EXHIBIT A
What is facial recognition?

Facial recognition is a digital technology that NYPD uses to compare images obtained during criminal investigations with lawfully possessed arrest photos. No one has ever been arrested solely based on a facial recognition search. When used in combination with human analysis and additional investigation, facial recognition technology is a valuable tool in solving crimes and increasing public safety.

How is facial recognition used by the NYPD?

Since 2011, the NYPD has successfully used facial recognition to identify suspects whose images have been captured by cameras at robberies, burglaries, assaults, shootings, and other crimes.

What happens after the computer matches are identified?

If possible matches are identified, trained Facial Identification Section investigators conduct a visual analysis to assess the reliability of a match and conduct a background check to compare available
information about the possible match and relevant details of the investigation.

Are matching photos grounds for arrest?

No. A facial recognition match does not establish probable cause to arrest or obtain a search warrant, but serves as a lead for additional investigative steps. The detective assigned to the case must establish, with other corroborating evidence, that the suspect identified by the photo match is the perpetrator in the alleged crime.

Has the software provided substantial leads in criminal cases?

Yes. In 2019, the Facial Identification Section received 9,850 requests for comparison and identified 2,510 possible matches, including possible matches in 68 murders, 66 rapes, 277 felony assaults, 386 robberies, and 525 grand larcenies. The NYPD knows of no case in New York City in which a person was falsely arrested on the basis of a facial recognition match.

Have studies shown that some facial recognition software is less accurate in analyzing the faces of African Americans, Asians, women and other groups than of white men?

Some studies have found variations in accuracy for some software products. The most important federal government study on the subject, however, noted that in "hybrid machine/human systems," where the software findings are routinely reviewed by human investigators, erroneous software matches can be swiftly corrected by human observers. The safeguards built into the NYPD's protocols for managing facial recognition, which provide an immediate human review of the software findings, prevent misidentification.

Is video from the body-worn cameras now worn by most NYPD officers routinely submitted for facial recognition analysis?

No. For example, the NYPD does not use facial recognition technology to examine body-worn camera video to identify people who may have open warrants. However, if an officer, whose body-worn camera is activated, witnesses a crime but is unable to apprehend the suspect, a still image of the suspect may be extracted from body-worn camera video and submitted for facial recognition analysis.

Does the NYPD use facial recognition technology to identify people recorded on the city's network of security cameras?

The NYPD does not use facial recognition technology in this manner. Video from city-owned and private cameras is not analyzed unless it is relevant to a crime that has been committed.

Does the NYPD use facial recognition to monitor and identify people in crowds or at rallies?

No.

Does the NYPD use facial recognition technology to routinely compare images of unidentified suspects to other government photo databases, like drivers' license photos from the NYS Department of Motor Vehicles, or to social media?

No. In rare cases, however, the Chief of Detectives or Deputy Commissioner of Intelligence and
Counterterrorism may specifically authorize the comparison of an unidentified suspect's image against images other than mug shots, if there is a legitimate need to do so.

Read our policy detailing the specific permissible use of facial recognition technology, click here.