June 10, 2019

Elham Tabassi
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8900
Gaithersburg, MD 20899

Re: Symantec Response to Request for Information on "Artificial Intelligence Standards"

Symantec Corporation appreciates the opportunity to provide this input, which was prepared with the assistance of our Office of the CTO (OCTO), Center for Advanced Machine Learning (CAML), and Symantec Research Labs (SRL). We have provided responses to questions 1-8 and focused on (1) those aspects of AI related to Security and Privacy – both on how AI can contribute to Security and Privacy and how Security and Privacy are required by AI; and (2) technical standards only.

As background, Symantec participates in the Organization for the Advancement of Structured Information Standards (OASIS) in leadership and board of director positions, the International Telecommunications Union (ITU) ITU-T in several leadership positions as well as within SG17 (Security), ITU-D, and the IETF. For the purposes of these comments, we are including machine learning, deep learning and other related technologies under the general umbrella of "AI".

RFI Questions 1-9:

1. **AI technical standards and tools that have been developed, and the developing organization, including the aspects of AI these standards and tools address, and whether they address sector-specific needs or are cross-sector in nature;**

While a number of SDOs do develop AI technical standards (see answer to question 4), we are not aware of any AI technical standards that have been developed specific to cybersecurity and privacy. However, some standards were set on constituencies in relationships with AI, like the ITU's X.1147, but concentrate on analytics and/or big data.

2. **Reliable sources of information about the availability and use of AI technical standards and tools;**

We are not aware of any authoritative reliable source of information about the availability and use of AI technical standards and tools on security and privacy aspects at this stage.

3. **The needs for AI technical standards and related tools. How those needs should be determined, and challenges in identifying and developing those standards and tools;**

There is a need for AI technical standards and related tools. In the context of security and privacy, there are two strategic aspects – *responsibility and interpretability*. *Responsibility* is rooted in four primary societal concerns: fairness, bias, ethics and privacy. Currently, standardization and regulatory efforts are focused on measuring the direct effects of the availability and use of AI on individuals, other entities and communities in this context. "Responsibility" requires consideration of other important (and often indirect) effects that remain generally unaddressed:

- the control of data selection for AI development, and its impact on decision bias and uncertainty;

- the disclosure of data and algorithmic details of an AI system in an effort to inform users of potential responsibility impacts;
- the assessment of the sensitivity of AI decisions to unanticipated inputs; and
- the provenance and custody AI systems for accountable ownership.

Interpretability is less clearly defined, but broadly speaking it is about understanding the risk, sensitivity and transparency associated with using an AI system. Put differently, it requires examining "what can go wrong", *e.g.,* the "unknown unknown", to a degree that best practices, standards and regulations can evolve in response. The ITU Workshop on Artificial Intelligence, Machine Learning and Security (organized by ITU-T SG17) in Geneva did work in this area and developed of terminology and ontologies for the Information and Communication Technology (ICT) sector (and Over The Top provides) including:

- Levels of autonomy, analogous to the levels 1-5 for self-driving cars
- Levels of impact of decisions
- Levels of privacy preservation
- Taxonomy for the type of AI/ML employed
- Durability, versioning and/or persistence of a model
- Taxonomy of security use cases addressed by a solution
- For classifier systems: formats for training/testing and efficacy comparison
- Transparency evaluation guidelines (Data, Business/Management model, Technical framework)
- To encourage the development of research in Stakeholder representations, Knowledge vs Models, Transparency/Interpretability/Trustworthiness and the Human Being in this loop

4. AI technical standards and related tools that are being developed, and the developing organization, including the aspects of AI these standards and tools address, and whether they address sector-specific needs or are cross sector in nature;

There are a number of organizations developing AI technical standards and related tools. In particular ITU, ISO, ETSI, 3GPP and some nascent work in IETF. The Organization for Economic Co-operation and Development's (OECD) work should also be included in this study.

While the ISO/IEC JTC 1/SC42, OECD can be considered cross-sector in nature, and perhaps to some degree the IETF as well, the ITU, ETSI and 3GPP have a focus on what can be called the Digital Service Provider (DSP) ecosystem. This ecosystem includes the current ICT and OTT worlds as well as Enterprise customers that are becoming service providers through digitalization. For example, Oracle recently announced that it is entering the 5G market and car makers are considering doing the same to compensate the lack of coverage for connected cars in the countryside.

Below is AI standards activity by organization:

ISO: (ISO/IEC JTC 1/SC42) has a comprehensive work program as presented at the ITU workshop (see answer to question 3) whose overall structure is as follows:

- WG 1 Foundational standards
- WG 2 Big data
- WG 3 Trustworthiness
- WG 4 Use cases and applications
- JWG 1 JWG SC42 – SC 40 Governance implications of AI
- SG 1 Computational approaches and characteristics of artificial intelligence systems
- AHG Dissemination and outreach

OECD: released a global standard for AI: 42 Countries Agree to International Principles for Artificial Intelligence
ITU:
Focus Groups (non-normative but usually used as pre-standardization work)

- FG-AI4EE – Environmental Efficiency for Artificial Intelligence and other Emerging Technologies
- FG-AI4H – Artificial Intelligence for Health
- FG-ML5G – Machine Learning for Future Networks including 5G

Study Groups (normative) include but are not limited to:

- SG13 has a few work items on machine learning in its work program
- SG16 has a few work items under development in its work program but more importantly is the reason for FG-AI4H. Therefore, it is fair to expect that more AI technical standards will develop in SG16
- SG17 – Security – the Q2/17 question text now contains within scope the matter of AI technical work, while Q7 and Q8 have specific aspects of Big Data and Analytics pertaining to the topic. Also note that at this level there are existing recommendations that were approved, for example X.1147
- SG20 has various work items under development in its work program such as Y.Sup.-AI4IoT in Q5/20

ETSI: ICT focused, and is about to start an Industry Specification Group (ISG) on AI and will be discussed at its ETSI Security Week this June.
3GPP: SA3 focuses on the security aspects of 5G and the above-referenced workshop revealed the large amount of areas where 3GPP is, or may focus on in the future.
Other conferences and associations: USENIX, CCS, IEEE S&P, NEURIPS, AAAI, ACM and Partnership on AI.

Other efforts: and documents to consider such as

- EU Ethics guidelines for trustworthy AI
- Singapore AI Model framework
- UK Centre for Data Ethics and Innovation

5. **Any supporting roadmaps or similar documents about plans for developing AI technical standards and tools;**

We are not aware of any.

6. **Whether the need for AI technical standards and related tools is being met in a timely way by organizations; and**

Standards can take hold when certain conditions are met, such as:

- when a market exists; there is a potential for interoperability that is unmet;
- competition leads to too many conflicting or overlapping standards; and
- actors agree that there is a benefit to standardization.

Today, it is unclear if these conditions are met for technical standardization of AI, and premature standardization could be counter-productive. With that said, there are some areas that *could* be ripe for standardization, including:

- characterizing datasets and/or standard datasets
- interoperability of models and datasets

- “reproducible” model development (important for auditability)
- test and characterization of AI performance, perhaps via standard test datasets and protocols, which may be sector- or application- specific
- disclosure of AI system details, for example the datasets used for training, the class of algorithms implemented, whether the system adapts, etc.

7. **Whether sector-specific AI technical standards needs are being addressed by sector-specific organizations, or whether those who need AI standards will rely on cross sector standards which are intended to be useful across multiple sectors.**

We believe it most likely that there will be a blend of generic and specialized approaches.

8. **Technical standards and guidance that are needed to establish and advance trustworthy aspects (*e.g.,* accuracy, transparency, security, privacy, and robustness) of AI technologies.**

Trust in these areas is as much about accuracy as it is about transparency, interpretability and risk assessment. For example: how does one quantify the chain of trust for an AI tool? Such tools are built on dependencies, like algorithms, that rely on big data infrastructures and data sets, with training that was done on a certain infrastructure. If any dependency is compromised, how would one assess the ‘trustworthiness’ of the final AI tool? Without visibility into how the chain was built, trust is hard to come by. Put differently, trust will flow from transparency and interpretability.

Conclusion

We thank NIST for taking on this important issue, and we appreciate the opportunity to provide this input. We look forward to the upcoming workshops.

Sincerely,

Jeff E Greene

Jeff Greene
Vice President, Global Government Affairs
& Cybersecurity Policy
Symantec Corporation