IGF 2018
Best Practice Forum on IoT, Big Data, AI

IGF 2018
Best Practice Forum on

Internet of Things
Big Data
Artificial Intelligence

BPF output report
December 2018

Disclaimer:
The IGF Secretariat has the honour to transmit the paper prepared by the 2018 Best Practice Forum on IoT, Big Data, AI. The content of the paper and the views expressed therein reflect the BPF discussions and are based on the various contributions received and do not imply any expression of opinion on the part of the United Nations.

Table of Contents

Executive Summary

The IGF Best Practice Forums (BPFs) bring experts and stakeholder together to exchange and discuss experiences in addressing Internet policy related issues.

The BPF on Internet of Things (IoT), Big Data, and Artificial Intelligence (AI) was part of the IGF intersessional work programme leading into the 2018 annual meeting of the Internet Governance Forum (IGF) in Paris, France, on 12-14 November 2018. This report reflects the work of the BPF and is the result of a community-driven bottom-up and open process.

Devices, networks and applications used by billions of users around the world generate a vast variety and high volume of data. IoT, Big Data and AI play a critical role in connecting, analysing, and generating value from this growing amount of information. IoT, Big Data an AI discussions are present in many fields, in the on- and offline world. The BPF's focus is on where these technologies are used in consort in an Internet context and where Internet governance can play are role in stimulating further development and widespread use, as well as helping to avoid unintended negative side-effects.

The expectations on how IoT, Big Data and AI are going to contribute to solving complex problems and facing global challenges related to the environment, transportation, health, etc. are high and complement a fast growing list of examples of how they support individual Internet users' daily lives. There are however a large number of unknowns, potential impacts, risks, and social and economic implications that ask for guidance, measures and policies for managing the impact of applying IoT, Big Data, AI technologies.

Stakeholder dialogue is crucial to allow the Internet to embrace IoT, Big Data and AI to the benefit of all. Each stakeholder group offers a unique understanding of how these technologies impact daily life, how to balance innovation with potential risks, and how to make the best of the opportunities while seeking ways to mitigate unwanted side-effects .

The BPF identified existing platforms and communication mechanisms for stakeholder discussion and collected examples and good practices of how stakeholder cooperation can help to media problems, avoid issues and support the use of IoT, Big Data, AI in the Internet. They are listed in section IV of this report.

The BPF suggested two Best Practices regarding definitios of IoT, Big Data, and AI that could contribute to an efficient and effective stakeholder dialogue dealing with the IoT, Big Data, and AI in an Internet context:

> **#1 - Define your terms narrowly** so that it is clear for policy makers and stakeholders what aspects of these 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 technology (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.

IoT, Big Data, AI are powerful technologies and when combined they become even more powerful tools that can be used for good or evil. Using IoT, Big Data, AI in an Internet context, creates a number of Internet Governance challenges. The BPF discussion pointed amongst other to the cybersecurity of IoT devices, risks related to AI mass data processing, and potential threats to human rights, security and social cohesion. The BPF had extensive discussions about the necessity that they are and how these technologies could be applied and further developed in ways that reflect ethical considerations and human rights.

BPF identified Best Practices for stakeholder to take into account when discussing the use of IoT, Big Data and AI:

> **#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. This requires that users are aware of the benefits and risks deriving from these technologies.

#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 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.

IGF 2018 Best Practice Forum on

Internet of Things - Big Data - Artificial Intelligence

I. Introduction

1. The IGF BPF on IoT, Big Data, AI

One of the key outcomes of the World Summit for the Information Society (WSIS) was the Internet Governance Forum (IGF). The 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 13th annual IGF meeting takes place in Paris, France, on 12-14 November 2018.

The IGF Best Practices Forums (BPFs) bring experts and stakeholders together to exchange and discuss best practices in addressing an Internet policy related issue in a collaborative, bottom-up process. BPFs prepare their work in a series of intersessional discussions and a workshop at the IGF's annual meeting. The activities of the BPFs culminate in an output document including an understanding of global good practice, that is intended to inform policy discussions, standards development, business decisions, as well as public understanding, awareness, and discourse.

2. Framing the work of the BPF IoT, Big Data, AI

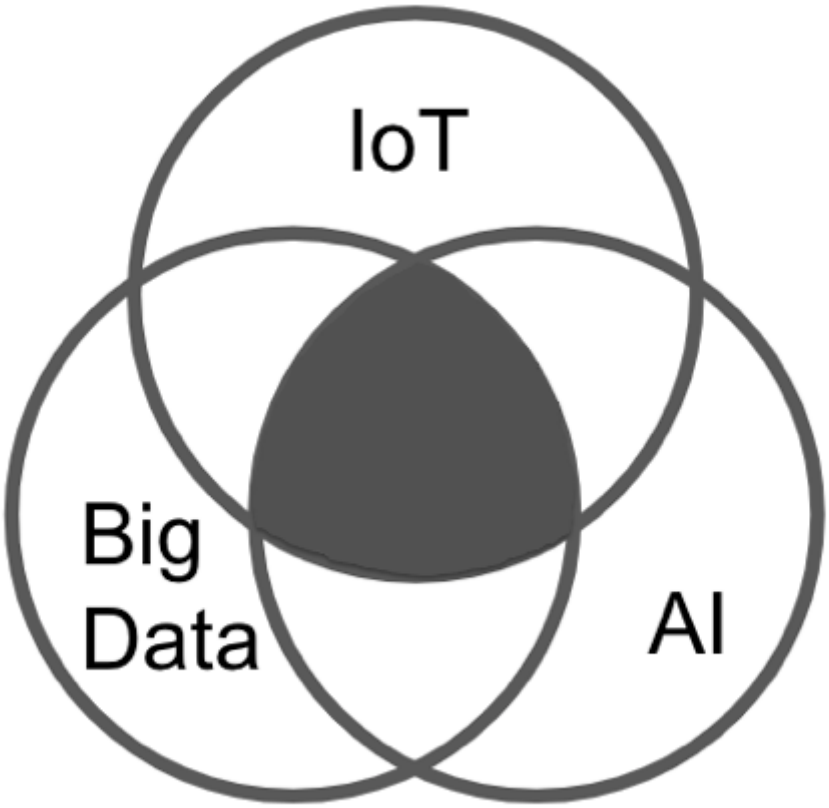
The BPF on the Internet of Things (IoT), Big Data and Artificial Intelligence (AI) aims to determine how combining these technologies can benefit Internet users and others around the

[1] IGF website: http://www.intgovforum.org

world, and what is needed to ensure that the benefits do not come at the cost of trust in society at large because of increase in (justified) concerns about affecting privacy or self-determination of people. It also examines how to address growing concerns about misuse and misunderstanding of emerging technologies.

Where IoT, Big Data, AI are being used in concert ...

Today IoT, Big Data, AI discussions are present in many fields, both in the on- and offline world. The BPF will focus on where these technologies meet in an Internet context, and how Internet governance can stimulate their development and widespread use, as well as help avoid unintended negative side-effects. Each of the three technologies are being used in many different ways in many different fields. The focus in this report is on where all three technologies are being used in concert. In other words, rather than try to cover all the issues 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.



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

While, already, there are multiple examples of benefits coming from IoT, Big Data and AI, the expectations about how these technologies will change our future are high: for example, by improving efficiency and cost saving, enabling better and more accurate decision-making and the discovery of specific data patterns, and complex cause and effect relationships, etc. IoT, Big Data, and AI can contribute to solving complex problems and facing global challenges related to the environment, transportation, health, etc., and will help achieve SDGs in ways that otherwise may not even be possible. Also on the level of the individual internet user there is an almost endless and growing list of examples of how new technologies and applications could help support daily life.

While the new technologies have the ability to help to tackle many global challenges and support people in their daily pursuits, there are a large number of unknowns, potential impacts, risks, and social and economic implications related to privacy and discrimination, inequality and infringement of human rights, etc.

Stakeholder Dialogue

Stakeholder dialogue should play an important role in identifying risks and seeking ways to mitigate unwanted side-effects, to understand how the Internet can further develop embracing IoT, Big Data and AI to the benefit of all.
Stakeholder debate and dialogue is required to help stakeholders to select, adopt and develop the right measures and policies for managing the impact of these new technologies on the society.

When considering the combination of the Internet of Things, Big Data, and Artificial Intelligence, the number and type of key stakeholders is even larger and more varied than in the case of traditional Internet governance.

They include the following groups, which in themselves are spread across different industry sectors:

- Researchers who develop new techniques;
- Engineers and developers who create, improve, and deploy solutions;
- Standards experts who craft international standards to foster adoption;
- Marketing teams who define how applications will be sold;
- Lawyers--in both businesses and government--who apply laws to technology;
- Regulators who apply existing rules or draft new rules for new use cases;
- Government policy makers who set policy goals;
- Consumer advocates who spot abuses and fight for remedies; and
- Diplomats and international organizations working for global approaches.
- Internet users, who are affected by AI through its mediation of their daily communications and information consumption (such as through delivery of advertising, news, and social media content through algorithms and profiling) and role in automated decision-making.

Each stakeholder group offers a unique and important understanding of how these technologies impact daily life, and how policy can balance innovation with potential risk. And within those stakeholder groups, it is important to recognise that those who contribute, for instance, to aerospace industry, or those contributing to personal health, or to domotics, will have different emphasis in terms of concerns and aims. They should be encouraged to collaborate as often as possible in order to manage the impact of these emerging technologies.

3. Objectives of the BPF output

The BPF document is intended to inform policy discussions, by describing different issues and reflecting on ongoing discussions in a format tailored to an audience of policy makers who do not necessarily deal with technology on a day-to-day basis.

The BPF aims to be a multi-stakeholder and multi-disciplinary platform to understand the wider context of IoT, Big Data, AI, for each stakeholder group, and discuss opportunities and threats related to the application of these technologies on the Internet, and ways to stimulate the positive or mitigate the negative, only then these new technologies can contribute to the benefit of all and support reaching the United Nations Sustainable Development Goals (SDGs).

The BPF identified a set of focus points for stakeholder discussion.

1. Explore the benefits and potential dangers of the use of IoT, Big Data, AI in an Internet context.
2. Identify existing platforms and communication mechanisms for stakeholder discussion on issues related to the use of IoT, Big Data, AI and the Internet;
3. Collect examples and good practices of how stakeholder cooperation can help to mediate common problems and issues and stimulate the use of IoT, Big Data, AI and the Internet to the benefit of all;
4. Identify how IoT, Big Data, AI can be used to reach the United Nations SDGs;
5. Identify the impacts on policies and regulations, policy making, of the application of IoT, Big Data, AI;
6. Start a discussion with stakeholders to highlight their roles and responsibilities and help focus attention on some of the most exciting opportunities and largest potential problems..

The 2018 BPF, as it is the first time a BPF is organised on these new technologies, is necessarily a fact finding exercise, and will focus on the first three points of the above list in order to start a discussion on a general principle on the use of these technologies to the benefit for all.

The 2018 BPF, as such, will be a sound basis for further discussion and strengthened stakeholder cooperation to stimulate the uptake and further development of these new technologies in such a way that they fully contribute to the benefit of all and the achievement of the SDGs.

4. Methodology and acknowledgements

This document reflects the work of the 2018 BPF on IoT, Big Data, AI . The BPF outcome document is the result of an open and iterative process during the months preceding the 2018 IGF meeting in Paris, France, 11-14 November 2018. 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[2], virtual webex meetings[3], and a BPF face-to-face meeting during the IGF in Paris. A short survey[4] conducted in June/July on the BPF and IGF mailing list helped the BPF in identifying potential topics for a BPF on IoT, Big Data and AI, and identify platforms and working groups that are discussing or well-placed to discuss IoT, Big Data, AI issues.

Acknowledgements

This BPF IoT, Big Data, AI output document is the collaborative effort of many.

We would like to recognise the IGF MAG for selecting IoT, Big Data, AI as topic for an intersessional Best Practice Forum in 2018; the BPF Coordinators Concettina Casa and Sumon A. Sabir for leading the BPF; the IGF Secretariat and BPF Consultant Wim Degezelle for supporting the work of the BPF; the Moderators and Panelists of BPF workshop at the IGF meeting in Paris; the numerous contributors to the document and participants to the BPF's deliberations on the mailing list, during the regular virtual meetings and at the workshop in Paris.

[2] https://intgovforum.org/mailman/listinfo/aiiotbd_intgovforum.org

[3] See meeting reports at https://www.intgovforum.org/multilingual/content/bpf-internet-of-things-iot-big-data-and-artificial-intelligence-ai

[4] Survey report https://drive.google.com/open?id=1L_x5BDSZvqb7PziPUdhksu5eaYbKV8C8

II. An Introduction to IoT, Big Data, and AI

1. Introduction

Devices, networks and applications used by billions of users around the world generate a vast variety and high volume of data. Technologies such as IoT, Big Data and AI play a critical role in connecting, analysing, and generating value from this growing amount of information. In this document, those technologies are therefore considered as a technological ecosystem where security, governance and ethics support the development of innovative services and applications impacting end-users daily life.

Thanks to the availability of big data and cloud computing, main players like Google, Facebook, and Amazon can classify and group user data by means of machine learning applications, to extract user profiles and models and apply them in a variety of contexts. Millions of images collected by online applications can be compiled and analyzed then used to "train" machine learning algorithms needed in fields as diverse as retail, security, and health care. Self-learning algorithms are also available on our mobile devices, influencing our choices, our purchases, and our behaviour, among other things. CDN companies such as Akamai and Cloudflare handle trillions of Web requests each day and apply machine learning to detect and block malicious attacks. Such algorithms also affect the news we consume through our social media feeds. Many of these algorithms work by collecting our personal information in order to make decisions about what to offer us.

The Internet of Things (IoT), as well as increasing the permeation of the internet into more aspects of our lives; provides an interface to feed data to, and receive data from AI in the cloud. Smart sensors distributed to several objects collect can distribute a huge amount of data over the Cloud. IoT devices generate a huge amount of data essential for much contemporary AI and big data.

2. Definitions

2.1. Internet of Things

While there is no universal definition, the Internet of Things (IoT) typically refers to "scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate,

exchange and consume data with minimal human intervention"[5] . Well known to the public are consumer IoT devices. They include everything from toasters, fridges and vacuum cleaners, to personal assistants and fitness coaches. They unlock our homes and keep the temperature inside regulated. They exist in our cars and our toothbrushes and our watches, and the use cases are only growing. There's also a vast amount of examples of IoT making an introduction in the public space and industrial IoT applications.

It is projected that IoT devices will number 38.5 billion in 2020, up from 13.4 billion in the year 2015[6].

While much public attention has been paid to consumer applications of the IoT, many of the most important and beneficial uses will be elsewhere.
Some existing and potential use cases that combine the IoT with Big Data and Artificial Intelligence include:

- Sensors for monitoring infrastructure (bridges, roads, sewers, water systems);
- Factory automation;
- Logistics and supply chain management;
- Medical treatment and home health care;
- Emergency warning systems;
- Crop optimization systems;
- Home security and crime prevention; and
- Personal health monitors.

When discussing the Internet of Things, it is critical to understand that the Internet has become more than just a communications network. It has become a computing platform as well. The simple model of the IoT where a device reports back to a single server has been replaced with an Internet architecture that includes secure gateways for protecting and managing the devices, Content Distribution Networks (often consisting of hundreds or even thousands of servers) that collect and cache data, layers of security, cloud computing data centers, and a range of edge computing services. For this reason it might make sense to refer to a "Cloud of Things," because that make clear that telecommunications networks are just part of the infrastructure that enables the IoT.

2.2. Big Data

Big Data can be defined as a set of data-processing applications, codes and platforms created to analyse high volumes, velocity and variety of data. Generating insights from complex and unstructured data sets, Big Data enables developers, businesses and governments to better

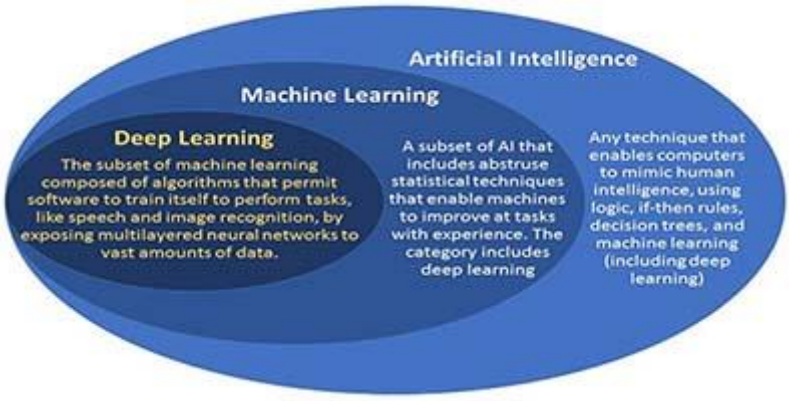
[5] https://www.internetsociety.org/resources/doc/2015/iot-overview
[6] https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020

scope and anticipate user experience and context of usage. As a supporting activity, data science provides standardized tools and methodologies to develop complex algorithms able to process and analyse such data streams.

While researchers and companies have been using computers to collect and analyze "Big Data" for more than five decades, the Internet of Things has fundamentally "changed the game." What's exciting about today's Big Data applications is that the amount of data being collected is not just massive--it's also changing rapidly: it is coming from widely-distributed locations (many of which are moving); it may come from a range of types of sensors; and it may be unstructured, messy, and full of noise or errors. The ability to collect and analyze data not only from sensors (like temperature or location) but also on the tone and emotional content of a tweet, an customer complaint, or a corporate email, could lead to unexpected insights and process improvements.

2.3. Artificial Intelligence

Artificial Intelligence refers to a set of theories, methodologies, approaches and practices that give computers or computing systems the ability to perform tasks that are associated with humans (intelligent beings). AI has been with us for over sixty years, and there are a number of theories and approaches that are included in the general discussion of AI; such as Machine Learning (ML) and Deep Learning (DL). Most of artificial intelligence used in practice and focused on by researchers and developers focuses on giving computers tasks commonly performed by humans. Some AI theory and practices focuses on creating computer systems that can learn and think like humans, and thus modelled on the way human beings reason, more like the AI we know from science fiction such AI, called "strong AI"[7] represents a minority of contemporary AI, although remains a focus of AI in media and contemporary discourse.



Source: cubicsol.com/deep-learning-machine-learning-ai/

[7] Searle, John R. "Minds, brains, and programs." Behavioral and brain sciences 3.3 (1980): 417-424. cogprints.org/7150/1/10.1.1.83.5248.pdf

The AI category includes sub fields that are sometimes discussed separately such as knowledge engineering and machine learning.

"AI traditionally refers to an artificial creation of human-like intelligence that can learn, reason, plan, perceive, or process natural language. These traits allow AI to bring immense socioeconomic opportunities, while also posing ethical and socio-economic challenges." (From Internet Society's AI/ML Policy Paper)

Machine learning is a particular approach to AI, and one of the most widely-used AI-related technologies used on the internet.
"Instead of programming the computer every step of the way, machine learning makes use of learning algorithms that make inferences from data to learn new tasks." (From Internet Society's AI/ML Policy Paper)

AI is already being used for tasks that many users may not be aware of, including email filtering, content personalization (such as Netflix recommendations), fraud detection, and speech recognition (such as Alexa and Siri). As the technology continues to develop and expand its applicability, users will likely interact with AI systems in greater capacities.

There is a great deal of confusion about Artificial Intelligence, in part due to confusion[8] about the term, which has been in use since at least 1956[9]. Since then it has been defined in many, conflicting ways.

At various times, "Artificial Intelligence" has been applied to almost every type of algorithm: Voice recognition systems; Image recognition systems; Decision support software; Factory robots; Machine learning; Autonomous vehicles (e.g. self-driving cars and drones); Cognitive computing; and MUCH more. Because of the exciting (and confusion) around the terms "artificial intelligence" and "machine learning" almost anything digital is being labelled "AI" or "machine learning." Indeed, the famous Gartner hype curve showed machine learning reaching peak hype in 2016[10].

2.4. How IoT, Big Data and AI come together

As the pervasiveness of IoT devices increases, so too does the likelihood that consumers will interact with dozens or even hundreds of IoT devices. Each of their devices collects huge amounts of data about their daily activities. Everything from heart rate, daily movements and routines, and even the layout of users homes can be tracked. This data is often compiled, sold, and used in very different ways than users may expect. This creates a perfect environment for

[8] For some useful cartoon examples: https://marketoonist.com/2017/09/ai.html
[9] http://agisi.org/doc/AGISI_DefinitionsIntelligence.pdf
[10] https://contently.com/2017/05/23/artificial-intelligence-hype-cycle-5-stats/

new AI applications and services, which rely on big data, to grow and evolve. As users adopt more IoT devices into their lives they are, often unknowingly, contributing data to future applications of AI and machine learning.

A practical example where the three technologies are used in synergy are Smart Cities, where through IoT devices you can harvest vast amount of datas that through AI could be used to develop predictive models to manage critical services such as public transportation, pollution monitoring, garbage collection, and others.

These are powerful technologies and when combined they become even more powerful tools, which can be used for good or evil. The BPF working group had extensive discussions about how loT, Big Data and AI could be developed and used in ways that reflect ethical considerations and human rights.

III. The key role of Internet Governance

1. Internet Governance Challenges

- **IoT Cybersecurity**
  IoT devices can be used to form botnets -- "networks of Internet-connected externally controlled devices" [https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/]. Once infected with malicious software, the devices and everything they are connected to can be compromised. The devices can be used to "infect" and disrupt entire networks, other users, and the Internet infrastructure at large. The 2016 botnet attack against Dyn, a DDoS attack that made thousands of major websites temporarily inaccessible, used IoT devices to facilitate the attack [https://www.internetsociety.org/blog/2016/10/trust-isnt-easy-drawing-an-agenda-from-fridays-ddos-attack-and-the-internet-of-things/].

  It is critically important that IoT device developers consider security at the earliest stages of development, i. E. implementing the principle of security / safety by design. But it is equally important that users understand what is at risk and what they can do to protect themselves and others from attacks through IoT devices. It will take mass education of developers, consumers, policy makers, and vendors to ensure that the Internet is protected from IoT attacks. Groups such as the Internet Society and Consumers International are already working together to ensure industry and consumer groups improve the overall security and privacy of IoT offerings, and to make sure consumers have products or services that are secure and privacy-respecting [https://www.internetsociety.org/blog/2018/06/a-partnership-to-tackle-growing-risks-in-a-connected-world/]. The IGF is another excellent forum for stakeholders from all over the world work together to secure IoT before another mass botnet attack is launched.

- **AI mass data processing**
  Some AI techniques, like machine learning, make use of massive amounts of data to train the system in producing significative answers and decisions. This creates three problems:

  "**Data dominance"**. Refers to the phenomenon where big companies like Google or Facebook (or large countries[11]) gather massive amounts of data, giving them an advantage over smaller competitors in the AI field.[12]

[11] https://foreignpolicy.com/2017/09/08/china-is-using-americas-own-plan-to-dominate-the-future-of-artificial-intelligence/ and https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/
[12] https://www.datasciencecentral.com/profiles/blogs/what-makes-a-successful-ai-company

Data bias. The problem of the quality of the datasets used to train the system: if data are incomplete, inaccurate, or reflect social inequalities, the answers and decisions taken by an AI application might be incomplete, inaccurate, flawed or discriminatory. Therefore accurate information needs to be fed into the system.

Ethical Decision Making. AI systems are wired to output the most logical solution to problems, but those solutions may not always be the most ethical. It is critical that programmers build ethical considerations into AI algorithms.
(example: BBC video AI & ethics - self driving car:
https://www.facebook.com/bbc/videos/2095617507120104/)

Anonymization. A privacy related issue: data used to train the systems must be rendered anonymous for preserving the privacy of users, but if too much information is omitted the data might be useless, so investigating the right tradeoff is important. Another issue lies in de-anonymization strategies used to re-identify users.

Transparency. AI systems can output solutions without clear justification, or understanding, of how and why it reached that conclusion. Consumers may not have any knowledge about why a system is interacting with them in a certain way. For this reason, developers must be as transparent as possible about how their algorithms are built. This will allow the public to serve as a check on any AI system making "bad" or wrong decisions.

- **AI threats to human rights, security, and social cohesion**
  AI can pose threats to human rights, security, and social cohesion. There is the legal issue of whom to consider liable for the errors or shortcomings of an outcome where an AI is used. Another concern is about improper use of AI: it might be easier to forge audio and video media and spread fake news; AI can guess more accurately an individual's tastes thus exacerbate filter bubbles; and new cyber attacks involving AI could be deployed.

  Another crucial aspect is **intelligibility***:* in some AI technologies like deep-learning, there is such a level of complexity that it is not possible even for their developers to know why and how the AI has come to the final answers or decisions. But this can create a huge problem when an AI is used to make decisions or get answers in critical situations where the outcome has a great impact on an individual's life, thus it's important to identify these situations and restrict the use of unintelligible AI's technologies in these scenarios. Therefore the EU GDPR regulates decision making based solely on AI in Art. 22 (1) as follows: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

Moreover AI technologies can have a dramatic impact on the labour market: they can increase productivity, reduce costs, and create new jobs; but they can also replace old ones, create new inequalities, and bring a decrease in wealth distribution. It is crucial to understand how and which jobs are automatable, and on what extent AI can replace human labour. It is important to discuss retraining programs to enable workers to enter new careers or to be able to fully exploit this new technology.

- ***Positive Impact on economies and Innovation***
  AI depends on Big Data to function. As the demand for "intelligent" technologies increases, so too will the demand for data. This may incentivize companies to collect more data about users, raising the risk of oversharing user information at the expense of privacy and security.

2. Proposed Best Practices

Regarding definitions of IoT, Big Data, and AI

#1 - Define your terms narrowly
The fact that the term "Artificial Intelligence" and "Internet of Things" has and can be used in so many ways make it essential that policy makers, business leaders, non-governmental organizations, and users of technology make clear what aspect of these technologies they are discussing. Not doing so can lead to sweeping generalizations or proposals meant to address a problem with a narrow technology or specific application that could have a range of unintended consequences. Worse, by conflating dozens of different technologies and hundreds of different applications into one conversation it is likely that the "fear factor" caused by science fiction depictions of SkyNet and other AI scenarios will cause discussions to lose focus.

#2 - Be ecumenical about technology (or "Strive to be technology-neutral")
Because technologies are changing so quickly and because potential problems with a specific applications 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 practice is usually to focus on what an application DOES not on how the technology DOES IT.

Regarding uses of IoT, Big Data, and AI

#3 - Collaborate

It is critical that government officials, technologists, civil society, academics, and others work together 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

The people developing and deploying systems, products, and services that leverage loT, Big Data and AI should take ethical considerations and human rights into account from the outset in the development, deployment and use phases of the life cycle. This requires that users are aware of the benefits and risks deriving from these technologies

#5 - Watch out for bias and incomplete data sets

Users of IoT data must realize that they data they collect may reflect only a small subset of the "real world." This may be due to the Digital Divide. It might be due to national regulations that restrict the export of consumer data. It might be 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, companies and governments should recognize the limits of the data and Big Data analysis. The Obama Administration released two very important reports[13] that addressed "data discrimination" and provided useful recommendations.

#6 - Make privacy and transparency a policy goal and a business practice

In a sector evolving as rapidly at the Internet of Things, it is important that potential problems be recognized before they become serious. Companies that develop new applications that collect and use data without informing their customers (or do not reveal all the ways in which they are using their data) often face a serious loss of reputation and trust when their business practices are revealed (usually by outside researchers or by current or former employees). More and more Internet companies are publishing 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. Transparency is one of the most effective ways for companies to nurture trust.

[13] https://obamawhitehouse.archives.gov/blog/2016/05/04/big-risks-big-opportunities-intersection-big-data-and-civil-rights

#7 - Ensure systems are adequately secured before they get to the market

Over time, and leading to a very high level pace of innovation, industry has been led by a drive of shortest possible "time to market". Whereas this has led to high pace of innovation, this has also led to failures of systems, and flaws in systems that will still haunt us in the years to come, as long as those systems with inherent flaws are in use within our networks. By making industry responsible for system failures and vulnerabilities, the price of such failures and vulnerabilities are likely to become more explicitly more part of the consumer price of the products. In many ways this is comparable to invoking a "taxation" on eco impact of household appliances, etc. 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

There is a common assumption that the biggest companies will be the biggest winners when it comes to the IoT, Big Data, and AI. Yet, already companies like IBM are building systems that enable the smallest companies to apply leading-edge solutions to their problems. The growth of edge computing[14] 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.

3. role of Internet Governance with regard to IoT/Big Data/AI

Why do these technologies matter to IG?

Key role of Internet Governance with regard to IoT/Big Data/AI

- Stimulate the development of new applications of these technologies on and using the Internet, to the benefit of all;
- Provide ways to highlight and disseminate information about new tools and applications;
- Avoid risks and threats emerging from the further developing use of these technologies;
- Make sure that business or government practices do not slow down the development and new applications of which all can benefit;

[14] https://www.economist.com/business/2018/01/18/the-era-of-the-clouds-total-dominance-is-drawing-to-a-close

- Caution towards decision making based solely on AI and machine learning (ref. to GDPR recital 71);
- Provide ethical guidance with regards to health, defense, cybersecurity and privacy usage;
- Facilitate access to skills and knowledge, inclusion;
- Facilitate conversations among relevant stakeholders, including creators of new technologies and users, to discuss ways to balance innovation and potential risk through policymaking.

From G20 Digital Economy Ministerial Declaration (Aug 2018)[15]

> *We encourage countries to enable individuals and businesses to benefit from digitalization and emerging technologies, such as 5G, Internet of Things (IoT), artificial intelligence (AI), distributed ledger technologies, by: i) considering*
> *appropriate policy approaches and flexible legal frameworks that create an environment that empowers entrepreneurs and fosters research, innovation and competition; ii) promoting the application of emerging digital technologies in manufacturing, agriculture and other vital areas; and iii) We face the challenge of capturing the benefits of digitalization to improve productivity that may lead to new business models including sharing economy, economic development, and the realization of broader taking into account the challenges that these new technologies may pose in terms of privacy and security, among others, and the opportunities to improve quality of life and foster economic growth.*

[15] *https://g20.org/sites/default/files/media/g20_detf_ministerial_declaration_salta.pdf*

IV. Stakeholder cooperation - Best Practices examples and experiences addressing Internet Governance challenges of IoT, Big Data and AI.

Existing platforms and working groups

- IGF DC IoT document on global Good Practice from a multistakeholder perspective https://www.iot-dynamic-coalition.org/wp-content/wp-content/uploads/sites/3/2018/05/IoT%20Good%20Practice%20Paper%202017.pdf

- Internet Society's Enhancing IoT Security project in Canada -- https://iotsecurity2018.ca/ and IoT for Policy Makers brief -- https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/

- Internet Society's guiding principles for AI: https://www.internetsociety.org/resources/doc/2017/artificial-intelligence-and-machine-learning-policy-paper

- Canadian government's multistakeholder conference on AI: https://www.itworldcanada.com/article/canada-to-host-multistakeholder-conference-on-ai-in-montreal/410456

- The Internet Society - https://www.internetsociety.org/iot/
    a. The Internet Society and the IETF https://www.internetsociety.org/resources/doc/2017/artificial-intelligence-and-machine-learning-policy-paper/
    b. The Internet Society ;Enhancing IoT Security; project in partnership with the Canadian government. Link: https://iotsecurity2018.ca/ .
    c. ISOC (in particular Canada and France chapters on IoT) and connectafrica@isoc.org / ogu@isoc.org , ISOCBB
    d. https://connect.internetsociety.org/communities/community-home/digestviewer?communitykey=03916595-8718-43b9-b457-44c28d329322&tab=digestviewer
    e. https://connect.internetsociety.org/communities/community-home/digestviewer/viewthread?GroupId=589&MessageKey=fb94b0bd-9d22-48cd-8c57-d8222388312a&CommunityKey=03916595-8718-43b9-b457-44c28d329322&tab=digestviewer&ReturnUrl=%2fcommunities%2fcommunity-home%2fdigestviewer%3fcommunitykey%3d03916595-8718-43b9-b457-44c28d329322%26tab%3ddigestviewer

- World Economic Forum
    a. https://www.weforum.org/communities/internet-of-things-and-connected-devices-47a97762-c4f8-427d-9194-bb998bbe72bf
    b. https://www.weforum.org/whitepapers/internet-of-things-guidelines-for-sustainability

- McKinsey Global Institute, Michael Chui https://www.mckinsey.com/industries/high-tech/our-insights

- OECD
https://www.oecd-ilibrary.org/science-and-technology/oecd-science-technology-and-industry-scoreboard-2017_9789264268821-en

- U.S. NIST https://www.nist.gov/publications/nist-big-data-interoperability-framework

- EU / France :
Cyber security regulator ANSSI, together with German regulator and EU agency ENISA (on security and certification)

- EU : France DPA CNIL, along with EDPS and EU related working groups

- High level group of experts on Artificial Intelligence of European Commission
https://ec.europa.eu/digital-single-market/en/high-level-group-artificial-intelligence

- IOT, Università La Sapienza di Roma - prof.ssa Chiara Petrioli

- AgID/OECD working group on E-Leaders Thematic Group on Emerging Technologies (AI; Blockchain) focused on public sector

- Politecnico di Torino (AI Ethics, brain simulation, face recognition)

- INRIA - AI (Nozha Boujema) https://www.inria.fr/en/news/news-from-inria/i2-drive-at-the-universite-paris-saclay https://www.universite-paris-saclay.fr/en/news/i2-drive-a-new-convergence-institute-for-universite-paris-saclay

- IGF DC IoT
http://www.iot-dynamic-coalition.org

- RIPE NCC https://www.ripe.net/participate/ripe/wg/iot

- AIOTI https://aioti.eu/

- The UN Secretary-General's new report on emerging technologies: http://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies.pdf

- The report on artificial intelligence by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression https://freedex.org/wp-content/blogs.dir/2015/files/2018/10/AI-and-FOE-GA.pdf

V. Next Steps ?

The BPF had an open exchange on next steps at the BPF workshop during the IGF 2018 in Paris. The full report of the workshop is available as an annexe, transcript and recording are available here. The discussion focussed on a way forward in case the BPF would continue and how the IGF ecosystem could help to make progress on the issue.

Way forward/potential next steps

During the discussion several speakers suggested including more specific examples of the use of IoT+Big Data+AI, especially in areas such as healthcare, environmental protection, and infrastructure. A number of speakers stressed the need to provide specific ways to enhance trust in technology.

How might the IGF ecosystem make progress on this issue?

A recurring theme was the need to attract more participants (with more varied views and experiences) to the effort to draft and revise the Best Practices Forum report on Iot+Big Data+AI. Better communications with the national and regional IGFs could help recruit talent and comments. One questioner stressed that it seemed that participants in some of the IGF 2018 sessions on AI and IoT did not know about the BPF.

Report of the BPF IoT, Big Data, AI session at the IGF 2018

IGF 2018 BPF Internet of Things (IoT), Big Data, Artificial Intelligence (AI)

Wednesday 14th Nov, 11:50-13:20 CET
Paris, France

Transcript / recording:
https://www.intgovforum.org/multilingual/content/igf-2018-day-3-salle-xii-bpf-artificial-intelligence-big-data-internet-of-things

Session Structure

1. Welcome and Introduction to the BPF IoT, Big Data, AI
   Concettina Casa, BPF Co-facilitator
   Sumon A. Sabir, BPF Co-facilitator
   Wim Degezelle, BPF Consultant

2. IoT, Big Data, AI in an IG perspective: Experiences and Best practices
   Moderator: **Alex Comninos**

   Discussion catalysts :
   - **Nobuhisa NISHIGATA,** OECD
   - **Imane Bello,** Sciences Po Lecturer, Human Rights & AI
   - **Taylor Bentley,** ISED, Canadian Government
   - **Peter Micek,** Access Now
   - **Michael R. Nelson,** Cloudflare

3. Open Issues and Next Steps?
   Moderator: **Maarten Botterman**

4. Summary & closing remarks

Session Rapporteur: **Michael R. Nelson**

Key messages of the discussion

1. There is a need to focus. Rather than discuss all of artificial intelligence, focus on machine learning and how it can be used to create insights from the data generated by the Internet of Things. The report should cover both the benefits and the risks associated with these three technologies.

2. More than ten speakers commented on the need for applications of IoT+Big Data+AI to be trusted and "trustworthy" (and how many different steps are needed to foster trust). These include protecting privacy and personal data, enhancing cybersecurity, being transparent about problems, respecting human rights, giving users alternatives if they find one service or application unsatisfactory, "design for safety," and "design for diversity."

3. A number of speakers and members of the audience highlighted the role that education, training, and capacity-building can play in promoting new and better use of emerging technologies like IoT and AI.

Summary of the discussion

Most of the session was devoted to conversation between the "discussion catalysts" onstage and members of the audience. There was time for more than 15 questions and comments including at least five from remote participants. There was support for added emphasis on: (1) Diversity and multi-stakeholder processes that could shape the development of IoT+Big Data+AI, (2) Education can help address some of the fear about emerging technologies like IoT and AI, (3) NGOs and other groups have a key role to play in working to ensure that applications of IoT+Big Data+AI are not used in ways that violate human rights, and (4) Capacity-building can help develop technical skills and improve policy-making, especially in emerging economies. One questioner stressed the need for governments and the United Nations to do more to shape the use of the IoT and AI. Other speakers disagreed.

Way forward/potential next steps

During the discussion about the next version of the BPF report, several speakers suggested including more specific examples of the use of IoT+Big Data+AI, especially in areas such as healthcare, environmental protection, and infrastructure.
A number of speakers stressed the need to provide specific ways to enhance trust in technology

How might the IGF ecosystem make progress on this issue?

A recurring theme was the need to attract more participants (with more varied views and experiences) to the effort to draft and revise the Best Practices Forum report on Iot+Big

Data+AI. Better communications with the national and regional IGFs could help recruit talent and comments. One questioner stressed that it seemed that participants in some of the IGF 2018 sessions on AI and IoT did not know about the BPF.

Additional questions

- Estimated total number of participants:
  At least 60 people
- Estimated total number of women and gender-variant individuals present:
  25 people
- To what extent did the session discuss gender issues?
  During the question and answers session, several members of the audience and speakers stressed the need for diversity and inclusion in developing and deploying new technologies and in crafting policies to shape and promote them.

Background and information sources

General or mixed

- Mike Nelson, Cloudflare, speaking notes ITU panel 'AI-IoT-Cybersecurity' (see mailing list 25 July) https://drive.google.com/open?id=1PxAGq5iTh1nbVHEx_KGt4PMZpAUwnn_B
- An Overview of National AI Strategies - https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd

Artificial intelligence

- IEEE AI and ethics initiative https://ethicsinaction.ieee.org/
- The Montreal Declaration for a Responsible Development of Artificila Intelligence https://nouvelles.umontreal.ca/en/article/2017/11/03/montreal-declaration-for-a-responsible-development-of-artificial-intelligence/
- The Toronto Declaration on maching learning systems launched by AccessNow and Amnesty International at RightCon in 2018 https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf
- AI Now Institute https://ainowinstitute.org/
- Oxford Internet Institute https://www.oii.ox.ac.uk/blog/tag/machine-learning/
- Harvard Berkman Center and ITS Rio initiative https://aiandinclusion.org/
- Kialo on Twitter - https://twitter.com/KialoHQ/status/1006532796171669504
- Internet Society Artificial Intelligence and Machine Learning Policy Paper: https://www.internetsociety.org/resources/doc/2017/artificial-intelligence-and-machine-learning-policy-paper/
- BBC video AI & ethics - self driving car: https://www.facebook.com/bbc/videos/2095617507120104/
- Artificial Intelligence at the service of citizens - AGID, The Agency for Digital Italy https://drive.google.com/file/d/1ZmMp8A0rhpyX0ffqt0GdkQOWBwTm7peC/view?usp=sharing
- Alex Comninos & Martin Konzett, *FABRICS: Emerging AI Readiness*, https://vous.ai/FABRICS-Emerging-AI-Readiness-Comninos-Konzett-First-Edition-2018-LQ.pdf

IoT

- "IoT Policies towards 2025, Benefitting from the opportunities", Maarten Botterman, November 2015
- https://drive.google.com/open?id=1YWHQcjQllaMRXWiMamkl7-d_L01Ja_s3
- Enhancing IoT Security -- https://iotsecurity2018.ca/
- Internet Society IoT Security for Policymakers: https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/

Big Data

- *'Data is a fingerprint': why you aren't as anonymous as you think online* - https://amp-theguardian-com.cdn.ampproject.org/c/s/amp.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy