Summary of IGF 2019 Conference & Best Practice Forum (BPF) on IoT, Big Data and AI and inputs to be discussed at next year's IGF 2020

General comment: The focus of both the IGF 2019 conference and the BPF report were the opportunities presented by IoT, Big Data and AI. The risks of digital transformation got discussed with less depth, which created a bit of imbalance of opinions and arguments. In order to address new 'policy challenges' arising from digital change, we yet need to critically evaluate both opportunities & risks and try to find a sustainable balance between the two that benefits the societies of the future. Ignoring the risks, is not only a very risky undertaking, but also creates a vague uncertainty that is difficult to grasp and negatively affects the level of trust we have in IoT, Big Data and AI. In order to create trust in digital technologies and avoid superstitions & myths, we need to openly talk about the risks and negative consequences.

Policy Challenge 1: Enhancing justified trust in IoT, Big Data and AI

Apart from openly discussing risks and disadvantages of digital technologies in public and together with civil society, we need more transparency and accountability both in the development of new technologies and their application. Trust has to be gained, i.e. trustworthy technologies have to be developed in a first step and trustworthy actors need to be in charge of taken adequate decisions that regulate their use. Somebody needs to be responsible & accountable that these technologies will not be used against their proclaimed purpose (e.g. IoT & surveillance) and / or produce unexpected negative side effects. The problem: Neither corporations nor governments who concentrate most decision-making power, tend to be regarded as very trustworthy actors. International organizations might enjoy more legitimacy yet are often very bureaucratic and not close enough to the people and their problems.

In sum: We need trustworthy technology and we need trustworthy actors who are responsible / accountable to that expectation. Both regarding the technical functioning and the purpose for which tech is used and what side effects it may have. Trust in tech will follow then. 'Producing' trust too early and without a solid base (trustworthy tech & accountability by trustworthy actors), could turn out to be very counterproductive – trust is easily lost and very difficult to regain.

Policy Challenge 2: Simulating the uptake and use of IoT, Big Data, AI to achieve positive policy outcomes to address societal challenges

What are 'positive' policy outcomes?
The term of 'positive' policy outcomes, i.e. what is perceived as being a positive policy outcome, and by whom and for whom, would need more in-depth discussion. Repressive social and political surveillance might be rated as a positive policy outcome by a repressive regime, no matter if it is a formal democracy or dictatorship, as it allows to control potentially regime threating activities of its citizens in the name of enhanced security and political stability. For the concerned citizens, if we could ask them, this might not be a 'positive' policy outcome though, as they are deprived of their civil liberties and freedoms. Often, citizens do

not have the possibility to opt out, either. >>> What is a 'positive' policy outcome lies, same as beauty, in the eye of the beholder.

How can we distinguish between negative and positive policy outcomes produced or enabled by digital technology? Or rather: What criteria should we apply in order to evaluate policy outcomes created by IoT, Big Data and AI (e.g. based on a basic sense of justice, the values of freedom, self-determination, human dignity, etc. and the respect for fundamental human rights)? An informed discussion why and for what purpose we want to use digital technologies is absolutely vital for discussing which 'positive' policy outcomes we do want to stimulate, and which not. As far as possible, and in order to not duplicate efforts and create confusion, it would make sense to build on an already established framework, i.e. as a minimum, the respect for fundamental human rights. Any policy challenge that violates international human rights norms, including civil and political rights, cannot be termed 'positive.'

In the case of competing norms (e.g. human security vs. civil freedoms; autonomy and human dignity etc.) we need an informed public debate that is based on a solid ethical ground and 'practical wisdom' that takes into account the context of a particular case and likely consequences of decisions and actions or non-actions. Combining global ethical and human rights standards with applied 'practical wisdom' that takes into account geographical and social differences, promises most success in defining priorities and standards for the definition of priorities and effective regulation of new technologies.

What societal challenges do we want to focus on?
Again, in order to avoid duplication of efforts and keep things simple, it would make sense to focus on societal challenges that we are already agreed upon on an international level, such as the Sustainable Development Goals (SDGs). >>> What can IoT, Big Data, AI do to achieve the SDGs?

Ethics and Fundamental Human Rights: From a point of view of justice and self-determination, not only the equal access to new technologies should get discussed, but also the distribution of risks and costs. In general, new risks created by digital technologies should be taken more seriously – not only in view of increasing justified trust and uptake – but also with regards to taking precautionary measurements to avoid them. This could also include a full or partial ban on certain technologies or certain purposes for which technologies are used, similarly as already done for certain weapons (e.g. biological and chemical weapons) and certain purposes (e.g. using arms to kill civilians or combatants who are not participating in hostilities anymore, for more details see international humanitarian law). In analogy, not only a ban of autonomous weapon systems should get discussed; but also surveillance systems employed to control and repress citizens and their fundamental human rights, incl. civil and political freedoms of movement and expression. What is more, marginalized groups that do not benefit from new technological developments (e.g. women, poor, ethnic and religious minorities) and people living in repressive government regimes might not have the same possibilities to opt out of certain technological applications as we have, plus do not have the same legal possibilities in case of violation of their rights (no guaranteed and equal access to justice in case their rights get violated by certain technological applications used by repressive government regimes or private corporations). >>> IoT, Big Data and AI can, and are often used for violent or repressive purposes >>> what can, and should we do to avoid this? How can we assure that the risks (e.g. tech used for political and social control, manipulation and

repression) and costs (e.g. loss of jobs) of new technologies are fairly shared among countries, regions and peoples?

In sum: The ethical & human rights perspective would definitely need to be strengthened with professional and academic expertise that would allow the in-dept exploration of arguments in favour or against a certain policy decision. For example: "From a point of autonomy and self-determination the freedom to 'opt-out' of technological applications is key etc…" or "Putting the human and his/her dignity at the centre of reflection, autonomous weapon systems that decide about life & death and only treat the targeted individual as a 'data point' are extremely problematic." Or: "From a point of justice, not only benefits need to be distributed fairly, but also possible risks arising from IoT, Big Data and AI." And so on…

Policy Challenge 3: Collection and use of data

General observation: There seems to be raising policy awareness and agreement about the importance of privacy issues and ownership surrounding data collection and use. The 'right to be forgotten', i.e. have one's data deleted or be able to do so autonomously, deserves more attention. How to avoid the intentional manipulation of data for political reasons, remains a challenge. Decentral data storage and/or individual control & ownership deserve further discussion.

Avoiding Biases & discrimination

Gaps in data sources that result in biased algorithms do not only produce the base for future discrimination of women, youth, elderly people, and the marginalized and poor in general, but in addition exhibit a strong path-dependency that favours the status-quo. Algorithms trained on data from the past possess a bias towards the past – i.e. the future is continued following the patterns and paths from the past. This leads to a two-folded problem: Firstly, power relationships are translated from the past to the present, which is partly expressed in discrimination, but goes beyond as it also makes certain assumptions on how things ought to be done. This can go as far as reproducing 'appropriate' hierarchies, authorities and communication styles between doctors, nurses and patients in the health sector for robots who are supposed to take care of patients in an 'appropriate' way and following an 'appropriate' process. Another example is AI based financial investment decisions based on profit making without taking into account systemic power imbalances between producers, traders and investors. In spite of all the digital change and its opportunities, this exhibits the danger of not allowing for social or political change. Secondly, and depending on the degree of decision-making power that is delegated to AI, there is the risk that we lock ourselves up in patterns of the past. Dynamic societies need creativity and empathy to evolve; AI that bases its decisions on past decisions, actions and outcomes makes it difficult to overcome patterns of the past that may not serve the future anymore. In an extreme case, this may even lead AI to propose or take 'bad', inappropriate or even dangerous decisions - taking into account that the context in which present and future decisions are embedded is not the same anymore as in the past. With digital change, interests, preferences and human needs and behaviours can be expected to change even more quickly. Decisions based on data from the past might not be very helpful anymore.

General comment / input for future IGF conferences:

The political and governance perspective (IGF = Internet **Governance** Forum!) is an important one and needs to be reflected upon with care. Who do we want to give the power to take present and future decisions concerning the internet, big data use and AI (e.g. private corporations, international organizations, governments, elected representatives of the people, end 'users')? When talking about decision-making power, this not only includes who takes the final decisions regarding the future development of the internet, but also who has to power to put the topics on the agenda to be discussed (= agenda setting power) and the power to influence political discourses and debates that may eventually lead to policy decisions. Related to this, is also the question of what has so far not been on the political agenda and only got discussed on the margin (and why), such as for example sharing the risks of tech, which includes the possibility that tech is used for surveillance and repression by authoritarian governments and private corporations, path-dependencies of AI based on data of the past that favour the consolidation of problematic power relationships and systems into the future, the imposition of a full or partial ban on certain technologies and/or purposes.

In sum: what tech do we want? What tech do we not want? And how does the current international system with all its shortcomings, which includes the maximization of financial profit making by private corporations, underrepresentation of the poor and marginalized groups, political instability and repressive government regimes, to just name a few problems, impact on the type of technologies we develop and for what purposes we use them (e.g. autonomous weapon systems for war, surveillance for repression, analysis of private data for manipulation of political and consumer choices and behaviour etc.)? In addition, there is the basic question of how policy output in terms of political decisions would differ if all the people who are currently not included in agenda setting and decision-making processes, were included and/or if we would care to listen more carefully.

Already existing power structures need to be taken into account if we want to avoid that the already powerful use new technologies linked to the internet to become even more powerful, be it in the political, social or economic sphere. IoT, Big Data and AI are powerful tools that act as 'magnifiers' both of our good and bad intentions and actions. They can either become tools of exploitation and repression by a small political and economic elite, or tools of empowerment and freedom for those who are most in need. The choice really is ours, but the question who makes this choice and for whom is not self-evident. This governance aspects relating to who decides about the future of the internet, deserves more attention in general, and in specific with regards to a critical reflection of our values and assumptions on which we base our arguments in favour or against a particular policy option and decision-making process.