NCRB move for new facial recognition system triggers fresh privacy concerns

New Delhi:

The National Crime Records Bureau (NCRB) has initiated the process of installing an automated facial recognition system (AFRS) that will help identify persons by matching digital images, photos and video feeds with an existing database, in a move that raises concerns over privacy.

According to the request for proposal (RFP) document seeking open bids for an AFRS solution, the benefits include a robust system for identifying criminals, missing kids and persons, unidentified bodies and unknown persons. For example, AFRS is intended to zero in on images or videos related to a crime or mob violence and compare select facial features with existing image database.

The AFRS will offer a repository of photographs of criminals and help the police check suspects with the hotlist of criminals. It will also contain images of missing persons that can be matched with images and videos that investigators might be examining. A match on a criminal spotted near an abduction site would be another example of the utility of the system.

However, the use of AFRS does raise issues of privacy and security and questions about how many agencies will access the system and what sort of safeguards are proposed. The concern about potential misuse of the system for purposes other than criminal investigation and the legal framework governing its use has been highlighted by privacy and transparency activists.

San Francisco bans facial recognition over safety issues

Recently, San Francisco in the US banned the use of facial recognition by the city’s police and other agencies. The AFRS solution will be a web-based application hosted at the NCRB data centre in Delhi, with connectivity to police stations through the Crime and Criminal Tracking Network and Systems (CCTNS).

The system shall offer logical algorithms and userfriendly, simple graphical user interface making it easy to perform facial matching. Face images can be captured from CCTV feeds and alerts generated if a blacklist match is found. The system would have the option to upload bulk subject images and generate alerts if images match with the registered faces in the database.

The system shall be able to broadly match a suspect or criminal’s photograph with a database created using images available with passport, CCTNS, prisons, state or national automated fingerprint identification system or any other image database available with the police/other entity.
While NCRB claims AFRS will greatly facilitate investigation of crime and detection of criminals and provide information for easier and faster analysis, cyber experts have raised data privacy issues given that the system is sought to be rolled out even as a data protection law has not been enacted. The possibility of the system being used for profiling and reliability of the matches is under discussion.

As per the RFP on the NCRB website, AFRS shall be implemented by the solution provider selected through a bid that must be submitted by August 16, followed by opening of bids on August 19.

The RFP said the system should be able to identify faces of individuals by extracting features, contours and other prominent points. It should be able to match facial images with change in facial expression, direction, angle, lighting, age, hairstyle, beard, glasses, scars, marks and tattoos.

It will enable a handheld mobile with an app to capture a face on the field and get the matching result from the backend server. Authorised requests for search, matching and verification of facial image would come from police stations.