Opening Statement of Dr. Cedric Alexander

Testimony to the Committee on Oversight and Reform, May 22, 2019

Based on a 2016 investigation by the Georgetown Law Center on Privacy and Technology, at least a quarter of U.S. law enforcement agencies use facial recognition searches of their own databases or those of other agencies to attempt to identify, find, and arrest criminal suspects. As of 2016, at least 16 states permit the FBI to use the technology to compare suspects' faces with images on state-issued IDs.

Now, sometimes law enforcement uses facial recognition prudently and wisely. Sometimes, quite recklessly. On May 16, *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 writes, "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."

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

At this point, law enforcement use of facial recognition in not only unregulated by law, it operates even without any consensus on best practices. Artificial intelligence systems do not invent results from thin air. They operate from databases of *identified* faces in an attempt—an *attempt*—to match one of those *identified* faces with the face of a suspect or subject of interest or an unsub, an *unknown subject* for whom no facial image is yet known. An artificial intelligence

system is only as good as its database, yet there is currently no standard governing the contents of any agency's facial images database.

Who is included in it? Who knows?

What we *do* know is that publicly available facial databases fail to represent the size and diversity of the American population and are therefore inherently biased samples.

Real-time video surveillance can identify criminal activity in progress, but, for the purposes of investigation, what are the risks to Fourth Amendment guarantees against unreasonable search and seizure? And what legal standards should be required prior to a facial-recognition search?

Answer: We don't know.

And before we leave the Constitution, is there a basis to fear that the combination of widespread real-time video surveillance and facial recognition AI may infringe on the First Amendment protection of free speech, assembly, and association?

So far, this remains unanswered—barely even addressed.

How accurate is facial recognition technology? The answer is "It depends." And that is an unacceptable answer for law enforcement, the justice system, and the people.

Facial recognition works best with frontal images and bright, even lighting. Identifying partially turned faces or those poorly lit is like trying to read a badly smudged latent fingerprint. Real-time video surveillance often supplies poor-quality images that result in erroneous identifications.

One would think that *artificial* intelligence would preclude racial and other biases. In fact, as *The New York Times* reported in February of last year, facial recognition algorithms marketed by such major software suppliers as Microsoft, IBM, and Face ++ [Face Plus-Plus] were significantly more likely to misidentify the gender of black women than white men. Gender was misidentified up to 1% of the time in the case of lighter-skinned males but 35% of the time in darker-skinned females.

The problem of AI skin-color bias is serious enough that, as CBS News reported on May 13, San Francisco is considering a citywide ban on facial recognition in all government agencies. Now, this seems to me an overreaction—but, considering the current absence of laws, regulations, or even generally agreed-upon best practices—it is an understandable overreaction.

We human beings are hardwired by evolution to fear and suspect danger when confronting the unknown. The opaque, even secretive attitude of law enforcement with regard to facial recognition plays into this primal fear. The Georgetown Law Center on Privacy and Technology reports that "defense attorneys have never received face recognition evidence as part of a Brady disclosure"—the legally required disclosure of exculpatory or impeaching evidence that may prove the innocence of a defendant.

Only a very small minority of law enforcement agencies disclose how and how frequently they use facial recognition. Very few agencies even claim to audit their personnel for improper use of facial recognition systems. Indeed, the vast majority of agencies do not have *any* internal oversight or accountability mechanism to detect misuse. Neither federal, state, nor most local governments subject police policies concerning facial recognition to legislative or public review. 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. It's become a normal part of 21st-century living, and most Americans have no trouble accepting 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, the technologies of *artificial* intelligence do not deserve to be called tools. They are instead blunt instruments. And in the worst cases, blunt instruments become weapons.