RESPONSE TO PUBLIC CONSULTATION
TORONTO POLICE SERVICES BOARD

Dubi Kanengisser, PhD
Senior Advisor, Strategic Analysis and Governance
Toronto Police Services Board
40 College Street
Toronto, ON M5G 2J3
dubi.kanengisser@tpsb.ca

December 15, 2021

Re: Use of New Artificial Intelligence Technologies Policy

Clearview AI appreciates the opportunity to provide a submission to the Toronto Police Services Board's ("TPSB") Use of Artificial Intelligence Technology Policy (the "AI Policy"). Clearview AI is a company based in the United States which provides facial recognition services to law enforcement. Clearview AI does not do business in Canada, and accordingly our technology is not currently available for use in Toronto or anywhere in Canada, by law enforcement or any other person. We write to you in response to your public consultation regarding the draft of the AI Policy in the belief that such public consultations can lead to police that align law enforcement interest with protecting fundamental rights enabling facial recognition technology to be used properly as a critical public safety tool.

We urge that such policies mandate:

(1) Accuracy requirements and non-discrimination;
(2) Recording that enables audit or review of each use;
(3) Match verification and secondary review of result by humans, to avoid automated decision making;
(4) Privacy protections that exclude and/or redact 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 agencies for persons engaged in protected activities.

BACKGROUND

One of the initial stumbling blocks in having an objective discussion on new technologies, specifically with respect to facial recognition technology, is the lack of a uniform definition.

Opponents of facial recognition technology continually use sinister characterizations in their definitions of facial recognition technology making it appear analogous to 24/7 mass surveillance. Yes, some companies have developed facial recognition technology that can be used in real-time surveillance and, yes, some countries do use facial recognition technology for real-time surveillance operations. But those relatively few use cases do not define the technology itself or how it can be appropriately and effectively utilized by governments for public safety while still protecting civil liberties.

Clearview AI offers an image search engine tool that is used after-the-fact to assist law enforcement investigations involving imagery, enhancing public safety while respecting fundamental rights, freedoms, and democratic values. To that end, we support reasonable and informed regulation of the use of facial recognition technology.

For the purposes of after-the-fact investigations, larger datasets are essential to effective law enforcement use of facial recognition. They increase the likelihood that law enforcement can make a positive identification, thereby reducing the likelihood of a false positive match. Every photo in the dataset is a potential clue that could save a life, provide justice to an innocent victim, prevent a wrongful identification, or exonerate an innocent person.

As a leading provider of facial recognition technology for law enforcement and national security applications, Clearview AI has developed a series of best practices to enable facial recognition software to be used for socially beneficial purposes consistent with the principles set forth in the draft AI Policy.

DRAFT AI POLICY

Review and Assessment of New AI Technologies states that AI systems must go through a review and evaluation prior to adoption. Specifically, it identifies certain risk categories and notes, under (c)(i)-(iii), the importance of having a "human-in-the-loop" and ensuring that the individual does not have difficulty in identifying "bias or other decision failures of the AI."

- Human Verification

In a properly designed platform for facial recognition technology, human review and independent verification are required as a part of every search so that no automated decision-making is relied upon. The section below on additional safeguards further details this important requirement.

- Elimination of Racial Bias

While human verification is critical, so is ensuring that the facial recognition technology service provider is at least 99% accurate in matching – to eliminate bias. The Director of the Information Technology Laboratory for the U.S. National Institute of Standards and Technology ("NIST")[1], Dr. Charles Romine testified in 2020 before the U.S. House of Representatives 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] In fact, unlike older algorithms which use manual measurements, advanced and high-performing algorithms, such as Clearview AI's, use a form of artificial intelligence called a "neural network".[3] These artificial neural networks operate similar to a biological brain, transmitting various signals to other neurons to map out the image. By way of 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.

Accurate non-discriminatory algorithms benefit both the users of facial recognition technology and the data subjects, by providing a neutral place for the users to begin their identification process. This principle should be a foundation for the use of the technology. Investments in AI to ensure accuracy make a concrete difference in results: 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)[4]. 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

[1] Established by the United States Congress in 1901, the National Institute of Standards and Technology, a division of the U.S. Department of Commerce, provides the marketplace with accurate and reliable information about companies' measurable industrial and technology performance capabilities.

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

[4] *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).

Clearview AI's algorithm #1 in the United States and #2 in the world (most difficult category VISA/Kiosk, as well as average ranking)[5].

Board Approval and Reporting Prior to Procurement, Utilization and Deployment calls for transparency in how the AI operates, what information will be collected, the accuracy of the technology, as well as the overall privacy impact.

- Accuracy and Transparency

Accuracy is fundamental to the appropriate use of AI. Testing by NIST or another impartial, technically competent independent third-party is therefore an essential requirement for facial recognition technology. One 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.

Transparency is also a 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 can be done by a platform requiring users to log on with an associated case number and type and made available to the administrative supervisor associated with each particular user agency, enabling user agencies to monitor their

[5] *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).

individual users and ensure compliance with agency policies. The application can generate statistics for user agencies to show how it is being used and by whom.

- Privacy Rights

Further safeguards assist in ensuring individual privacy rights are not violated. 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."[6]

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.

FURTHER SAFEGUARDS TO PROTECT INDIVIDUALS, WHILE PROVIDING A CRITICAL PUBLIC SAFETY TOOL

The below safeguards will further assist TPSB's in its policy goals related to AI technology, including, but not limited to, preserving "the privacy, rights and dignity of individuals and communities," ensuring consideration and mitigation of "possible unintended consequences," and ensuring evaluation and reassessment as needed.

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-

[6] *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.

relevant tracks evaluated by the Face Recognition Vendor Test (FRVT) from NIST (and scored well) or tests from other independent and reliable technology review agencies in the applicable jurisdiction ("other tests"). 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/other tests, or at high retrieval ranks. We note that FRVT regularly puts out new test datasets and retires old ones, so our recommendations have to 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. ***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.

3. ***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.

4. ***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.

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 facial recognition technology.

In conclusion, Clearview AI believes the draft AI Policy properly aligns the protection of individual privacy with the enhancement of public safety, but as set forth in this repose, there are additional requirements which could provide further protections to individuals and enhance the value of facial recognition technology for law enforcement uses. The suggestions we have made would further ensure that facial recognition technology service providers have accurate, high-performing, and transparent technologies and systems to provide preliminary matches for human review and assess to assist law enforcement and protect victims, reducing the risk of misidentification and bias. Accordingly, Clearview AI urges Toronto to move forward with adoption of an AI Policy consistent with these principles as a means to ensure that technological development in the field of investigative image tools is accompanied by a clear and appropriate legal and public policy framework.