SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (646) 602-5600

COMMENT OF THE
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

TO THE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

IN RESPONSE TO
REQUEST FOR INFORMATION DOCKET No. [210726-0151]: "ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK"

SUBMITTED
SEPTEMBER 15TH, 2021

We thank NIST for inviting comments relating to the NIST Artificial Intelligence Risk Management Framework (Docket Number [210726-0151]). Our comments will align with select specific requests for information from the Request for Information (RFI).

NIST asks respondents to identify the greatest challenges in managing the AI-related risks stemming from novel tool development. Unfortunately, this is a dangerous starting place, since it bypasses the single most important threshold question in AI development: should an AI tool be built at all. NIST overestimates the degree to which tools' harms can be anticipated, particularly in policing and other fields with acute, asymmetrical error costs. The stakes could not be higher, or the potential consequences grimmer; AI has put at risk individuals' freedom from wrongful imprisonment, safety, privacy, and freedom of association, among other fundamental rights. Facial recognition has already misidentified Black men who are then wrongfully arrested;[1] once in the criminal justice system, the potential for injustice at the hands of AI increases, as arrested individuals can be subject to algorithms which mete out recommendations for pretrial release, bail, and prison sentences.[2]

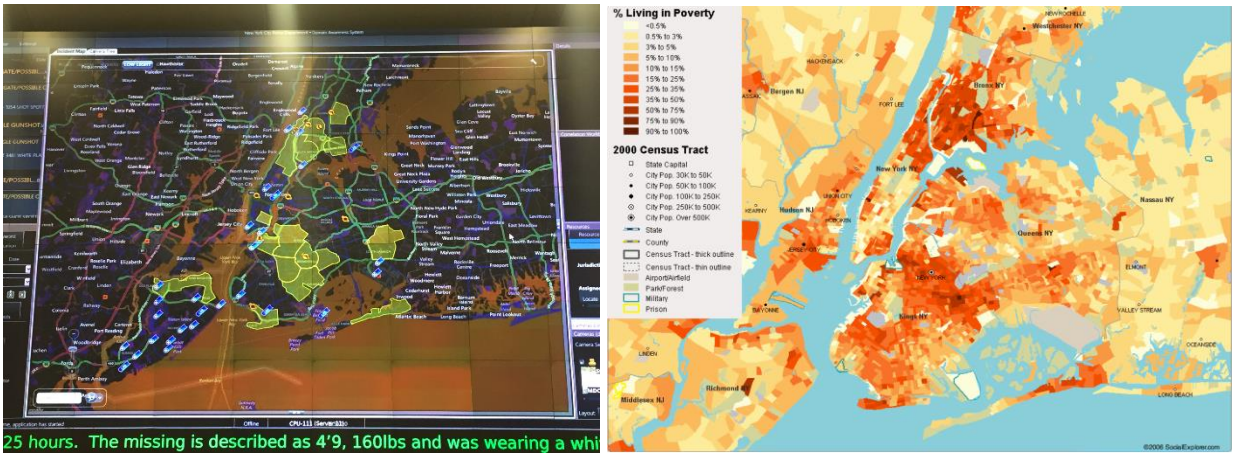
Furthermore, the Framework's aim of developing approaches to mitigating bias must include the fundamental question of to what extent it is possible to entirely debias AI tools. NIST must employ greater humility in approaching this and other, similar questions; the reality is that algorithms trained on police administrative data faithfully reflect historical patterns of police abuse and bias, because this abuse and bias is still very much 'baked in' to policing.[3] Thus, any data that would train the algorithms will simply reflect the bias that the algorithms are intended to be limiting, and, quickly, the algorithms will too. NIST must not allow this attempted "debiasing" to be so ineffective, even as it creates a shield for developers and the companies they work for from liability for bias, rather than as a tool likely to curb biased policing.

Finally, the RFI asks for "AI risk management…principles and practice which NIST should consider to ensure that the AI RMF aligns with and supports other efforts." NIST must include in its framework a question of how the intended use aligned with the actual use of the AI, and the ramifications of this difference. The gravity of police technology abuses demands closer analysis and tracking of such differences. As an example, a brief description of the use of ShotSpotter and the effect of biased placement. ShotSpotter is used in several cities to identify and locate

---

[1] Rashida Richardson, Jason Schultz, and Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," *N.Y.U. Law Review Online* 94, no. 192 (February 13, 2019), https://papers.ssrn.com/abstract=3333423.
[2] Julia Angwin et al., "Machine Bias," ProPublica, May 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing?token=m1ze0Mrj6m52j-J8AvluRGJmCGvDt8BG.
[3] Ashley Southall and Michael Gold, "Why 'Stop-and-Frisk' Inflamed Black and Hispanic Neighborhoods," *The New York Times*, November 17, 2019, sec. New York, https://www.nytimes.com/2019/11/17/nyregion/bloomberg-stop-and-frisk-new-york.html; Joseph Goldstein, "Judge Rejects New York's Stop-and-Frisk Policy," *The New York Times*, August 12, 2013, sec. New York, https://www.nytimes.com/2013/08/13/nyregion/stop-and-frisk-practice-violated-rights-judge-rules.html; Jake Offenhartz, "Lawsuits Against NYPD Cost Taxpayers $230 Million Last Year," Gothamist, April 17, 2019, https://gothamist.com.

gunshots through audio surveillance that is then fed through algorithmic software. First, consider the fact that this software is simply wrong, often: one study found as much as 89% of sounds identified as gunshots by ShotSpotter were actually other noise.[4] This is obviously a problem – but more so when one looks at how ShotSpotter is deployed in cities. A prime example is New York City, where ShotSpotter is deployed invariably in parts of the City where low-income New Yorkers of color live. Below, we juxtapose a photo of NYPD's ShotSpotter deployments (left) with a map of NYC's low-income neighborhoods (red areas on right).



ShotSpotter deployments in 2018. Photo credit: Clare Garvey. Map of Poverty in NYC. Credit: Visualizing Economics.

ShotSpotter is thus incorrectly identifying gunfire and then alerting police, deploying officers on high alert to locations where low-income, BIPOC New Yorkers live. This is an ominous threat that hangs over these communities, and lest you think the worst has not yet happened, think again. In March 2021, Chicago police shot and killed 13-year-old Adam Toledo after being alerted by ShotSpotter to gunfire in the neighborhood. Adam Toledo has already demonstrated the tragedy of the gap between actual and intended use of AI. NIST must acknowledge it or risk more fatalities.

NIST's work on this Risk Management Framework must be informed by the reality of our age; AI is already in use, and there are lessons to be learned from the tragedies and abuses that have already unfolded. AI poses unique risks when in the policing arena that must be acknowledged. To truly address these, NIST must shift away from the technical fixes it seems to favor to forcing the AI actors themselves to reckon with the human behavior that informs the decisions made about AI in the first place.

[4] "End Police Surveillance," Roderick & Solange MacArthur Justice Center, 2021, https://endpolicesurveillance.com/.