August 26, 2021

National Institute of Standards & Technology
100 Bureau Drive
Gaithersburg, MD 20899
ai-bias@list.nist.gov
via Email

Re: Comment of 20 Civil Rights and Community-Based Organizations In Response To First Public Draft of NIST SP 1270 "A Proposal for Identifying and Managing Bias in Artificial Intelligence"

We, the undersigned civil rights and community-based organizations, write to express our serious concerns with NIST's draft proposal for identifying and managing bias in Artificial Intelligence ("AI"). Contrary to NIST's proposal, mere technical safeguards in development and deployment of AI are incapable of fully mitigating the technology's risk of bias. NIST's suggestion – focus on fixing the algorithm – is unhelpful and dangerously idealistic.

We raise concerns regarding the proposal's focus on narrow technical definitions of bias. Technical drivers of AI bias, such as design failure and poor training data selection, only account for a small fraction of the harms these systems create. While the report includes a long list of biases in its appendix and acknowledges external influences and contextual issues, the framework does not solve for the systemic and institutional biases and dynamics of power that compound the technical bias of AI systems. Additionally, such a framework ignores how probabilistic risk scores deprive individuals of the opportunity to be evaluated on their own merits and the tremendous power of law enforcement.

This risk is most acute for law enforcement AI, including forecasting and surveillance tools. Even on the rare occasions when such AI systems are technically unbiased, their broader community impact is deeply distorted by the over deployment of such systems in low-income and BIPOC communities. Such inequity is further compounded by officer discretion in how to respond to system outputs, as well as the endemic discrimination that impacts every decision point for those who are arrested as a result. Even worse, the constant stream of revelations about police bias are a reminder that no AI system can remain unbiased in the hands of a biased user.

NIST fails to account for how AI systems are routinely *misused* by public and private sector entities. For example, in many cities that use facial recognition, officers routinely edit images prior to running a search. Such alterations add multiple layers of bias that would never be identified during NIST's pre-design, design, and deployment review. Using "unbiased" algorithms only addresses a minute aspect of AI Bias.

Even if every technical driver of bias in such facial recognition software is addressed, doing so does not address the bias in the decision-making process that determines when to use the algorithm, how to interpret its results, and its broader social impact.

Turning to NIST's evaluation of data set integrity, the proposal is once again far too narrow. In many of the most sensitive areas of AI deployment, the underlying data can never be effectively

sampled because the data itself is the distorted product of biased human decision making. A powerful example of this is crime rate data, which is frequently incorporated into predictive AI systems.

If we simply focus on the algorithm, as NIST suggests, we see sampling bias: overpoliced communities are overrepresented in algorithms' training data, and disproportionately targeted by algorithms. The technical solution to sampling bias is to seek out a more balanced training dataset. But the truth is that there simply is no unbiased dataset for policing in America, and sampling techniques will only automate the human-made inequality that has defined policing in America since its inception.

NIST's laboratory evaluations of AI efficacy are often received by the public without the understanding that the reliability of such systems was demonstrated under testing conditions and not real-world conditions. In fact, there is no available data on how AI systems perform in the hands of law enforcement users in real life settings. Contrary to the proposal, "deployment monitoring and auditing" is woefully inadequate to address such a performance gap. This is particularly true as there are few standards on how users can deploy such technologies, leading to near-infinite permutations of AI deployment that would need to be compared to lab benchmarks. This type of data needs to be evaluated before the technology is tested on vulnerable communities when its results can impact life and liberty.

Lastly, NIST fails to answer the most important question of all: Should we build this technology in the first place? This is a threshold inquiry that must be satisfied in the pre-design phase before moving on to questions about how to measure and optimize such technology. The report does not give sufficient weight to the importance of the pre-design phase and should more forcefully emphasize the need to stop development of harmful technologies or technologies whose just and equitable use cannot be assured at that phase.

In other areas of scientific development, we've long recognized that some advances simply come at too high a price. Consider the breakthroughs we could have made in chemical and biological warfare over the past 50 years if permitted. Such agents would be potent weapons in our military arsenal, but they would pose an intolerable risk to all of humanity. Many of the AI systems under development today also impose an intolerable cost, and not merely in the "wrong hands," but in any hands.

Technical fixes remain important, but for the foregoing reasons, they are insufficient for assuring the just and equitable development of AI technologies in this proposal.

Signed,

ACCESS of WNY
American University SOC
Arab American Association of New York
Aspiration
Citizens Privacy Coalition of Santa Clara County
Council on American-Islamic Relations, New York (CAIR-NY)
Defending Rights & Dissent
Electronic Privacy Information Center (EPIC)
Emonyo Yefwe International

Ethics In Technology
European Center for Not-for-Profit Law
Fight for the Future
Hamai Consulting
Occupy Bergen County (New Jersey)
Privacy Watch STL
Restore The Fourth
RootsAction.org
S.T.O.P. – Surveillance Technology Oversight Project
The Legal Aid Society of NYC
X-Lab