14 Jun 2020

UNIVERSITY OF CAMBRIDGE
Department of Computer Science & Technology

Comment on §5Db "Keeping of records and data" requirements in
"On Artificial Intelligence – A European approach to excellence and trust" COM(2020) 65

The Compliant and Accountable Systems research group is based in the Dept. Computer Science & Technology, University of Cambridge. We comprise an interdisciplinary team exploring the interplays of law and emerging technology.

We are keen share our thoughts regarding the data and record keeping requirements, as outlined in the white paper.

1. We agree that record-keeping requirements are an important part of an AI regulatory framework. We were pleased to see these included in the discussion.

2. However, we consider the "keeping of data and records" requirements described in the white paper (§5Db) as *too narrowly focused on machine learning specifics*.

3. There is more to an AI system than just the 'AI' (model). A model doesn't operate by itself, but rather is deployed and operates as part of a wider socio-technical system. An AI system comprises various technical aspects (inputs, outputs, software/hardware components, the underlying technical platforms and infrastructures, training data and models), as well as organisational processes and workflows, the actions of individuals, and so forth.

4. The record-keeping requirements in the white paper are described as relating to "the programming of the algorithm, the data used to train high-risk AI systems, and, […] the data themselves". These are overly model (machine learning) centric, and do not sufficiently account for these broader aspects.

5. In our view, **a more effective record-keeping regime is one that explicitly recognises that models form only a part of an AI system**. Therefore any record-keeping requirements should take a more holistic approach, by accounting for the relevant socio-technical considerations, system-wide. This entails a documentary regime that encompasses a range of concerns, from technical details and system interactions, to organisational processes, workflows, human actions, and so forth.

6. We also consider the documentary aspects described in §5Db as *overly focused on system design.* We argue that **record-keeping requirements should also target the systems' run-time operation**; i.e. capturing information on how a system operates and behaves. This is crucial given AI systems are complex, where such information will help with investigating failures, facilitating on-going monitoring and oversight, and more (see 8).

7. The nature of the records themselves are important. Record-keeping requirements should strive towards supporting and facilitating *meaningful* systems oversight, audit and review. There will also be sensitivities regarding such records, and therefore regimes for appropriate record management also require consideration.

8. Generally, robust documentary and record-keeping requirements will result in capturing more complete and relevant information about the nature of a system. Such information works towards better oversight, investigation and review, and supports repair, rectification and recourse when failures inevitably occur. Such regimes may also drive higher-quality systems, as a result of the design and monitoring practices they encourage.

9. In closing, we seek to emphasise that record-keeping requirements that account for the broader aspects of systems will be crucial for the regulatory framework's long-term relevance. This is because systems are becoming increasingly complex and interconnected; i.e. a *system-of-systems*. These will exhibit emerging properties, meaning failures and harms will be inevitable, with some difficult to foresee.

We have published various papers on these cocerns. Two particularly relevant include:

- *Decision Provenance: Harnessing data flow for accountable systems* [https://arxiv.org/pdf/1804.05741.pdf]
- *Responsibility & Machine Learning: Part of a process* [https://ssrn.com/abstract=2860048]

Of course, we would be happy to further discuss any of the points raised. Moreover, our research covers a broad range of topics regarding the regulatory and governance aspects of emerging technology, including AI and the IoT. We would therefore be pleased to give input on other topics as well.

Best regards,

Dr Jat Singh
Compliant & Accountable Systems Research Group
Dept. Computer Science & Technology
University of Cambridge
jatinder.singh@cst.cam.ac.uk / www.compacctsys.net