IGF2019 BPF IoT, Big Data, AI
Feedback on draft report

Update Nov 25

---

1).The first diagram could include a circle for the human brain to show human to computer interaction that is now the space...with AI IoT and Data ...or hovering over the other 3 circles as a leadership driver

2) Provide a hierarchy of leadership responsibility for this space such as:

International Human Community
  Individual / Teams of Humans
    AI
      IoT
        Other technologies

3) Data quality is key for effective outputs and the need to rigorously safe guard quality, truthful ,information by excellence in timely data cleaning is critical.

4) Important to create a tree of human values for this space ...This allows developers to parse options for ethical standards to achieve the required human outcome when perhaps a single option or route requires clarification.

Amali De Silva-Mitchell

Here the general comments:

Structure: Not sure if this was done on purpose or accidentally, but I missed a chapter on 'Risks', ideally after Opportunities, and before Policy Challenges. On p. 12 the survey question asks about worries & concerns >>> = risks & threats. Policy challenges in my view are to balance opportunities & risks.

The **ethical & human rights perspective** is several times mentioned in the report, but never really elaborated upon. This would definitely need more depth & arguments in several sections. For example: From a point of autonomy and self-detemination the freedom to 'opt-out' of technological applications is key etc… Or: Putting the human and his/her dignity at the centre of attention, autonomous weapon systems that decide about life & death and only treat the targeted individual as a 'data point' are extremely problematic. And so on… happy to discuss in more detail.

Trust: Good point, but the argument is a bit twisted, i.e. in my view starts a bit at the wrong end. Trust has to be gained, i.e. trustworthy technologies have to be developed in a first step and trustworthy actors (corporations & government, etc.) need to be in charge of their use, i.e. somebody (who?) needs to be responsible & accountable that these tech will not be used against their proclaimed purpose (as could happen e.g. with IoT & surveillance). The problem: Neither corporations nor governments tend to be very trustworthy actors. IO's not sure. So the problem starts earlier. We need trustworthy tech and we need trustworthy actors who are responsible / accountable to meet that expectation. Both regarding the technical functioning and the purpose for which tech is used. Trust in tech will follow then. 'Producing' trust too early and without a solid base (trustworthy tech & accountability by trustworthy actors), could be very counterproductive – trust is easily lost and very difficult to regain.

Evelyne Tauchnitz