IGF 2019

Best Practice Forum on

Internet of Things
Big Data
Artificial Intelligence

"Best Practices (for policy and business) to enhance justified trust in IoT, Big Data, AI applications and to stimulate their use to address societal challenges that otherwise would be more difficult to address."

Final BPF Output Report

- January 2020 -

Acknowledgements

The *Best Practice Forum on Internet of Things, Big Data, Artificial Intelligence (BPF IoT, Big Data, AI)* is an open multistakeholder group conducted as an intersessional activity of the *Internet Governance Forum (IGF)*. This report is the output of the IGF2019 BPF IoT, Big Data, AI and is the product of the collaborative work of many.

Facilitators of the BPF IoT, Big Data, AI:

Ms. Concettina CASSA, MAG BPF Co-coordinator
Mr. Alex Comninos, BPF Co-coordinator
Mr. Michael Nelson, BPF Co-coordinator
Mr. Wim Degezelle, BPF Consultant

The BPF document was developed through open discussions on the BPF mailing list and virtual meetings. We would like to acknowledge participants to these discussions for their input.
The BPF would also like to thank all who submitted input through the BPF's Call for contributions.
More on the BPF process on the 2019 BPF IoT, Big Data, AI webpage.

The BPF would like to thank the panelists and participants to the BPF IoT, Big Data, AI workshop at IGF2019 in Berlin. Their discussion provided additional input for this report. Workshop panelists: Christine Tan (FIOT Open Lab), Olivier Bringer (European Commission), David Salomão (INCM), Raymond Onuoha (Research ICT Africa), Bruna Martins dos Santos (CodingRights), Emanuela Girardi (Pop AI), Evelyne Tauchnitz (Centre for Technology and Global Affairs, University of Oxford), Marco Zennaro (workshop Rapporteur).
Workshop online moderator: June Parris; Workshop Rapporteur: Marco Zennaro (report)
A recording of this meeting is available online.

Report editor: Wim Degezelle

IGF 2019
Best Practice Forum
Internet of Things, Big Data, Artificial Intelligence

Table of Contents

Executive Summary

Introduction

The IGF *Best Practice Forums (BPFs)* provide a platform for experts and stakeholders to exchange and discuss best practices in addressing Internet policy issues in a collaborative, bottom-up manner. BPFs prepare their work in a series of intersessional discussions that culminate in a workshop at the annual meeting of the *Internet Governance Forum (IGF).* BPFs intend to contribute to an understanding of global good practice, inform policy discussions, standards development, business decisions, as well as public understanding, awareness, and discourse.

The *BPF on Internet of Things (IoT), Big Data and Artificial Intelligence (AI)* focusses on where these technologies meet in an internet context, and how Internet governance can stimulate their development and widespread use, as well as help to avoid unintended negative side-effects.

Building on the IGF2018 BPF IoT, Big Data, AI

The IGF2019 BPF IoT, Big Data, AI can build on the work done in 2018. The IGF2018 BPF IoT, Big Data, AI compiled a set of best practices to facilitate the stakeholder dialogue on issues pertaining to the application of the new technologies in an internet context.

IoT, Big Data, AI to address societal challenges - endless opportunities

IoT, Big Data, AI have an enormous potential and already play an increasing role in addressing societal challenges. The new technologies may improve existing solutions, make them more efficient, or make it possible to approach issues in a totally new and more effective way. IoT, Big Data, AI applications can also empower people who today, for a variety of reasons, may have limited possibilities to act or influence. The examples showcased in the BPF report are only a snapshot of an endless and growing range of opportunities and applications.

In almost every facet of today's world, there are examples of how the new technologies are or can be used. IoT, Big Data, AI applications can be enablers to make progress in different, in almost all, SDG areas. Using IoT, Big Data, AI can improve cybersecurity, e.g. by making use of records of previous data attacks to recognise suspicious activity faster. IoT, Big Data, AI applications can empower internet users to manage their own lives the way they want them. Other examples are the use of IoT, Big Data, AI for civil protection, smart cities, health, etc.

IoT, Big Data, AI to address societal challenges - policy challenges

From policy and decision makers is expected that they face current and future challenges. They should guide us by dealing with a series of pertinent policy questions and providing future proof answers that address today's concerns but remain relevant for applications of the IoT, Big Data, AI that are yet to be discovered.

The BPF identified identified three clusters of policy challenges: **trust** in the technologies and applications, their **use and uptake** and concerns related to the collection, management and use of **data**.

- Policy Challenge 1 - Enhancing justified trust in IoT, Big Data, AI, to stimulate their use to address societal challenges that otherwise would be difficult to address.
- Policy Challenge 2 - Stimulating the uptake and use of IoT, Big Data, AI applications to achieve positive policy outcomes to address societal challenges.
- Policy Challenge 3 - The collection and use of data generated, collected and analysed by IoT, Big Data, AI applications.

In its discussions the BPF further refined the three broad policy challenges to come to a better understanding of what positive actions are needed and what concerns need to be addressed, and collected examples of best practices and relevant initiatives.

Enhancing justified trust in IoT, Big Data, AI

Trust in Iot, Big Data, AI is important for the development and uptake of new and improved solutions that are based on applications of these technologies to address societal challenges. This trust, however, is a multi-layered concept, and establishing the right balance between the different dimensions can upto a certain degree be influenced by policy choices. The BPF called this balance: *"correct (and justified) trust" : that is, neither too little trust (preventing benefits from being realised) nor too much trust (exposing unsuspecting users to undesired risk).*

The policy challenge 'enhancing trust in IoT, Big Data, AI can be formulated as follows:

1. Be aware of the importance of trust and of its multi-layered character,
2. Understand the balances and trade-offs between different layers,
3. Based on 1 & 2 make policy choices and take initiatives to enhance trust.

Stimulating the use and uptake of IoT, Big Data, AI

IoT, Big Data, AI and their applications have a huge potential when it comes to contributing to solving day to day societal challenges. Policy and decision makers therefore need to reflect on what actions and initiatives can be taken to support the new technologies, but also, what concerns need to be addressed. The BPF identified the following:

1. Stimulating the development of IoT, Big Data, AI applications;
2. Stimulating the use and uptake of IoT, Big Data, AI applications;

Concerns:

3. Algorithms may possess a bias towards the past;
4. Algorithms may reinforce views and biases of the developers;
5. Unequal access to the benefits of IoT, Big Data, AI;
6. Distribution of risks;
7. Ethics and Fundamental Rights.

Collection and use of data, generated, collected and analysed by IoT, Big Data, AI applications

The increase of computing power makes that unseen quantities of data can be analysed in ever shorter time and at lower cost. The growth of the internet, the polarity of social platforms, and the roll-out of the IoT make that enormous quantities of data are generated. This data, often combined data from different sources, are analysed using AI technologies to gain insight, draft conclusions and take decisions. One step further, systems based on AI technology are fed with large amounts date to train them in machine learning and automated decision making.
There's a wide range of policy issues and concerns directly linked to the collection, management, and use of data in an IoT, Big Data, AI context. The BPF identified following:

1. Data quality;
2. Impact of legislation on data quality and accuracy;
3. Respecting privacy;
4. Data ownership;
5. Data availability and digital data divides;
6. Data sharing and the free flow of data.

Links and resources

IGF2019 BPF IoT, Big Data, AI
Webpage

IGF2019 BPF IoT, Big Data, AI workshop
Agenda and report
Recording

IGF2019 BPF IoT, Big Data, AI Survey
Compilation survey feedback

I. Introduction

1. Best Practice Forums at the Internet Governance Forum (IGF)

The *Internet Governance Forum (IGF)* is a global forum where governments, civil society, the technical community, academia, the private sector, and independent experts discuss Internet governance and policy issues.[1] The annual IGF meeting is organized by a Multistakeholder Advisory Group (MAG) under the auspices of the United Nations Department of Economic and Social Affairs (UN DESA). The 14th annual IGF meeting took place in Berlin, Germany, from 25 to 29 November 2019.

The IGF *Best Practice Forums (BPFs)* provide a platform for experts and stakeholders to exchange and discuss best practices in addressing Internet policy issues in a collaborative, bottom-up manner. BPFs prepare their work in a series of intersessional discussions that culminate in a workshop at the IGF's annual meeting and a BPF output document. BPFs intend to contribute to an understanding of global good practice, inform policy discussions, standards development, business decisions, as well as public understanding, awareness, and discourse.

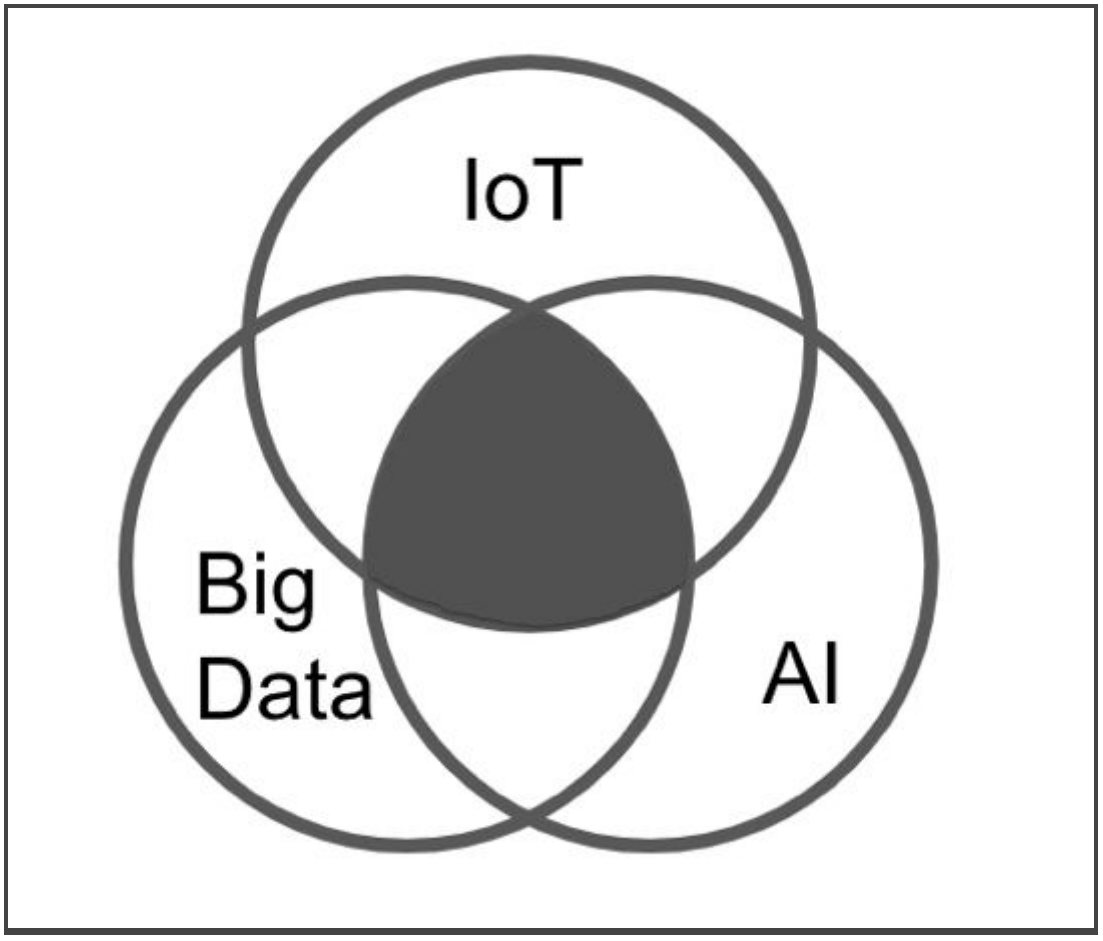
2. Scope of the BPF IoT, Big Data, AI

Internet of Things (IoT), Big Data, and Artificial Intelligence (AI) discussions are present in many fields, both in the on- and offline world. The *BPF on Internet of Things (IoT), Big Data and Artificial Intelligence (AI)* focusses on where these technologies meet in an internet context, and how Internet governance can stimulate their development and widespread use, as well as help to avoid unintended negative side-effects.

Each of the three technologies are being used in many different ways in many different fields. The focus of the BPF is on where all three technologies are being used in concert, for example where the Internet is used to collect data (e.g. generated by IoT devices or social platforms) which is then analysed with the use of artificial intelligence and machine learning technologies. In other words, rather than trying to cover all the issues that can be situated in any of the areas in the entire Venn Diagram below, we will focus on the overlap in the middle. In this, we are aware that the overlap will grow, and the edges (where IoT is not relating to big data, or does not become part of AI applications) are blurry, at best. Sometimes a link with the Internet is obvious, sometimes less clear and diffuse. Therefore the BPF is not too strict on what is within and what is not within its scope, as the concerns, expertise and best practices pertaining to the use of IoT, Big Data or AI separately remain relevant when the three technologies are used in

[1] IGF website: http://www.intgovforum.org - the IGF is one of the key outcomes of the World Summit for the Information Society (WSIS).

concert in an internet context. For example, learned best practices for the 'offline' application of AI and machine learning remain relevant when AI is applied in a similar way to analyse large amounts of data generated in real time on the internet.



Focus of the BPF: where IoT, Big Data, AI are being used in concert.

3. Objectives of the IGF2019 BPF IoT, Big Data, AI

An opportunity to bring stakeholder experience to the policy debate

The BPF document is intended to inform policy discussions. It describes different issues and reflects on ongoing discussions, and is tailored to be useful for an audience of policy makers, including those who do not deal with technology on a day-to-day basis. The output generated by a BPF is the result of an open processes and thrives on bottom-up input and experiences sharing by different stakeholders.

In his statement to IGF 2018 in Paris, UN Secretary-General Guterres called upon the IGF community to (i) extent from multistakeholder to multidisciplinary, (ii) create shared language and references, and (iii) include and amplify the weak and missing voices. The BPF takes these recommendations to heart.

Building on the IGF2018 BPF IoT, Big Data, AI

The IGF2019 BPF IoT, Big Data, AI can build on the work done in 2018. The IGF2018 BPF IoT, Big Data, AI compiled a set of best practices to facilitate the stakeholder dialogue on issues pertaining to the application of the new technologies in an internet context.

2018 BPF IoT, Big Data, AI

Facilitating stakeholder dialogue on issues pertaining to IoT, Big Data, AI in an Internet context.

Identified best practices

1. **Define terms narrowly** so that it is clear for policy makers and stakeholders what aspects of the technologies they are discussing. Not doing so can lead to sweeping generalisations or proposals that are meant to address a problem with a narrow technology or specific application that could have a range of unintended consequences. Worse, conflating different technologies and different applications will cause discussions to lose focus and is likely to create fear.
2. **Be ecumentical about technolgy (or "Strive to be technology-neutral")**, because technologies are changing so quickly and because potential problems with a specific application of a technology may or may not develop (or may be solved rapidly), it is dangerous and unproductive to try to write laws and regulations that cover one specific type of technology or one specific type of application. Best practices should focus on what an application DOES not on how the technology DOES IT.
3. **Collaborate** to ensure that these technologies are deployed in ways that protect user privacy and security, and network resiliency while fostering innovation. Stakeholders should communicate openly about the impact new technologies have on the public and existing networks and find ways to work together to develop future-looking policies.
4. **Consider ethics and human rights when applying IoT, Big Data, and AI** from the outset in the development, deployment and use phases of the life cycle.
5. **Watch out for bias and incomplete data sets** that may reflect only a small subset of the "real world" due to the Digital Divide, due to national regulations that restrict the export of consumer data, due to marketing decisions to only focus on certain geographies, demographics, or industry sectors. In some cases, statistical techniques can weight data to compensate for some problems. But in ALL cases, the limits of the data and Big Data analysis should be recognized.
6. **Make privacy and transparency a policy goal and a business practice.** Potential problems must be recognized before they become serious. Transparency is one of the most effective ways to nurture trust, and can for example be achieved by the publication of transparency reports and such reports are likely to become more common and more detailed as the IoT enables data collection about more intimate aspects of our lives.
7. **Ensure that systems are adequately secured before they get to the market.** A balance will need to be found to distinguish "flaws resulting from irresponsible behavior" to flaws that could not be foreseen at the time, whereas system development has followed good practice - industry self-regulation may be the best way forward as to avoid regulation that is stalling innovation.
8. **Foster technologies and business practices that empower SMEs.** The growth of edge computing and "serverless computing" promises to give SMEs much cheaper and simpler ways to create the software needed to exploit the power of the data generated by the Internet of Things. The best response to the threat of "Data Dominance" is not regulating monopolies, it is ensuring their are not monopolies by ensuring vibrant competition.

IGF2019 IoT, Big Data, AI to address societal challenges

Building on the work done in 2018 the BPF in 2019 decided to focus on the potential of the new technologies to contribute to addressing societal challenges. Starting from the MAG agreed proposal[2], the BPF developed the following overarching narrative for the 2019 work and report:

> Overarching narrative BPF2019 IoT, Big Data, AI
>
> *"Best Practices (for policy and business) to enhance justified trust in IoT, Big Data, AI applications and to stimulate their use to address societal challenges that otherwise would be more difficult to address."*

The policy questions pertaining to the use of IoT, Big Data, AI applications to address societal challenges identified in the BPF report have been clustered under three main themes:

(1) **Trust** in IoT, Big Data, AI applications;
(2) **Using** IoT, Big Data, AI;
(3) **Data** collection and use.

The three clusters are chosen to structure the document and the work of the BPF. They are to a certain extent artificial and there exists overlap. For each of the clusters the BPF discussed concerns and challenges pertaining to the use of the new technologies and collected best practices, case studies and lessons learned to address them.

The BPF does not want to duplicate work done elsewhere, but intends to provide pointers to best practices and ongoing work in existing expert fora, to inspire and support policy and decision makers that are confronted with questions and considerations pertaining to the application of the new technologies.

This document reflects the work of the IGF2019 BPF IoT, Big Data, AI . The BPF outcome document is the result of an open and iterative process during the months preceding the IGF2019 meeting in Berlin, Germany, 25-29 November 2019. The structure and the content of the document were developed through a series of open and collaborative discussions with interested stakeholders, on an open mailing list[3], virtual webex meetings[4], and a BPF face-to-face discussion during the IGF in Berlin. A public survey launched in July on the BPF webpage helped to collect input for the discussions and report.

[2] https://www.intgovforum.org/multilingual/filedepot_download/8398/1774
[3] https://intgovforum.org/mailman/listinfo/aiiotbd_intgovforum.org
[4] See meeting reports at https://www.intgovforum.org/multilingual/content/bpf-internet-of-things-iot-big-data-and-artificial-intelligence-ai

II. Opportunities :
IoT, Big Data, AI, to address societal challenges

The number of applications of IoT, Big Data, and AI technologies is booming and will continue to grow exponentially in the coming years and decades. At the moment it looks like we are entering a new world of unlimited possibilities and opportunities. The new technologies find their way into every aspect of our lives, and appear in a multitude of forms and applications.

Often users don't realise that their are already frequent users of technology based on IoT, Big Data and AI. For example when they open their favorite app on their smartphone to organise their shopping, switch on the device to stream music into their living rooms, or subscribe to a platform that offers them a huge catalogue with their favorite series and movies. IoT, Big Data, AI, may be used by these applications to, for example, suggest new music to discover, selected based on the user's personal taste, play a role in the security and protection of the online payment systems in the e-shop, or to optimise the connection for a better quality when watching HD movies online.

The BPF asked in its survey what people consider the most exciting development that is based on IoT, Big Data, AI technologies.

BPF Survey: "*Which Applications and developments that combine IoT, Big Data, AI excite you most ?*

- Traffic control and management based on real-time traffic monitoring.
- Autonomous vehicles.
- Systems to help to decrease air pollution.
- Medical technologies and their ability to scan and diagnose; E-health devices preventing diseases, mixing medical improvement and transhumanism.
- Cloud applications.
- Recommendation tools for accessing media allowing for more personalised access instead of mass media.
- Smart assistants (e.g. Elexa, google home) allowing new use cases for the Internet and making existing ones more efficient.
- Smart watches connected to a mobile phone that collect data on a user's behavior, health, location, etc and provide this information to web-based services.
- Hardware and software that speed up the adoption of connected devices everywhere. This includes edge computing chips and AI-edge algorithms, energy harvesting/power management chips, tiny wearables that enhance communication mobility.
- Flood-alarm system.
- Smart electricity grid systems.
- Management of water resources. E..g. distribution of the Nile water between Ethiopia (electricity production), Sudan (irrigation for agriculture), and Egypt (agriculture, tourism) depending on water supply, efficiency of resource use and urgency of needs.

The IGF2019 decided to focus on IoT, Big Data, AI used in applications to achieve positive policy outcomes. IoT, Big Data, AI play an increasing role in addressing societal challenges. The new technologies may improve existing solutions, make them more efficient, or make it possible to approach issues in a totally new and more effective way. The new technologies can also empower people who today, for a variety of reasons, may have limited possibilities to act or influence. The examples showcased in this section intent to provide an idea of the broad range of opportunities and applications, rather than being exhaustive.

- **IoT, Big Data, AI contributing to achieving SDGs**

IoT, Big Data, AI applications can be enablers to make progress in different, in almost all, SDG areas. The data and data analysis can assist policy makers in making better choices and taking the right decisions, as well as allow to measure the effect of the decisions and progress made.

In a recent message on the occasion of the 50th anniversary of the World Telecommunication and Information Society Day UN Secretary-General António Guterres highlighted the importance of international technology standards in accelerating innovation worldwide and said that technological advances such as 5G and the Internet of Things have the potential to deliver considerable social and economic benefits and to drive progress towards the Sustainable Development Goals.[5]

- **IoT, Big Data, AI improving cybersecurity**

AI makes it faster to overcome cybersecurity risks by making use of records of previous data attacks to recognise suspicious activity. It allows to detect, identify and automatically manage a threat and solve it by using automated solutions. Big Data, information collected through different sources, helps in analysing, observing, detecting and examining irregularities in a network, and as such makes it possible that an issue is addressed in a fraction of the time compared to traditional methods. Also, it helps the cyber analyst in predicting the possibilities of invasion and intrusion.[6]

- **IoT, Big Data, AI making the Internet more useful & more accessible to people**

IoT, Big Data, AI applications can empower internet users if designed to help end users to manage their own lives the way they want them, rather than to put external agencies in control.

- **Urbanisation, Smart cities**

Several cities are experimenting with IoT, Big Data, AI applications, for example to automate street lightning to increase safety, traffic lights to manage traffic flows, optimise maintenance based on tracking use and structural health of infrastructure, cognitive CCTV for safety, etc.

[5] http://www.globaltimes.cn/content/1150440.shtml
[6] Danish Wadha, 'How AI and Big Data will shape the future of cybersecurity', 2018, https://www.iottechexpo.com/2018/10/iot/how-ai-and-big-data-will-shape-the-future-of-cybersecurity/

- **Civil Protection and security**

The flood-alarm system (FAS) in the village called "Li Xing Cun" (China), deployed by FIOT-LAB, is based on 4 monitoring systems that collect data on the water level, water speed, local rainfall, wind speed, local humidity in air and soil, images of ground topography, images of river, and one IoT cloud platform to perform data analysis (deep learning of data collected). The system will set off a flood alarm well in advance of the imminent danger.

- **Agriculture**

Data from IoT sensors is processed to advise farmers about the optimal time to plant, harvest, apply nutrients, water, etc. IoT data is used to track and collect data about livestock.[7]

- **E-commerce, financing**

Some e-commerce platforms collect data on a customer's payment history to calculate a user's score which is used amongst others in decisions to extend credit and other benefits, and as such helps to protect both the provider and user against loss and overspending.

- **Nature conservation**

Tracking of animal populations and numbers, change of land use and vegetation during time via satellite images and managing big visual data with AI allows to recognise patterns in how animal populations change and behave.

- **Coordination of humanitarian aid**

Coordination of international assistance to identify where the resources are needed most, i.e. at the right time and at the right moment and in the right amount. Pooling together of different donor sources to be employed most effectively and to direct resources on a need-based analysis as opposed to media attention.

- **Violence prevention & more effective crisis response**

Mapping of violence during elections or armed conflicts based on an analysis of the information transmitted online from observers, victims or bystanders.

[7] The Internet of Things, Accelerating a Connected New Zealand (2018), New Zealand IoT Alliance, https://iotalliance.org.nz/wp-content/uploads/sites/4/2018/09/Accelerating-a-Connected-New-Zealand-eBOOK.pdf

III. Policy Challenges:

IoT, Big Data, AI to address societal challenges that otherwise would be difficult to address

The fast development of the technologies and their applications comes with a growing number of concerns and questions pertaining to the effects and side-effects of a massive use of IoT, Big Data and AI.

The BPF survey asked respondents: *"Which of the applications and developments that combine IoT, Big Data, AI do you fear the most?"*. The answers, of which a selection is listed below, reflect a wide range of worries and concerns.

> BPF survey: *"Which of the applications and developments that combine IoT, Big Data, AI do you fear the most?"*.
>
> - Applications affecting our lives such as autonomous vehicles, remote robot surgery, armed drones and how they could be hacked.
> - Abuse of health data.
> - Robots acting like humans and able to have emotions; AI's that will supplement love life for married couples.
> - Software implants in humans;
> - Privacy threats when passing through internet platforms.
> - Surveillance and the inability to opt out.
> - Profiling while unclear what data is used (e.g. what means 'private mode' in an IoT world?)
> - Facial or any bio-recognition or biometrics technology in government surveillance.
> - Large platforms and companies such as Facebook, Google, etc.
> - Security and privacy issues related to our data shared through social networks, IoT platforms and through the air (energy harvesting).

From policy and decision makers is expected that they face current and future challenges. They should guide us by dealing with a series of pertinent policy questions and providing future proof answers that address today's concerns but remain relevant for applications of the IoT, Big Data, AI that are yet to be discovered[8].

The BPF intends to depict the most prominent concerns and policy questions, refer to ongoing discussions and collect best practices and experiences from stakeholders already addressing them. To structure its work, the BPF identified three clusters of policy challenges: **trust** in the technologies and applications, their **use and uptake** and concerns related to the collection, management and use of **data**.

[8] The BPF 2018 recommended that policy discussions should be technology neutral, and focus on what a technology does rather than how it does it, as the latter may quickly change when a new technology is introduced.

Policy Challenge 1 - Enhancing justified trust in IoT, Big Data, AI, to stimulate their use to address societal challenges that otherwise would be difficult to address.

Introduction

The BPF aims to facilitate the propagation of best practices that promote and enhance the use of IoT, Big Data, AI applications to address societal challenges. This will maximize the contribution of these new technologies to achieving the United Nations Sustainable Development Goals (SDGs).

Trust plays an essential role as a motivator stimulating the uptake of IoT, Big Data, AI and a lack of trust in the new technologies negatively impacts the interest or motivation to start using IoT, Big Data, AI to solve existing problems. This trust has to be gained. Trustworthy technologies have to be developed first and trustworthy actors (cooperations, geovernments, etc.) need to be in charge of their use.

Trust in IoT, Big Data, AI is an important factor to stimulate the uptake and use of the new technologies to address societal challenges. Trust in technology is crucial for its growth and uptake. Without trust users - individual as well as companies and organisations - will not invest in the technology and not riks to depend on a technology and its applications to achieve a desired outcome.

Trust itself is a multilayered concept and establishing the right balance between the layers to enable *"correct (and justified) trust"* is an important policy challenge. The UN SG's High Level Panel on Digital Cooperation underlined the importance of shared standards, values and best practices to build trust: 'As the digital economy increasingly merges with the physical world and deploys autonomous intelligent systems, it depends ever more on trust and the stability of the digital environment. Trust is built through agreed standards, shared values and best practices. Stability implies a digital environment that is peaceful, secure, open and cooperative. More effective action is needed to prevent trust and stability being eroded by the proliferation of irresponsible use of cybercapabilities.'[9]

Trust - a universal concept

Trust is a 'firm belief in the reliability, truth, or ability of someone or something.'[10] Trusting someone or something means 'to believe that someone is good and honest and will not harm you, or that something is safe and reliable.'[11]

[9] The age of digital interdependence, UN-SG's High-level Panel on Digital Cooperation, 2019, p. 31
[10] Oxford Dictionaries, https://en.oxforddictionaries.com/definition/trust .
[11] Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/trust .

Trust can be viewed as '(1) a set of specific beliefs dealing with benevolence, competence, integrity, and predictability (trusting beliefs); (2) the willingness of one party to depend on another in a risky situation (trusting intention); or (3) the combination of these elements.'[12]

In a practical and operational context one can emphasize the expectation that someone or something will fulfil their promises and obligations. Trustworthiness, defined as a quality of being "honest, competent and reliable, is considered by some as a more valuable concept than trust.[13]

Trust plays an important role for the functioning of societies, human interactions and organisations. It is important however to recognise that definitions of trust are determined by culture. 'Cultures and communities have such deep and varied experiences of trust that there is no single shared definition that would make sense.'[14] Very easily discussions and interpretations risk not to transcend the false-consensus bias[15] and one overestimates the extent to which others share the own opinions and beliefs. It is an important responsibility for policy makers to identify aspects of trust, relevant to IoT, Big Data, AI , that could help to build up notions of trust which hold across cultures and applications.

Trust - A multi-layered concept

Trust in IoT, Big Data, AI is a multilayered concept. Trust in the technologies and their applications can mean that one believes in the benefits or gains the technology will bring compared to other ways of dealing with a challenge; or trust that the technology will deliver and behave as expected; but also the trust that the technology will not bring harm to their users, to others or to humanity as a whole.

'Issues of compliance and accountability directly relate to trust, as they are key to both the adoption and public acceptance of technology, and to ensuring that the technologies deployed are, and remain, appropriate and fit for purpose, align with social norms, where possible can be held to account when and where necessary.'[16] 'As AI systems are widely deployed in real-world settings, it is critical for us to understand the mechanisms by which they take decisions, when they can be trusted to perform well, and when they may fail.'[17]

The BPF identified different layers and dimensions of trust in IoT, Big Data, AI technologies and applications. We are sure this is not an exhaustive list and one can easily imagine additional layers or elements. Throughout its discussions and based on the input received the BPF

[12] Siau, K. Wang, W. (2018), Building Trust in Artificial Intelligence, Machine Learning, and Robotics, *CUTTER BUSINESS TECHNOLOGY JOURNAL (31), S. 47-53;* quoted in: Ethics Guidelines for Trustworthy AI, HLEG on AI (2019).
[13] Laura James, Talking about trust, TRUST & TECHNOLOGY INITIATIVE, p.37
[14] Laura James, Talking about trust, TRUST & TECHNOLOGY INITIATIVE, p.37
[15] https://psychology.iresearchnet.com/social-psychology/social-cognition/false-consensus-effect/
[16] Jatinder Singh, Compliant and Accountable Systems, TRUST & TECHNOLOGY INITIATIVE, p.43
[17] Adrian Weller, AI Trust & Transparency with the Leverhulme Centre for the Future of Intelligence, TRUST & TECHNOLOGY INITIATIVE, p.44

established the following list of different layers and approaches to trust in IoT, Big Data, AI and their applications:

Trust in IoT, Big Data, AI - layers and aspects

- Trust in what?
  - Security
    - Adequate security of IoT, Big Data, AI technologies and applications, set up in a way that actors *__can__* take responsibility for their part in it.
  - Reliability
    - Consistent performance according to its specifications.[18]
  - Availability
    - Trust that applications will be available as expected
  - Transparency
    - Meaningful transparency, so that there is adequate certainty that systems do what their suppliers promise.
  - Ethics
    - Respect for ethical principles and application of the technology is not intentionally harming humans or humanity.
  - Compliance
    - Active pursuit of compliance (in terms of checks and actions when suppliers do not do what they promise (obliged by law, or self-declared).
  - Liability & Accountability
    - Provider of the technology is legally responsible and accountable for the behaviour of the technology.

- Trust by who?
  - User and providers of services
    - Trust to describe the quality of the interactions between two parties using a digital medium, typically the users and the companies that build a digital platform or technology. The users ask for trust, the provider should guarantee trust.
  - Supply chain intermediaries

- Trust that is generated & backed up by who?
  - International Community, International Organizations
  - Governments
  - Corporations
  - International civil society

- Trust at various levels and evolving understanding of trust
  - At macro-level:
    - geographic differences (for example between countries and cultures)
  - At micro-level:

[18] https://whatis.techtarget.com/definition/reliability

        - At company level, for example different companies or organisations define trust differently based on their ethical guidelines and commitments
    - Evolving insight
        - Knowledge and trust evolve over time. New insights, e.g. in the working or effects of IoT, Big Data, AI applications may influence the trust in a technology in a positive or negative way.

A correct (and justified) trust in IoT, Big Data, AI

Trust in IoT, Big Data, AI and their applications is multilayered. Maximising the desired result within one layer is difficult and may impact and limit what is possible on other dimensions. This makes trust a complex composition with trade-offs between its dimensions. As a result, it is possible to make choices based on priorities and policy preferences. For example: providing 100% security and 100% reliability is almost impossible and some security measures can conflict with ethical and privacy considerations. Finding a right balance between security, privacy, ethical and other considerations is a policy challenge. People accept that there exist trade-offs when using a technology. For policy makers it is a challenge to understand these trade-offs and support the right balance.

The BPF called this balance a "correct (and justified) trust" : that is, neither too little trust (preventing benefits from being realised) nor too much trust (exposing unsuspecting users to undesired risk).

> *Correct (and justified) trust" :*
> *that is,*
> *neither too little trust (preventing benefits from being realised)*
> *nor too much trust (exposing unsuspecting users to undesired risk).*

The BPF survey put this description of *"correct (and justified) trust"* to the community. Below is a summary of the feedback received:

> BPF Survey: *The BPF wants to understand what is important to establish "correct (and justified) trust", that is, neither too little trust (preventing benefits from being realised) nor too much trust (exposing unsuspecting users to undesired risk). Do you agree that "trust" in relation to IoT, Big Data, AI applications should mean 'correct (and justified) trust', as just explained? If not, please explain why and give your preferred definition.*

- The definition lacks an ethical component.
- Trust should mean REAL TRUST.
- Agree with the definition.
- There are some principles that need to be absolutely certain (an A.I software can never take a decision of life or death on humans without human involvement). For other kinds of relation the trust needed could be "correct and justified".

- The definition is unclear, you should be able to trust technologies, while at the same time not be naive about how it COULD be used against you.
- Yes, without "trust" people would not follow the policies and won't buy the products.
- No, I don't believe. Know and understand your situations and cases before putting your trust or not to trust then, make a decision. I would suggest "intellect and trust".
- Yes I agree, too little can prevent use, too much can create errors.
- There is no "correct (justified)" trust, there is only "informed and controlled" trust. We cannot live in information silos/islands alone, this is not practical in our world today where we need to access internet for news and information. What is correct? This is a relative term.
  Hence I believe there is only informed and controlled trust. "Informed" meaning that at the point of data collection, the user is fully aware and told of where his information goes to. Along the way, if there are changes/updates on how information is handled, the user then gets a notification informing him, which he can choose to opt in/opt out, hence giving him control of his data.
- As for balancing the efficiency and security, it is very hard to construct a non-centralized mechanism that is efficient enough that can be trusted by anyone in the system, therefore a voted centralized system shall be implemented to as an agent for connecting the truster and trustee. However, a supervising mechanism shall be implemented to supervise this centralized mechanism for making any mistakes.

BPF Survey: *From your perspective, what is important and influences this trust?*

- Developers, scientists, community to work with security in mind.
- AI-algorithms need to be well-developed with ethics in mind.
- Gaining and maintaining legitimacy.
- Informed consent / transparency.
- Nowadays, no one can be sure that IoT, Big Data and Ai will be used only to his/her benefit and not to the benefits of corporates.
- The fact that corporations or states that failed in respect this trust could be punished and pursued if they don't respect the engagements taken.
- Transparency:
    1. How do public and private sectors collect and use those data?
    2. What will they do?
    3. Where do they save those data?
    4. how many people provide their own data etc.
- Have the right intellectual and build a lot more confidence through sacrificial.
- Transparency and communication.
- Reliability and resiliency.
- Companies or organisations that routinely handle user data should consistently show that they place high importance in maintaining privacy, and have rules to ensure this is enforced. They should not repeatedly and knowingly risk users' data for business gain. There needs to be an Ethics Guideline on the informed and controlled trust and maintaining user privacy.

A hierarchy of trust in IoT, Big Data, AI ?

In an attempt to further differentiate and better understand trust in IoT, Big Data, AI, and the relation between different layers of trust, the BPF had a discussion on whether the different layers of trust could be ordered in a hierarchical system, comparable to Maslow's pyramid of

needs. This would mean that the presence of a lower layer is a condition to optimise the trust on the higher level. Such a system, with some layers being more fundamental because other layers depend on them, could be read top-down as a 'hierarchy of trust', or bottom-up as a hierarchy of distrust. Below is how such a system could look like.

A hierarchy of trust in IoT-Big Data-AI applications?

- Human Rights - Trust that apps respect all human rights
- Privacy - Trust that apps protect privacy
- Choice - Trust that apps empower users[19]
- Data Divide - Trust that apps will not be biased
- Legal - Trust that apps do not violate national laws
- Security - Trust that apps will secure users' data
- Accountable - Trust that apps will be accountable to users
- Reliability - Trust that apps will work and be reliable
- Availability - Trust that apps will be available

Conclusion

Trust in Iot, Big Data, AI is important for the development and uptake of new and improved solutions that are based on applications of these technologies to address societal challenges. This trust, however, is a multi-layered concept, and establishing the right balance between the different dimensions can upto a certain degree be influenced by policy choices. The BPF called this balance: *"correct (and justified) trust" : that is, neither too little trust (preventing benefits from being realised) nor too much trust (exposing unsuspecting users to undesired risk).*

The policy challenge 'enhancing trust in IoT, Big Data, AI can be formulated as follows:

1. Be aware of the importance of trust and of its multi-layered character,
2. Understand the balances and trade-offs between different layers,
3. Based on 1 & 2 make policy choices and take initiatives to enhance trust.

We refer to academic and interdisciplinary discussion for those who wish to further christalise the dimensions and gain insight of the relation and trade-offs between them.

The BPF, in the next section, will look for best practices to deal with the policy challenge to define, establish and enhance *"correct (and justified) trust"* in IoT, Big Data, AI.

[19] Including for example, trust that apps do not "lock users in"; "the right to be forgotten" - Choice basically relates to self-determination and the freedom to opt out of a certain tech application (including surveillance tech such as facial recognition in public spaces!) and delete all private data that was generated.

Best Practices to address Policy Challenge 1

The BPF collected the following examples of best practices and initiatives that are intended to contribute to trust in IoT, Big Data, AI and their applocations.

- **BPF Survey Feedback**
  BPF Survey: *Are you aware of any best practices or promising initiatives that could address your concerns and improve your trust in the applications and developments that combine IoT, Big Data and AI*
  - Google Self-driving cars are an example of technology being audited a lot. They made tests with possible edges of decisions in machine level.
  - Medical ethics / enforceable principles (legally : competition law / breach of contract)
  - Yes. there are many projects and applications, like Journalism Trust Initiative of Reporters Without Borders or the research project SoBigData of the EU
  - Initiatives to address concerns about the use of facial recognition, as for example discussed in 'California Considering Banning Facial Recognition Devices for Police Software' (url), 'Opinion: Don't Regulate Facial Recognition. Ban It.' (url), 'Facial recognition tech is creeping into our lives – I'm going to court to stop it' (url).
  - Usage of single cloud provider.
  - Automated vulnerability detection and complex data analysis.
  - No, I don't think so; Not really; Not yet.
  - Blockchain technologies could be one way to securely store data; in a way that cannot be easily hacked. Also the connection of edge devices with edge computing capabilities, are very similar concept to blockchain (I.e. edge devices linking to each other is like a Physical Blockchain). This is also an exciting area to look into.
  - There should be a standard of security level that the human's bio-ID collecting and analyzing system.

- **OECD - Recommendation of the Council on Artificial Intelligence**

5 value-based principles	**5 recommendations**
- inclusive growth, sustainable development and well-being; - human centered values and fairness; - transparency and explainability; - robustness, security and safety.	- investing in AI research and development; - fostering a digital ecosystem for AI; - shaping an enabling policy environment for AI; - building human capacity and preparing for labour market transformation; - international cooperation for trustworthy AI.

  On 22 May 2019, the OECD adopted the first 'Intergovernmental standard on AI policies', which aims to foster innovation and trust in AI by promoting the responsible stewardship of **trustworthy AI** while ensuring respect for human rights and democratic values. The Standard is considered to be implementable and sufficiently flexible to stand the test of time.
  https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

- **UNESCO - COMEST**
  Within the framework of its work programme for 2018-2019, COMEST decided to address the topic of the Internet of Things (IoT), reflecting on the ethical considerations of IoT in relation to

society, science and sustainability. This work builds on the COMEST Report on Robotics Ethics (2017) and is undertaken with the participation of UNESCO's Communication and Information (CI) Sector.
http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SHS/pdf/COMEST_Concept_Note-IoT_en.pdf

- **OECD AI Policy Observatory**
  The OECD AI Policy Observatory (launch planned late 2019) is intended to become an online inclusive hub for AI information, evidence, and policy options. The Observatory aims to help countries encourage, nurture and monitor the responsible development of trustworthy artificial intelligence (AI) systems for the benefit of society. The core attributes of the Observatory will be 'Multidisciplinary', 'Evidence based', and 'Multistakeholder'. The Observatory will include a live database of AI strategies, policies and initiatives that countries and stakeholders can share; AI measurements and metrics, and good practices.
  https://www.oecd.org/going-digital/ai/about-the-oecd-ai-policy-observatory.pdf

- **Ethics Guidelines for Trustworthy AI - Independent High Level Expert Group on Artificial Intelligence (European Commission)**
  Trustworthy AI has **three components** that should be met throughout the system's entire life cycle; its should be:
  (1) Lawful - complying with all applicable laws and regulations,
  (2) Ethical - ensuring adherence to ethical principles and values,
  (3) Robust - from a technical and social perspective.

  Development, deployment and use of AI systems should meet the **seven key requirements** for Trustworthy AI:
  (1) Human agency and oversight,
  (2) Technical robustness and safety,
  (3) Privacy and data governance,
  (4) Transparency,
  (5) Diversity, non-discrimination and fairness,
  (6) Environmental and societal well-being,
  (7) Accountability.
  https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

- **Example of domestic initiative to enhance trust: Canadian Multistakeholder Process: Enhancing IoT Security**
  Recognizing the complexity of mitigating cyber security risks from the global proliferation of the Internet of Things (IoT) and the resulting necessity for a made in Canada policy to address these risks, the Internet Society, in partnership with the Ministry of Innovation Science and Economic Development (ISED), the Canadian Internet Registration Authority (CIRA), Canadian Internet Policy and Public Interest Clinic(CIPPIC), and CANARIE, undertook a voluntary multistakeholder process for the development of a broad-reaching policy to govern the security of the IoT for Canada.

  Impact on Trust: This initiative was designed to enhance trust in IoT and related technologies by creating an open, bottom-up dialogue where specific issues negatively impacting trust could be addressed. For example, the October 2016 Mirai Botnet attack was frequently cited by academics, civil society and users involved in the process as a significant breach of trust.

Recommendations on consumer education and awareness, labelling and network resilience leveraged the expertise of all participating stakeholders to enhance trust by reducing the risk of another Mirai-style attack. Government participation from a full range of departments and agencies contributed to building trust between stakeholders by providing an ongoing dialogue to address breaches of trust and mitigate risk.
Final Outcomes and Recommendations Report is available online at
https://iotsecurity2018.ca/draft-outcomes-report/ .

- **Trust & Technology Initiative**
  The Trust & Technology Initiative at the University of Cambridge brings together and drives forward interdisciplinary research to explore the dynamics of trust and distrust in relation to internet technologies, society and power; to better inform trustworthy design and governance of next generation tech at the research and development stage; and to promote informed, critical, and engaging voices supporting individuals, communities and institutions in light of technology's increasing pervasiveness in societies.
  https://www.trusttech.cam.ac.uk

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

Introduction

IoT, Big Data, AI and their applications come with a huge potential which they can contribute to solving day to day societal challenges. Embedding the new technologies in existing solutions can make these solutions more appealing, more effective, and more efficient. The use of IoT, Big Data, AI applications can also lead to completely new approaches to solve an issue.

Therefore the BPF put forward as a second Policy Challenge: Stimulating the use and uptake of IoT, Big Data, AI and their applications to achieve positive policy outcomes. What actions and initiatives can be taken to support the new technologies, but also, what concerns need to be taken into account.

"Positive policy outcome"

The designation "positive policy outcome" is not neutral. What is perceived as positive policy outcome, by whom and according to what criteria is context related, and within the same context can differ depending on the position of the person who the question is asked to. Similarly, identifying which social challenges need to be focussed on is a question with multiple answers. It makes sense to prioritise identified societal challenges that are supported by a broad international consensus, such as the United Nations Sustainable Development Goals.

Stimulating IoT, Big Data, AI for positive policy outcomes

- **Stimulating the development of IoT, Big Data, AI applications**
  Research and development of new technologies requires not only funding and resources. They are of major importance, but the challenge is much broader and includes for example having a training and educational system that delivers skilled researchers and developers, stimulating cooperation between education and research institutions and the industry.
  An extra stimulus might be needed to support the development of IoT, Big Data, AI solutions that help addressing challenges that are less interesting from a business perspective.

- **Stimulating the use and uptake of IoT, Big Data, AI solutions**
  The deployment of newly developed solutions based on IoT, Big Data, AI may need some additional promotion or support. In some cases existing legislation may hamper the introduction and use of new technologies. Also here, special effort might be needed to stimulate the use of new technologies that help to address a problem in less profitable contexts.

Capacity building and digital literacy should not be forgotten. People will not and cannot use what they don't understand, no matter how beautiful and promising and application looks.

Concerns, unintended outcomes and side-effects

While IoT, Big Data, AI have an enormous great potential, there are also concerns about the possible unintended impact and side-effects of the new technologies. When asked about the potential of IoT, Big Data, AI, one survey respondent, for example, answered *'I'm not excited at all. On the contrary - there are so many real threats to people.'* A reaction that many probably recognise.

So the policy challenge spreading the new technologies and stimulating use and uptake, should be accompanied by an awareness of the concerns pertaining to the introduction and use of IoT, Big Data, AI applications and unintended effects. Some side-effects may be easy to observe while other effects only surface after a longer time or additional research. One survey participant stressed that *'Decision makers need to understand the benefits and disadvantages of these developments and at least have a fair knowledge [and] the big picture view on the impact.'*

Access to IoT, Big Data, AI technologies and applications and their benefits, as well as the applications themselves may have a major social impact, which often is not immediately visible or remains unnoticed.

The BPF identified the following policy challenges and concerns:

- **Algorithms trained on data from the past possess a bias towards the past**
  Gaps in data resulting in biased algorithms do not only produce the base for future discrimination of women, youth, elderly people, marginalized and poor, but exhibit a strong path-dependency. 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 are AI based financial investment based on pure profit making without taking into account systemic risks or commodity trading that is based on exploitive producer and buyer relationships. In spite of all the digital change and its opportunities, this exhibits the danger of not allowing for spontaneous change and overcoming past patterns based on the needs of the future through creativity and empathy.

Secondly, and depending on the decision-making power that is given to AI, basing its decision on past decisions, outcomes and actions, may lead to 'bad', inappropriate or even dangerous decisions and actions - 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.

- **Algorithms may reinforce views and biases of their developers**
  Intelligent systems may reinforce discrimation as they reinforce the views and biases of their developers and are typical for the society or part of the world they live in.

  'It is also becoming apparent that 'intelligent' systems can reinforce discrimination. Many algorithms have been shown to reflect the biases of their creators. (...) Gaps in the data on which algorithms are trained can likewise automate existing patterns of discrimination, as machine learning as only as good as the data that is fed to them.'[20]

- **Unequal access to the benefits of IoT, Big Data, AI**
  'Both within the spaces where AI is being created, and in the logic of how AI systems are designed, the costs of bias, harassment, and discrimination are borne by the same people: genderminorities, people of color, and other under-represented groups. Similarly, the benefits of such systems, from profit to efficiency, accrue primarily to those already in positions of power, whoagain tend to be white, educated, and male. This is much more than an issue of one or two bad actors: it points to a systematic relationship between patterns of exclusion within the field of AI and the industry driving its production on the one hand, and the biases that manifest in the logics and application of AI technologies on the other.'[21]

- **Distribution of risks**
  From the 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.

  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 measures to avoid them. This could also include a full or partial bans 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, a ban on autonomous weapon systems should get discussed; same might also be the case for surveillance systems employed to control and repress citizens and their fundamental human rights, incl. civil and political freedoms of movement and expression.

[20] The age of digital interdependence, UN-SG's High-level Panel on Digital Cooperation, 2019, p. 17
[21] West, S.M., Whittaker, M. and Crawford, K. (2019). Discriminating Systems: Gender, Race and Power in AI. AI Now Institute, p7. Retrieved from https://ainowinstitute.org/ discriminatingsystems.html .

What is more, marginalized groups (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 purposes. What can, and should we do about it?

- **Ethics and Fundamental Rights**
  Ethics and respect for Fundamental Rights need to be taken into account when exploring new applications of IoT, Big Data, AI and assessing their potential impact. This includes discussions on autonomy and self-determination in the use of digital technologies (what technologies do we want to use for what purpose and who decides), justice (access to technology, but also distribution of risks), or what technology means for human dignity (which is close to human rights, but goes a bit beyond, and for example includes the interactions between humans - machines).
  The UN Human Rights Council Advisory Committee recently invited all stakeholders to report on 'how human rights opportunities, challenges and gaps arising from new and emerging digital technologies could be addressed.[22]

22
https://www.business-humanrights.org/en/un-human-rights-council-advisory-committee-invites-inputs-on-opportunities-challenges-of-new-emerging-digital-technologies-on-rights

Best Practices to address Policy Challenge 2

The BPF collected the following examples of best practices and initiatives that are intended to stimulate the uptake and use of IoT, Big Data, AI and initiatives that aim to address the concerns about the side-effects and unintended results.

- **BPF Survey Feedback**
  Survey: *In your area (geographical region, professional environment, stakeholder group, or field of specialisation), what are the key policies, and policy making-approaches directly or indirectly related to the use of IoT, Big Data, and AI?*
    - My country is totally under-developed in Digital Laws, and people has no concern at all.
    - Privacy / contract law / competition and consumer law (in EU region).
    - The ethical initiative on AI promoted by UNESCO, the Council of Europe working group on algorithms, the initiatives announced by French and German government on A.I.
    - A lot of talk, not very specific. Especially AI is badly defined. I do not see a clear difference between Big Data and AI. Big Data is useless until combined with machine learning, which is an approach to AI. what's important in AI is the relative autonomy in the system's decision making (which is enabled by ML applied to BD).
    - Asia-Pacific countries are crazy to have Smart Cities. They must be using a lot of data analysis, IoT devices connection and AI deployment in Smart City development solution.
    - The IoT creates distinctive challenges to privacy, many that go beyond the information privacy problems that currently exist. Abundant of this stems from integrating devices into our environments without consciously using them. This is becoming more prevalent in consumer devices, like tracking devices for phones and cars as well as smart televisions. Voice recognition or vision features being integrated that can endlessly listen to conversations or watch for activity and selectively transmit that information to a cloud service for process, that generally includes a third party. Gathering of this information exposes legal and regulatory challenges facing information protection and privacy law.
    - No policies at the moment and business minded people can make use of the situation knowing there is nothing in place to assist as guidance.
    - My Government is in the process of developing a Smart Barbados, I am not too sure how far this has gone and if training is really done to update everyone.
    - Afrinic expert group.
    - These are new areas. Asian governments have some guidelines but little experience in forming and reinforcing industry standards.

- **National strategies and action plans to stimulate the use of IoT, Big Data, AI**
  In many countries and regions governments, sometimes in close cooperation with other stakeholders have developed strategies and action plans to support the development and uptake of IoT, Big Data, AI. For example:
    - German Strategy for Artificial Intelligence https://towardsdatascience.com/ai-made-in-germany-the-german-strategy-for-artificial-intelligence-e86e552b39b6
    - Italian Strategy for Artificial Intelligence https://www.mise.gov.it/images/stories/documenti/Strategia-Nazionale-Intelligenza-Artificiale-Bozza-Consultazione.pdf

- **IoT Large Scale Pilots Programme**
  The EU-funded IoT Large-Scale Pilots Programme (LSP) comprises comprises a total of seven innovation consortia (5 LSPs and 2 Communication Support Actions), working hand in hand to foster the uptake of Internet of Things (IoT) in industrial sectors in Europe and beyond within the European IoT Pilot working group. By addressing both societal and industrial challenges through IoT, the LSP seeks to improve the competitiveness of Europe at the global level, while increasing the quality of life of its citizens.
  https://www.iof2020.eu/about/large-scale-pilot-programme

- **CLAIRE - pan-European Confederation of Laboratories for Artificial Intelligence Research in Europe**
  CLAIRE is an initiative by the European AI community that seeks to strengthen European excellence in AI research and innovation. To achieve this, CLAIRE proposes the establishment of a pan-European Confederation of Laboratories for Artificial Intelligence Research, a network of Centres of Excellence in AI, strategically located throughout Europe, and a new, central facility that will promote new and existing talent and provide a focal point for exchange and interaction of researchers at all stages of their careers, across all areas of AI.
  https://claire-ai.org

- **Recommendations for Addressing Bias and Discrimination in AI Systems (AI Now Institute)[23]**
  - Remedying bias in AI systems is almost impossible when these systems are opaque. Transparency is essential, and begins with tracking and publicizing where AI systems are used, and for what purpose.
  - Rigorous testing should be required across the lifecycle of AI systems in sensitive domains. Pre-release trials, independent auditing, and ongoing monitoring are necessary to test for bias, discrimination, and other harms.
  - The field of research on bias and fairness needs to go beyond technical debiasing to include a wider social analysis of how AI is used in context. This necessitates including a wider range of disciplinary expertise.
  - The methods for addressing bias and discrimination in AI need to expand to include assessments of whether certain systems should be designed at all, based on a thorough risk assessment.
    https://ainowinstitute.org/discriminatingsystems.pdf

- **IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems**
  Within the framework of the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems eight high-level General Principles of Ethically Aligned Design were discussed. The ethical and values-based design, development, and implementation of autonomous and intelligent systems should be guided by the following General Principles:
  1. Human Rights
     A/IS shall be created and operated to respect, promote, and protect internationally recognized human rights.

[23] West, S.M., Whittaker, M. and Crawford, K. (2019). Discriminating Systems: Gender, Race and Power in AI. AI Now Institute, p4. Retrieved from https://ainowinstitute.org/ discriminatingsystems.html .

2. Well-being
   A/IS creators shall adopt increased human well-being as a primary success criterion for development.
3. Data Agency
   A/IS creators shall empower individuals with the ability to access and securely share their data, to maintain people's capacity to have control over their identity.
4. Effectiveness
   A/IS creators and operators shall provide evidence of the effectiveness and fitness for purpose of A/IS.
5. Transparency
   The basis of a particular A/IS decision should always be discoverable.
6. Accountability
   A/IS shall be created and operated to provide
   an unambiguous rationale for all decisions made.
7. Awareness of Misuse
   A/IS creators shall guard against all potential misuses and risks of A/IS in operation.
8. Competence
   A/IS creators shall specify and operators shall adhere to the knowledge and skill required for safe and effective operation.
   https://ethicsinaction.ieee.org
   https://standards.ieee.org/industry-connections/ec/autonomous-systems.html

- **UNESCO - Steering AI for Knowledge Societies: A ROAM Perspective**
  https://en.unesco.org/news/unesco-advocated-roam-principles-steering-ai-knowledge-societies
  https://en.unesco.org/system/files/unesco-steering_ai_for_knowledge_societies.pdf

- **UN Human Rights Council Advisory Committee -**
  In July 2019, the UN Human Rights Council adopted a resolution entitled, "New and emerging digital technologies and human rights". In this resolution, the Council requested that the Advisory Committee prepare a report on the possible impacts, opportunities and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights and to present the report to the Council at its forty-seventh session.[24]

[24] https://www.business-humanrights.org/en/un-human-rights-council-advisory-committee-invites-inputs-on-opportunities-challenges-of-new-emerging-digital-technologies-on-rights

Policy Challenge 3 - The collection and use of data generated, collected and analysed by IoT, Big Data, AI applications.

Introduction

The increase of computing power makes that unseen quantities of data can be analysed in ever shorter time and at lower cost. The growth of the internet, the polarity of social platforms, and the roll-out of the IoT make that enormous quantities of data are generated. This data, often combined data from different sources, are analysed using AI technologies to gain insight, draft conclusions and take decisions. One step further, systems based on AI technology are fed with large amounts date to train them in machine learning and automated decision making.

There's a wide range of policy issues and concerns directly linked to the collection, management, and use of data in an IoT, Big Data, AI context. The BPF is focussing on data generated by or collected via the internet, however many of the considerations, issues and best practices related to the collection and use of data for AI, machine learning and automated decision making processes are expected to be relevant regardless of whether the data is collected off- or online.

In this section the BPF explores some of the most pressing challenges that frequently come up when discussing the collection, use and governance of data used in the context of IoT, Big Data, AI applications.

> Quote: "*(...) computers and systems, only do what they have been programmed to do. Extending this to the future of AI, it can be said that systems of Artificial Intelligence and learning in general, are equipped to make decisions, that are dependent on the rules that they have been provided, the data that they have been provided, and the quality of that data.*"[25]

[25] Comninos A., Konzett M, (2018), FABRICS, Emerging AI Readiness, p. 15/16.

Policy issues, questions and considerations

- **Data quality**
  While large amounts of data are essential for the training of AI systems[26] , this doesn't mean that more data is automatically better or that the system with the most data is automatically the best system. It is a challenge for companies, governments and civil society foster the collection of high-quality datasets so that machine learning systems are trained using accurate and representative data.

  Incomplete, inaccurate, or biased data can lead to wrong conclusions and wrong of less optimal decisions. For example, when a facial recognition algorithm trained on a set that contains only faces of white men it will have trouble recognising any other kind of face. When an evaluation function is trained with data based on historical decisions any past bias will be learned by the algorithm. For example, mortgage loan algorithms may copy the historic decisions of human loan officers or hiring algorithms can manifest existing sexsim.[27]

- **Impact of legislation on data quality and accuracy**
  Existing legislation intended to increase privacy (e.g. GDPR, right to be forgotten, copyright) may impact the data quality and, for example, make it more difficult to check the representativeness of a dataset.

- **Respecting Privacy**
  Collecting and analysing data may conflict with privacy considerations. Personal data and information on a person's online behaviour may be collected without the user being aware and different data sets can be combined to allow data profiling.

  Can data be collected whilst respecting privacy? How can personally identifiable information be removed and data disaggregated in an age of machine learning and

[26] Accessible explanation of how machine learning / AI training works: "Current machine learning techniques aren't all that sophisticated. All modern AI systems follow the same basic methods. Using lots of computing power, different machine learning models are tried, altered, and tried again. These systems use a large amount of data (the training set) and an evaluation function to distinguish between those models and variations that work well and those that work less well. After trying a lot of models and variations, the system picks the one that works best. This iterative improvement continues even after the system has been fielded and is in use.
So, for example, a deep learning system trying to do facial recognition will have multiple layers (hence the notion of "deep") trying to do different parts of the facial recognition task. One layer will try to find features in the raw data of a picture that will help find a face, such as changes in color that will indicate an edge. The next layer might try to combine these lower layers into features like shapes, looking for round shapes inside of ovals that indicate eyes on a face. The different layers will try different features and will be compared by the evaluation function until the one that is able to give the best results is found, in a process that is only slightly more refined than trial and error."
Bruce Scheier, James Waldo, 'AI Can Thrive in Open Societies', FP, 13 June 2019, https://foreignpolicy.com/2019/06/13/ai-can-thrive-in-open-societies/

[27] Bruce Scheier, James Waldo, 'AI Can Thrive in Open Societies', FP, 13 June 2019, https://foreignpolicy.com/2019/06/13/ai-can-thrive-in-open-societies/

increasingly accessible compute power? Are traditional methods of doing this rendered vulnerable?

The UN SG's High-level Panel on Digital Cooperation calls for 'clear and transparent standards that will enable greater interoperability of data in ways that protect privacy while enabling data to flow for commercial, research and government purpose, and supporting innovation to achieve SDGs. Such standards should prevent data collection going beyond intended use, limit re-identification of individuals via datasets, and give individuals meaningful control over how their personal data is shared.'[28]

- **Data ownership**
  'Expanded access to data could be ideal for all countries. However, the data originates with individual people. Their data individually and collectively is being used and will in the future be used in many instances for commercial purposes, and consequently has value. People should be able to share in the wealth that is created from their data. They should be compensated for this use.'[29]

- **Data availability and digital " data" divides**
  'Today a few large corporations are favoured, as they are the best positioned to collect and process vast quantities of data from ecommerce, digital assistants and other sources. Several countries also have inherent advantages due to their sizeable populations, with vast pools of collectable data about many facets of life, from driving behaviours to cell phone use to internet browsing. This leads to an imbalance of power and wealth, caused by information being in the hands of the few, which gives them the opportunity to use these large volumes of data to draw meaningful inferences and achieve economies of scale.'[30]

- **Data sharing, free flow of data**
  Concerns are mounting that valuable reservoirs of information will increasingly be confined within national borders, a phenomenon known as data localization.[31]

[28] The age of digital interdependence, UN-SG's High-level Panel on Digital Cooperation, 2019, p. 31
[29] Murat Sönmez, 'How data exchanges can level the digital playing field', WEFORUM, 2019, https://www.weforum.org/agenda/2019/06/data-exchanges-digital-ai-artificial-intelligence/
[30] Murat Sönmez, 'How data exchanges can level the digital playing field', WEFORUM, 2019, https://www.weforum.org/agenda/2019/06/data-exchanges-digital-ai-artificial-intelligence/
[31] Masumi Koizumi, 'Japan's pitch for free data flows 'with trust' faces uphill battle at the G20 amid 'splinternet' fears', Japan Times, 2019, https://www.japantimes.co.jp/news/2019/06/27/business/tech/japans-pitch-free-data-flows-trust-faces-uphill-battle-g20-amid-splinternet-fears

Best Practices to address Policy Challenge 3

The BPF collected the following best practice examples to address policy considerations pertaining to the collection and use of Internet generated data.

- **Council of Europe - Guidelines on Artificial Intelligence and Data Protection (January 2019)**
  The Guidelines on Artificial Intelligence and Data Protection published by the Consultative Committee of the Convention for the Protection of Personal Data (Convention 108) aim to assist policy makers, artificial intelligence developers, manufacturers and service providers in ensuring that AI applications do not undermine the human dignity and the human rights and fundamental freedoms with regard to data protection.
  https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8
  https://www.coe.int/en/web/artificial-intelligence/-/new-guidelines-on-artificial-intelligence-and-data-protection

- **Council of Europe - Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data (January 2017)**
  The 2017 Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data provides a set of principles and guidelines pertaining to (1) Ethical and socially aware use of data; (2) Preventive policies and risk-assessment; (3) Purpose limitations and transparency; (4) By-design approach; (5) Consent; (6) Anonymisation; (7) Role of the human intervention in Big Data-supported decisions; (8) Open Data; and (9) Education.
  https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0

- **Big Data UN Global Working Group**
  The UN Global Working Group on Big Data for Official Statistics is chartered
  (a) To provide a strategic vision, direction and coordination for a global program on big date for official statistics, including for indicators of the post-2015 development agenda;
  (b) To promote practical use of big data sources, including cross-border data, while building on existing precedents and finding solutions for the many existing challenges , including:
    - Methodological issues, covering quality concerns and data analytics,
    - Legal and other issues in respect of access to data sources,
    - Privacy issues, in particular those relevant to the use and re-use of data, datalinking, and re-identification,
    - Security, information technology issues and management of data, including advanced means of data dissemination, assessment of cloud computing and storage, and cost-benefit analysis,

  (c) To also promote capacity building, training and sharing of experience;
  (d) To foster communication and advocacy of the use of big data for policy applications, especially for the monitoring of the post-2015 development agenda;
  (e) To build public trust in the use of big data for official statistics.
  https://unstats.un.org/bigdata/
  Terms of reference and mandate (.pdf) of the Global Working Group on Big Data for Official Statistics

- **G20 - Statement on free flow of data**
  The G20 ministers, in June 2019, in a statement released after a ministerial meeting on trade and the digital economy in Tsukuba, Ibaraki Prefecture, ahead of the Osaka summit, endorsed the vision that a set of international rules enabling the free movement of data across borders is desirable “In order to build trust and facilitate the free flow of data, it is necessary that legal frameworks both domestic and international should be respected.
  https://www.japantimes.co.jp/news/2019/06/27/business/tech/japans-pitch-free-data-flows-trust-faces-uphill-battle-g20-amid-splinternet-fears

Links and resources

IGF2019 BPF IoT, Big Data, AI
Webpage

IGF2019 BPF IoT, Big Data, AI workshop
Agenda and report
Recording

IGF2019 BPF IoT, Big Data, AI Survey
Compilation survey feedback