Issues in Facial Recognition in Law Enforcement

Statement by Dr. Cedric L. Alexander

On July 9, the Portland, Maine, *Press Herald* reported on two newly enacted laws that make Maine the first US state to enact a broad ban on government use of facial recognition technology. In Maine, state, county, and municipal governments will not be allowed to use any sort of FRT. Law enforcement may use the technology for investigating certain serious crimes, but state law enforcement agencies are barred from implementing their own FRT systems. They may request FRT searches from the FBI and the state Bureau of Motor Vehicles in certain cases.

A year earlier, in August 2020, the Portland City Council totally banned the use of facial recognition by the police. Indeed, currently some 24 American cities ban police FRT use, and Black Lives Matter has called for a nationwide ban because of evidence that false positive identifications in the case of people of color exceed the rate for whites. So far, the federal government has enacted no laws on how law enforcement may or may not use FRT.

The benefits of facial recognition systems for policing are quite evident. It is a fact that the technology can aid in the detection and prevention of crime. For example:

- Facial recognition is effectively used when issuing identity documents and is usually combined with other long-accepted biometric technologies, such as fingerprints and iris scans.

● FRT face matching is used at border checks to compare the portrait on digitized biometric passports.

● In the United States, at least 26 states (perhaps more) permit law enforcement to run searches against their databases of driver's license and ID photos. (The FBI has access to the driver's license photos of 18 states.)

● FRT was used to identify suspects in the January 6 violent breach of the U.S. Capitol, and high-definition digital photograph and videography (sometimes deployed from aerial drones) may be used increasingly to identify faces in mass events.

● Facial recognition closed-circuit TV systems may be used in such public security missions as finding missing children and disoriented adults, identifying and tracking criminals and criminal suspects, and generally supporting and accelerating investigations.

Currently, the FBI is the nation's leading law enforcement agency using FRT, and it has developed technologies and best practices to promote the intelligent use of the technology to reduce errors and protect constitutional rights. In addition, the Facial Identification Scientific Working Group (FISWG), operating under National Institute of Standards and Technology (NIST) Organization for Scientific Area Committees, is working to develop standards in FRT.

Facial recognition technology has been useful in law enforcement and, I believe, will continue to develop technically and therefore become even more useful. Blanket bans on FRT in policing are unwarranted and deny to police agencies a tool that is an important aid to public safety.

But make no mistake. There are urgent constitutional issues relating to privacy, protection from unreasonable search, due process, and the presumption of innocence. Especially concerning are false positive and negative identification results. Although a Customs and Border Patrol (CBP) internal analysis found a false positive rate that compared favorably with identifications made directly by human observers, a late 2019 NIST study confirmed that FRT accuracy does vary by demographic factors, including age, sex, and race. And, yes, aalse positives are higher for Asian and African American faces compared to those of Caucasians.

In addition, police do not always use FRT correctly. For instance, on May 16, 2019, *The Washington Post* reported that some agencies use altered photos, forensic artist sketches, and even celebrity look-alikes for facial recognition searches. "In one case," the *Post*'s Drew Harwell wrote, "New York police detectives believed a suspect looked like the actor Woody Harrelson, so they ran the actor's image through a search, then arrested a man the system had suggested might be a match."

Forgive my being blunt. But this is stupid.

Using artificial intelligence to confer upon a highly subjective visual impression a halo of digital certainty is neither fact-based, prudent, efficient, nor just. But, under federal law, at least, it is not illegal—for the simple reason that no federal laws govern the use of facial recognition.

Absent federal laws—or even a fully developed professional and legal consensus—states are beginning to fill the legislative vacuum. In some cases, they are doing so by simply banning all police use of FRT.

What we really need is intelligent policy and legislation, beginning with a requirement for transparency. At present, very few law enforcement agencies disclose how and how frequently they use FRT. Even fewer audit their personnel for improper use of facial recognition systems. Most departments have no internal oversight or accountability mechanism to detect misuse. Secrecy in matters of constitutional rights, human rights, and civil rights provokes fear and suspicion.

And it should.

Like so many digital technologies, facial recognition was not long ago the stuff of science fiction. Today, many of us carry it in our pockets in the form of a smartphone that recognizes our face when we take it out to make a call or send a text. FRT has become a normal part of 21st-century living. I believe that most Americans are willing to accept that facial recognition can be a valuable tool in law enforcement. But without the judicious and just application of ***human*** intelligence, including full-disclosure transparency, public accountability, prudent legislation, and science-based regulation and best practices guidance, the technologies of ***artificial*** intelligence are not tools. They are blunt instruments. And we all know that blunt instruments can become weapons. We cannot afford to sacrifice constitutional rights on the one hand or, on the other, a technology that can promote justice and even save lives.