Good morning and thank you for the opportunity to address the Commission. My name is David Ray, and I am the COO and General Counsel of Rank One Computing, a leading developer of face recognition technology based in Denver, Colorado. Our algorithms are widely used by the federal government, state and local law enforcement and the financial sector.

Proponents of face recognition bans assert the technology is inaccurate, racially biased and abused by law enforcement. These three claims are so frequently repeated that they’ve often been accepted as fact. In reality, claims of inaccuracy, bias and abuse are not well supported by the record.

The 2018 Gender Shades paper claims that face recognition “misidentifies” dark-skinned women nearly 35% of the time. The problem is: Gender Shades evaluated demographic-labeling algorithms not face recognition. Gender Shades tells us that IBM was not very good at gender classification when tested in 2017, which result IBM challenged, saying that its replication of the study found an error rate of 3.5%, not 35%. Gender Shades says nothing about the accuracy of face recognition technology.

The only scientific article cited by the Georgetown Privacy Law Center found that algorithms in 2012 were 5-10% less likely to retrieve a matching photo of a Black individual than other demographics. The now-obsolete algorithms predate deep learning techniques that have enabled a thousand-fold increase in accuracy. Ten years ago, accuracy was measured in errors per thousand candidates versus per million today.

The 2019 NIST Demographic Effects report found that top-tier face recognition technologies had “undetectable” differences in accuracy across racial groups. Critics seized upon differences in accuracy with the lowest performers and claim the report showed “African American people were up to 100 times more likely to be misidentified than white men.” Government applications use top-tier face recognition algorithms from NEC, Idemia and Rank One Computing, not the lower-performing submissions.

NIST’s FRVT Ongoing shows that accuracy among demographics is very closely balanced, and if anything, the White male demographic shows the lowest accuracy, not the highest. According to last month’s evaluation, each of the top 150 algorithms are over 99% accurate across Black male, White male, Black female and White female demographics. For the top 20 algorithms, accuracy of the highest performing demographic versus the lowest varies by 0.1%, the difference between 99.7% and 99.8%, and White male is actually the lowest performing of the four demographic groups.

To summarize, Gender Shades is not a study of face recognition, and the obsolete 2012 FBI study pre-dates deep learning. On the other hand, the 2019 NIST Demographic Effects study showed “undetectable” differences for top-tier algorithms, and the FRVT Ongoing shows accuracy at 99.7% for White male vs. 99.8% for other demographics.

The claim of inaccuracy is not supported. Automated face recognition is today more accurate than the human eye witness. Per NIST FRVT Ongoing, top performers show a 99.8% True Accept Rate at 99.9999% True Reject Rate on the largest dataset. The best science available suggests that face recognition is highly accurate, across all demographics. As an industry, face recognition developers would welcome a high fidelity ongoing academic study to definitively address the bias question.

Second, is police abuse of face recognition rampant? There are 3 false arrests total all-time across the country, totaling 2 weeks in jail, due in each case to inexcusable human police work not face recognition. On the other hand, the technology has been used tens of thousands of times, resulting in thousands of possible matches. In 2019 alone, NYPD used face recognition 9,850 times resulting in 2,510 possible matches, including 68 murders, 66 rapes, 277 felony assaults, 386 robberies and 525 grand larcenies and no known false arrests.

Every technology and technique has an error rate. Policies and procedures ensure that any errors are mitigated, and face recognition has well established policies and procedures from joint FBI-NIST efforts known as FISWG and OSAC. These require trained human facial examiners to make final determinations based on morphological matching guidelines, and that result is merely an investigative lead. Further police investigation is required prior to making an arrest. Face recognition is highly effective at preventing & solving crime and there has been minimal false arrest error to date.

The sage purpose of this commission is to closely examine the technology prior to rulemaking. Claims of inaccuracy, bias and abuse by law enforcement are not well supported by the record, and we urge this commission to study and adopt the best practices already in use by leading law enforcement agencies.