety, and provide justice to victims. Clearview AI is pleased to provide public comment on the future of facial recognition technology to the Economic Affairs Interim Committee.

This Committee is to be commended for its attention to the multifaceted issues implicated by facial recognition technology—which critically includes protecting the privacy and constitutional rights of Montanans while not limiting appropriate use of facial recognition by government agencies. Clearview AI believes that these goals can be mutually attained, without compromising law enforcement's ability to investigate crimes and protect victims.

Clearview AI's Support of Law Enforcement

Clearview AI is a facial recognition search engine, used by law enforcement agencies around the United States. Clearview AI has developed a neutral algorithm and database that analyzes images from publicly available sources on the web. Clearview AI makes this patented technology available to law enforcement agencies to aid in identifying crime victims—particularly exploited minors and alleged perpetrators. Indeed, law enforcement agencies across the country rely on Clearview AI to investigate and help solve crimes, including financial fraud, human trafficking, and crimes against children.

As Montana continues to grapple with how to address a rise in violent crimes, including homicide, the responsible use of facial recognition technology is an important option in the government's toolkit.[1] Clearview AI's platform, which uses information already accessible to any member of the public online, is an important early investigation tactic.

Clearview AI's Platform Ensures Oversight & Transparency

There are some misconceptions regarding facial recognition particularly in regards to Clearview AI's platform. Facial recognition technology as provided by Clearview AI does not involve surveillance, ongoing monitoring of people, or real-time identification of anyone. Instead, Clearview AI provides assistance after an incident occurs, as part of a human-led law enforcement investigation. As an initial matter, use of Clearview AI technology involves human input on the front end, requiring a law enforcement officer to upload a photo of a person of interest, such as an alleged perpetrator or victim. And on the back end, results populated in the Clearview AI platform based on the source photo are naturally subject to further human review and investigation.

---

[1] Keith Schubert, *FBI: Rate of Violent Crime in Montana Continues to Surpass National Rate* (Nov. 3, 2021), available at https://dailymontanan.com/2021/11/03/fbi-rate-of-violent-crime-in-montana-continues-to-surpass-national-rate/.

Moreover, accountability is a principle coded into Clearview AI's platform as the technology cannot be used for a fishing expedition or for other improper purposes. Instead, internal system controls only allow Clearview AI's platform to be used in connection with specific cases or investigations—with a record of which individuals are using it and for what purposes. The gatekeeping controls that are built into Clearview AI's system include:

(1) Intake controls: Users are required to complete of intake forms and provide information including the CJIS code, case number and investigation type (if applicable) before running a search;

(2) Administrative oversight: Among other things, system administrators can view organizational and individual user search history to deter and detect improper use of the Clearview AI platform; and

(3) Usage reporting and auditing: Additionally, system usage reports are generated automatically, enabling meaningful oversight.

Clearview AI's Superior Algorithm Does Not Result in Bias

Unlike mugshot databases, which are limited to people with previous arrests, large public image sets like Clearview AI's are race-neutral. Indeed, Clearview AI provides results at consistently high rates of accuracy across all types of demographic groups. Law enforcement's use of independently validated, non-discriminatory technology like Clearview AI's reduces risks to innocent people and helps law enforcement more quickly identify suspects or victims from a pilot image, so they can investigate further.

The data from the tests conducted by the U.S. government's National Institute of Standards and Technology ("NIST") have confirmed the superior accuracy and reliability of the Clearview AI's platform. In October 2021, NIST ranked Clearview AI's algorithm #1 in the United States and #2 in the world (most difficult category WILD photos, as well as average ranking)[2]. In NIST's key test that evaluates demographic accuracy, Clearview AI's algorithm consistently achieved greater than 99% accuracy across all demographics. 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 category VISA/Kiosk, as well as average ranking)[3].

The accuracy of Clearview AI's algorithm across all demographics can also reduce the harm caused by mistaken eyewitness identifications, which according to the Innocence Project contributed to approximately 69 percent of the more than 375 wrongful convictions in the United States overturned by

---

[2] *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).

[3] *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).

post-conviction DNA evidence.[4] Facial recognition can help prevent wrongful arrests, in addition to helping with the identification of perpetrators and victims alike.

Clearview AI Supports Law Enforcement Efforts to Stop Human Trafficking and Protect Vulnerable Groups, Including Minors

Facial recognition technology offers unprecedented capabilities to identify stalkers, rapists, child abusers, and other online predators and to facilitate identification of previously unknown child victims depicted in child sexual-abuse material proliferating online. Laws that narrowly limit the ability of law enforcement to use facial recognition technology risk harming victims and enabling serious criminals to escape. This is especially true for victims of ongoing child abuse who need to be rescued from child predators.

For instance, a Nevada Police Department investigator needed to identify a child that was being sexually exploited before she was trafficked by criminals outside of the city. Using an image from an online solicitation ad, the investigator used facial recognition technology to provide a possible lead, which generated 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. The next day, thanks to this lead, the investigator rescued 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 Clearview AI's technology was critical to this victim's rescue.

Americans Support the Responsible Use of AI and Facial Recognition Technology by Law Enforcement

Responsible use of facial recognition technology is supported by the public for appropriate uses, such as solving crimes, protecting victims, and rescuing endangered persons. These results match with a 2019 study by the Center for Data Innovation, which found that only 26% of Americans believe the US government should strictly limit the use of facial recognition technology, and only 18% believe the government should strictly limit its use if it comes at the expense of public safety.[5] A 2020 study by NetChoice similarly found that 83% of Americans want state and local governments to improve law enforcement use of facial recognition rather than ban it.[6] 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.

---

[4] *The Innocence Project: Eyewitness Identification Reform* (undated), available at https://innocenceproject.org/eyewitness-identification-reform/#:~:text=Mistaken%20eyewitness%20identifications%20contributed%20to,by%20post%2Dconviction%20DNA%20evidence.&text=Inaccurate%20eyewitness%20identifications%20can%20confound%20investigations%20from%20the%20earliest%20stages.

[5] 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/.

[6] *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/.

Proposed Framework

At the beginning of this calendar year and legislative calendar, a number of legislatures have introduced bills that will either hamper or restrict law enforcement's use of AI and facial recognition technology. In addition to these bills' and their sponsors' failure to recognize the public safety benefit that comes with the responsible use for technology like Clearview AI's, many of these states have failed to recognize the perhaps unintended economic consequences that overreaching laws will have on businesses in their states. By way of example, Illinois' Biometric Information Privacy Act ("BIPA") has resulted in nearly a thousand lawsuits against Illinois businesses of all sizes. And with BIPA's statutory liquidated damages provision, these lawsuits can entail millions if not billions of dollars in litigation exposure. Meanwhile, insofar as BIPA is concerned, the law has provided limited appreciable privacy protections to Illinois citizens and at the same time being a boon for plaintiffs' lawyers. Many of the bills introduced in this session nationwide would similarly result of flooding those states courts with similar claims and subjecting their states' businesses to billions of dollars of risk, while providing minimal to no benefits to their citizens.

Montana should take into account the above unintended effects when framing any legislation regulating privacy generally or more specifically, biometric information or law enforcement's use of AI or facial recognition technology.

Facial recognition technology can be used responsibly to protect the public and our common values, with appropriately designed guardrails. These should include:

- **Requiring facial recognition technology to be based solely on publicly available information and existing government databases**. Since no private information is being accessed, there is no need for a search warrant or court order. Similarly, requiring consent for the use of information collected from public sources is not feasible and even if it were, obtaining the consent of, for example, a suspect in a criminal investigation or a minor victimized by human trafficking would hamper the investigation.

- **Requiring Accuracy and Non-Discrimination**. Any facial recognition technology service provider should have its accuracy independently verified. Clearview recommends a minimum accuracy standard of 98% as determined by the National Institute of Standards & Technology (NIST) for face matches in all demographic groups to ensure non-discrimination, with a lower standard of accuracy possibly permitted to identify a person under the age of 18 at risk of abuse, kidnapping, or other threats to a minor's life or safety.

- **Mandating Record Requirements for Audit**. Every facial recognition technology provider should be required to create a system enabling records to audit and verify the images and information used to make a match of a person—as Clearview AI has done.

- **Mandating Independent Match Verification by Humans**. All facial recognition technology search results should be required to have a separate human review and verification prior to law enforcement acting on any match of a person. Decisions on investigating suspects are too important to have the decisions be made by any machine. A separate decision by a trained official

to initiate any law enforcement action following an apparent match through facial recognition technology is essential.

Conclusion

The Montana legislature is to be commended for its consideration of these issues in a way that balances the continued right of Montanans to privacy protections while remaining a friendly place to do business. At Clearview AI, we are proud of the steps we have taken to set what we believe should be a model for the use of facial recognition technology and look forward to working with this committee to solidify best practices and a legislative framework in a way that balances the need for Montana citizens' privacy, public safety, and the responsible use of technology by law enforcement.