Reply Delete Junk Block ···

RFI: Developing a Federal AI Standards Engagement Plan

JK

Joshua Kroll <jkroll@jkroll.com>
Mon 6/10/2019 5:17 PM
ai_standards

NIST_RFI_AI_Standards-Kroll-...
111 KB

To Whom It May Concern:

I wish to submit the attached article, "Data Science Data Governance" for the NIST RFI on Artificial Intelligence Standards (Docket Number: 190312229-9229-01). While it was published in IEEE Security and Privacy, I hold an independent copyright and so can submit it for public posting here. The article, which describes high level approaches to data governance and software system governance I've encountered during my research on the governance of software systems, speaks most closely to question (8) on "Technical standards and guidance that are needed to establish and advance trustworthy aspects (e.g., accuracy, transparency, security, privacy, and robustness) of AI technologies."

I would, in addition, raise that the creation of standards for Artificial Intelligence itself is unlikely to be a useful activity. AI is such a broad suite of technologies, applied in such a range of applications, that claims of standardization can only be vacuous. Attention should instead be paid to functional requirements for particular application areas. NIST's own evaluation programs in facial recognition and information retrieval have been immensely valuable to those areas, and similar programs for evaluation of functional capabilities in other domains (e.g., object recognition, vehicle control) have the potential to be at least equally as influential.

Rather than standardizing performance, I would argue for NIST to develop a functional assessment framework which allows developers to structure their own evaluations of their requirements and designs, as well as the performance of the systems they are building. Such a risk-oriented (rather than outcomes-oriented) approach would improve the breadth of applicability of any standards pursued. Further, it is an area where NIST already has significant capacity and experience by way of the existing "Framework for Improving Critical Infrastructure Cybersecurity".

I would be eager to engage with this process as it continues and develops. If desired, you may extract the paragraphs of this e-mail into a separate submission or include this e-mail in its entirety as a preamble to the attached submission.

Best regards,
Joshua A. Kroll, PhD
Postdoctoral Scholar, UC Berkeley School of Information