Reply Delete Junk Block ···

NIST Request for Comment: Plan for Federal Engagement in Development Technical Standards and Related Tools for AI

MP MOLARET Philippe <Philippe.MOLARET@ca.thalesgroup.com>
Fri 7/19/2019 2:12 PM
ai_standards; YARIN Paul <paul.yarin.e@thalesdigital.io>

Line 56 (also linked to comment on line 338 below):

- In order to qualify further AI and Trustworthiness and in an effort to gage the efforts and focus in establishing a standard, tools and possibly practices, the notion of critical decision supported by an AI agent should be introduced. Non critical AI based decisions like the selection of a restaurant or a movie on Netflix do not need to be supported by an AI design and development standard, hence no need to impede this type industry sector and their business. On the other hand conveying thrust to a radiologist that the AI agent allowing for pathology detection has been designed, developed and tested in accordance to a standard that provides robustness, reliability and explainability such that he feels confident interfacing with the patient about the AI generated return is part of critical decision he will have to make. And that applies to many industrial sectors where AI agent based recommendations in legal, financial, safety critical machinery operators (and this is not an exhaustive list), will apply subject to a critical decision.

Line 107:

- Another consideration to the timing and pertinence of a standard for AI. I would not make a too close relationship in standard approach to SDOs in the IT world for 1) AI belongs more to the digital world than the software world, and giving the AI standard a SW look alike standard approach would just miss the specific needs of AI in the digital domain and 2) IT would welcome to consider AI as another activity in their domain and yet AI, does use IT but it is much more than that, very often the AI solution exists only through its application to a specific domain problem, hence it needs strong domain knowledge to provide industry solutions.
- AI systems are high-level "systems-of-systems" that are intended to replace or augment human thought; this is not the case for IT elements like hard drives or encryption protocols. AI standards must reflect system integrity and reliability, but they should also reflect the consequences of the AI system's decisions.
- But it is true that because of its multi domain application the AI standard would have to be horizontal but able to cater to verticals.

Line 173:

- I believe AI needs to contribute to the cyber security concerns in two ways, 1) being cyber safe by design and 2) applying AI to cyber security solutions. Not sure if this fits in either table 1 or 2, but I though it important to mention here. Cyber is as much a technology that needs to benefit from all technology innovations and also it is becoming a matter of policy that nations are starting to inforce.

Line 184:

- Another aspect of data standard and data set that will support all other claims in that section, is the need to have 'Gold standard' data sets that will support the need to qualify, 'certify' a given AI solution against the applicable AI standard. Different gold standard data sets would be required because the levels of qualification would be different for each domain of application, clinical medical practice, health management for outdoor patients, pharma, transportation, etc. Setting these gold standard data sets will require substantial research work which should include bias agnosticism.