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

I. Promising applications and developments

1.a. Which applications and developments that combine IoT, Big Data and AI excite you most ?

- Autonomous Vehicles requires IoT performance and a little of IA or none. Despite this, the monitoring of real-time vehicles requires BigData processing (for example with Hadoop) and a little of IA for Traffic Lights and other traffic control computarized smart systems. BMW is using this: https://www.bernardmarr.com/default.asp?contentID=1274 and Google also: https://datafloq.com/read/how-autonomous-cars-will-make-big-data-even-bigger/1795?amp-content=amp In the future, Routers will continue to become more secure and smarter, Decrease in air pollution will be possible by technology. So IoT is the priority. BigData is applicable only to a short portion of the applications in the future. IA will be more applicable than BigData in the short-term.
- None
- eHealth devices allowing preventing of diseases
- I am not exited at all. On the contrary - there are so many real threats to people.
- Pcloud
- recommendation tools for accessing media contents
- Smart assistants (e.g.Alexa, Google home etc)
- Smart watch. Smart watch may connect to mobile phone and record user's behaviors, health data, locations. For example, Apple Watch, it can connect to mobiles, web services, https://www.apple.com/apple-watch-series-4/
- The Internet of Intelligent Things (IoT, Big Data and AI)has the ability to breakdown massive quantities of information coming and going through devices. The most effective part concerning this is that since the entire process is machine and software-driven, it will be performed without any human intervention that makes it error free with improved accuracy rate.
  The best example of AI and IoT with success operating together is self-driving cars by Tesla Motors. Cars act as “things” and use the facility of AI to predict the behavior of cars and pedestrians in various circumstances. Moreover, all Tesla cars operate as a network. Once the intelligence is set on one automotive it cascades to the rest of the automotives.
- Algorithms /AI because if the Government wishes to use AI in big projects and ongoing monitoring functions and or to sustain life. Next generation will need to be aware on the impact.
- Everything, but my interest is mostly in medical technology and the ability to scan and diagnose.
- Google and facebook
- 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.
- We, as FIOT-LAB, had recently deployed a flood-alarm system (FAS) in a village called “Li Xing Cun”. The FAS includes 4 monitoring systems (to collect the data of water level, water speed, local rainfall, wind speed, local humidity in air and soil, images of ground topography, images of river), and 1 IoT cloud platform to perform data analysis (deep learning of data collected) and to set off flood alarm in advance.

For detailed information, please refer to the following link:
http://www.fiot-lab.org/cn/?p=news_content&id=26144

-

1.b. Why are you excited about these applications or developments?

- Because my studies in Computer Engineering and my complementary studies in Network engineering and the applications that are right now being developed in my city.
- Mix of medical improvement and transhumanism
- I am not exited.
- because it is quite easy to use.
- because it could transform mass media into personalized media
- Smart assistants enable new use cases for the Internet, or makes current one more efficient. E.g. a smart light turned on by your phone is not much different than using a switch on the wall. But when you can use your voice the use case for smart lights becomes more appealing. It won't replace the keyboard, but for some actions it will reduce "latency" between brain and action, thereby making those actions more appealing.
- I've seen some advertisement in Hong Kong. The insurance company persuade people to purchase their health insurance solution, and they will give you a free, new Apple Watch. Insurance may ask users to provide their health data or users may decide to give data to doctors or insurance company. Region: Asia-Pacific stakeholder group: Academia
- Improved Customer Satisfaction
  Increased Operational Efficiency
  Predictive Analysis and Maintenance
  Improved Accuracy Rate
  Error free

  For example, ATM withdrawals, e-commerce transactions and on-line payments are vulnerable to high risks of fraudulent activities. With the combined power of human understanding and IoT machine learning and Robotic Process Automation (RPA) techniques of AI, potential frauds will be taken into consideration in advance, therefore preventing any loss of cash.
- Indeed, if IOT is already complicated to understand and even to understand some benefits that it is producing, how much more is the operations of AI. And, we do not want AI to remove feeling of ownership from human beings to do something or own something in terms of performance.
- This makes a big difference to medicine and patient care.
- Because of my interest on computer science
- We are entering the next generation of social media/network. In the future, we will not only use our mobile phones to connect with each other, but will increasingly rely on wearables to enhance our social networking experience. Devices that will help increase our mobility, our connection and interaction with each other, will pave the way for new social connections globally. Globalised Social Networking is happening on worldwide scale, and this is happening at grassroots level from the most remote villages to government bodies.
  To support this social need, devices need to be faster, smaller, smarter, and powered by equally small and smart energy sources, and devices need to have its own computational "brain" (AI-edge algorithms). Advances in IOT, AI and Big Data will be the bright new future powering up Globalised Social Networking.

- The application of FAS enables the local residents to be evacuated earlier before the flood come, and so as to reduce lost of precious properties and even human life. And combining IoT, big data and AI is going to do the job more accurately and timely, especially in the future.

1.c. Are you aware of any best practices or promising initiatives that could further improve this application or promote its uptake and use?

- Yes, bringing cowork meetings locally, motivating business incubators. Talking about this in present with examples and motivate developers and enthusiasts with possible applications and let the imagination fly.
- No
- Yes, mainly with regards to ethics
- N/A
- yes. EBU is working on many projects in this field, such as Eurovox and PEACH
- Mozilla has a smart assistant project that is focused on understanding diverse english accents.
- Yes. For example, how people can sure the insurance company would not abuse data or sell data as commodities.
- According to Microsoft's new report IoT Signals, "IoT is creating opportunities to leverage more advanced cloud and networking technologies". The era of the IoT and AI can bring a modification to existing processes for good. As automation and in-depth analysis work hand in hand, industries and businesses can reap the benefits of growth, while making immense profits. The necessity of the hour is to make higher strategies for utilizing IoT and artificial intelligence for a much better future. For example, IoT appliances (such as smart fridges or smart Television) tend to remain in service for much longer, and should be able to function even if their manufacturer goes out of service. Blockchain is for powering crypto currencies like bitcoins promises to reduce costs and establish trust, but faces challenges like the speed of processing transactions.
- Not at this stage, but I understand through MAG meetings, a group is working on one.
- The medical fraternity is meeting regularly and conducting workshops to bring members up to date.
- IoT,AIBP mailing list
- There are now new startups focusing on platform technologies like new edge computing chip and edge computing algorithms, new energy harvesting chip+power management control modules, new wearable devices.
- 1) Lowering the cost, especially the initial cost related to training the AI for imaging analysis. 2) It is necessary to explain to the people in the village that this FAS is not accurate in the very beginning and need to be trained for a certain period.
-

1.d. Are you aware of any practices or issues that hinder this application's further uptake and use?

- https://ongrin.com/
  Footbot Air Quality Monitor.
  Kuri Mobile Robot
  Flow by Plume Labs Air Pollution Monitor
  Philips Hue Bulbs and Lighting System
- No
- ToS abuse
- n/a
- Main problem is the respect of the privacy of the users, that it's quite impossible when you have to pass through internet platforms.
- Accuracy. Voice recognition might be, lets say 85% accurate, which might be acceptable for some use cases (like switching on lights), but might hinder adoption of the technology for e.g. dictating email. Other issues includes privacy due to active microphone.
- I hope I will see how companies (private sectors) to follow the GDPR or how to use customer data with privacy protection or discrimination issues.
- - The future of IoT will have to depend on decentralizing IoT networks.
  - Connecting numerous devices will be one of the most important challenges of the future of IoT, and it'll defy the structure of current communication models and the underlying technologies.
  - When networks grow to join billions and hundreds of billions of devices, centralized brokered systems will turn into a bottleneck.
- Drones to supply medical to remotes islands of Vanuatu. Somehow it stops due to conditions of its operations related to national airline flying, daily routine and the geographical distance itself.
- None except inadequate training.
- No
- Security/privacy issues with social networking data transmitted through these devices. Hacking energy harvesting devices, edge devices.
-

II. Feared applications and developments

2.a. Which of the applications and developments that combine IoT, Big Data and AI do you fear the most?

- Little cameras. Relevance to pedophile, security, privacy. Companies involved, be careful with surveillance at protocol level. IA also affecting our lives: Autonomous vehicles, Robot Surgery Remotely, Armed drones. And how they could be hacked easily depending on the protocols involved. So security by default is important, and AI audit is relevant (for bad decisions for example killing people in case of Autonomous Vehicles)
- Abuse of health data
- Robots acting like humans and able to have emotions; software ID chips implants in humans
- I can't identify any
- the same mentioned above.
- Surveillance and the inability of opting out. IoT is essentially sensors, and not knowing which sensors track you, and how they can collerate using Big Data to profile me is terrifying. We have private mode in our browsers, and the notion of cookies are increasingly well understood by the broader public. But what constitutes "private mode" in an IoT world?
- Facial or any bio-recognition or biometrics technology in government surveillance. For example, Beijing, China. Use bio-ID with their social credit system and transportation, national security system. https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report
- · Cloud Attacks
  · AI-Built Security Issues
  · Botnet Problems

  Other security concerns include creating strong user authentications, tracking and managing each IoT device and securing endpoints for eachIoT device.
- AI's that will supplement love life for married couples. This can be abused and cause disaster it is is promoted in a small islands states but especially a christian country like Vanuatu. https://www.youtube.com/watch?v=oKR6OJlF77o
- Flying on the Max is scary
- Facebook and Google
- Security and privacy issues related to our data shared through social networks, IOT platforms and through the air (energy harvesting).
- Face recognition system and its own security level.
-

2.b. Please explain why you fear this application or development.

- First of all. Because machines working at our service, the most we use for crucial things in our life, the most dangerous it becomes. On one hand, Pedophile and Privacy concerns are real.

So we need to keep attentive to IoT security. On the other hand, the quantity of people dying because of machines will increase no matter what we do, is a reality, We need to put our lives the most secure possible, so avoiding bugs, and making good tests, with IA in priority in this case.

- Abusing health data could lead to vast breaches of privacy and human exploitation
- Because IoT, AI can modify and programme human behaviour and emotions; loss of expertise and experience; continuous, dependence on electricity or other power source(s)
- n/a
- because if it is developed without a guaranteed 100% respect of privacy could be transformed into the most powerful tool for controlling citizens and to twist democratic processes.
- impact on my freedoms and rights
- I am in Taiwan and some of my friends in Hong Kong. People in HK are running anti-extradition bill related protests. They fear China's government will use their facial recognition to find them or punish them. so they wear a mask. I support Taiwan is an independent country. That against China's political perspective. I am afraid my personal safety. I am worried about Lee Ming-Che event will happen to me. https://www.hrw.org/news/2019/03/18/taiwanese-activist-risk-chinese-prison
- A large amount of information that will run the IoT will be stored within the cloud. It's possible that cloud providers are going to be one of the principle targets during this kind of war. Cybersecurity continues to be under-resourced compared to the potential scale of the threat. Though the threat magnitude of ransomware has already fully grown thirty five times over the last few years with ransom worms and different types of attacks, there's more to come. IoT botnets will direct huge swarms of connected sensors like thermostats or sprinkler controllers to cause damaging and unpredictable spikes in infrastructure use, resulting in things like power surges, harmful water hammer attacks, or reduced availability of vital infrastructure on a city or state-wide level.
- It is much more to do with religion and also traditional ways of living that the nation is promoting. Living a Vanuatu way and life.
- It seems that there is confusion on development and training
- Users data collection
- Private information leaked. Think Facebook's recent privacy/security issues.
- Unlike the system for monitoring the nature of water/rain data, the face recognition system monitors and collects human's facial ID, if the security level is not high enough, then it is exposed to hackers.

2.c. Are you aware of any best practices or promising initiatives that could address your concerns and improve your trust in the applications and developments you mentioned in question 2.a.?

- Google Self-driving car are an example of technology being audited a lot. They made tests with possible edges of decisions in machine level.
- No
- Medical ethics / enforceable principles (legally : competition law / breach of contract)
- n/a
- Yes. there are many projects and applications, like Journalism Trust Initiative of Reporters without borders or the research project SoBigData of the EU
- No

- 1. California Considering Banning Facial Recognition Devices for Police Software
  https://interestingengineering.com/california-considering-banning-facial-recognition-devices-for-police-software
  2. Opinion: Don't Regulate Facial Recognition. Ban It.
  https://www.buzzfeednews.com/article/evangreer/dont-regulate-facial-recognition-ban-it
  3. Facial recognition tech is creeping into our lives – I'm going to court to stop it
  https://www.theguardian.com/commentisfree/2019/may/21/facial-recognition-tech-court-south-wales-police-face-scanning-consent
- · Usage of single cloud provider
  · Automated vulnerability detection and complex data analysis.
- No, I don't think so
- Not really
- Not yet
- Private information leaked. Think Facebook's recent privacy/security issues.
- 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 shall be a standard of security level that the human's bio-ID collecting and analyzing system.
-

III. Policy approaches enhancing the use of IoT, Big Data, AI

3.a. 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.
- None
- Privacy / contract law / competition and consumers law. EU region
- n/a
- the ethical initative 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. There 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. We at China-FIOT Lab are taking up the leadership to form AI+IOT standards in industry nationwide. As a government linked non-profit Organization, we could like to take on a more active role in international leadership of setting such standards and guidelines. We are a good participant for drafting such white paper and standards as we have a lot of experience in landing AI-IOT-Big Data projects in China testbed (the world's largest IOT market) and always reiterating and improving best practices.

3.b. Please provide more detail and explain why you consider them successful or unsuccessful in addressing your concerns in relation to the use of IoT, Big Data, AI applications.

- I think ethics are involved, so following rules don't work this time. We need to consider lots of factors. and is impossible to represent by law.
- They are successful but should be quite stronger in particular competition law and consumers law
- n/a
- a critical mass of one or more world region is needed to introduce decision on A.I. ethics. cannot be an initiative of a single state.
- badly defined AI. AI has been around for a while, so more suitable to the the UN LAWS approach of talking about decision making by autonomous systems.
- They may use some technology with personal identification, for example, RFID in electronic ID card (eID). When people get into a store or bus, it will know some details of customers, gender, age, medical records. Then they may provide a customize solution or discount for customers. Or the eID connect to your bank account, every consumption will deduct from the bank account directly. That might be convenient but full of risk. Maybe AADHAAR system is an unsuccessful application. India government record many details, even fingerprints, other bio recognition, and connect to the bank account in their database. But some people met fraud and lost their money.
  News:Ex-banker warns about growing Aadhaar scams, here's how you can save yourself from being tricked
  https://www.indiatoday.in/technology/news/story/how-to-save-yourself-from-aadhaar-scams-1416910-2018-12-25
- · Standard for handling unstructured data to be developed.
  · New technologies are slowly adopted.
  · Many IoT Systems are poorly designed and implemented.
  · Lack of mature IoT technologies and business processes.
  · Limited guidance for life cycle maintenance and management of IoT devices.
  · Limited best practices available for IoT developers.
  · Lack of standards for authentication and authorization of IoT edge devices.
  · Existing IoT complexities and lack of resources prevent IoT decision makers from more IoT adoption.
- Decision makers need to understand the benefits and disadvantages of these developments and at least have a fair knowledge at the big picture view on the impact.
- I really think that we need to be careful when we talk about AI etc, I am not sure if we are really up to date on this subject. Governments in Small Island states ten to send one or 2 persons away to train, but is this training passed on and put into effect.
- The working in close relationship with the various stakeholders
- Most policies are somewhat unsuccessful because the policy makers are not experts in landing IOT projects that involve on-site technical installation support and experience. Most policies are targeted to give the final big picture (bright future) with little consideration on what to do in the interim/transition stage. We at China FIOT-Lab help play a role in smoothening this transition stage by taking on technical challenges at project/product level and translating them into industry standards and best practices. These standards form the foundation for reference and might pave the way for better policies.

- People tend to firstly “Enable” the AI system, and then addressing the security issue, I think this needs to be done reversely.

3.c. Do you consider other policy challenges related to the use of IoT, Big Data, AI and how would you suggest that they are (better) addressed?

- I think companies need to have free-liberty to develop AI-IoT- devices but with the appropiate audit. Laws don't fit here, only technical decisions and symposium collaborations for better develop algorithms and evolutionary IA approaches.
- Stimulate digital literacy on the subject
- International competition law
- n/a
- the use of A.I. to produce media contents is also very challenging and need to be clearly considered to avoid deresponsabilization about its possible (intended or unintended) consequences.
- Unemployment and changing social structures. Report like the one from Oxford estimating 50% of jobs replaced by automation is not helpful. More realistic approach from OECD estimates 12%. But even if the real answer is 6%, what is relevant is the impact on structural unemployment. If that doubles or just increase by 50-75% you will see social unrest.
- I hope the government can regulate the private sector:
  1. They can't treat customer data as commodities.
  2. Let consumers know what are you doing with their own data.
- · Machines’ actions in unpredictable situations.
  · Information security and privacy.
  · Machine interoperability.
- Digital Road map that will ask the very key question "Do you want your nation to be digitize -
- Transparency is needed
- No
- Need to consider issues at the grassroots level, make a Pareto list of the most urgent issues and escalate them to the policy (gov) level.
- formulate related standard such that products/systems related to this kind of Human’s Bio-ID shall comply with.

IV. Trust in applications that combine IoT, Big Data, and AI

4.a. Trust in applications and developments is an important policy challenge.

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.

- I think that definition is not ethical. I prefeer to use the term "it works in most cases" because is impossible to test every scenario in AI.
- Trust should mean REAL TRUST
- Ok
- No. More information and campaigns are needed.
- 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 others kinds of relation the trust needed could be "correct and justified".
- a bit unclear. You should be able to trust the 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.
- · Customer demands and necessities change constantly.
  · New uses for devices—as well as new devices—sprout and grows at dangerous speeds.
  · Inventing and reintegrating must-have features and capabilities are expensive and take time and resources.
  · The uses for the Internet of Things technology is increasing and changing.
  · Consumer Confidence
  · Lack of understanding or education by consumers of best practices for IoT devices security to assist in improving privacy, for instance change default passwords of IoT devices.
- No, I don't believe. Know and understand your situations and cases before putting your trust or no trust then, make a decision. I would suggest "intellect and trust"
- Yes I agree, too little can prevent use, too much can create errors
- Yes
- Yes
- 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 a agent for connecting the truster and trustee. However, a supervising mechanism shall be implemented to supervise this centralized mechanism for making any mistakes.
-

- From your perspective, what is important and influences this trust?

- As I said before, community, scientists working hard, developers working with security in mind. AI allgorithms well-developed with ethics in mind. No way of control it specifically, only the good ones would make it better, in secure terms.
- 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
- n/a
- 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.
- breach of trust?
- 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 the high importance of maintaining privacy, and how they set up rules in place 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.

4.b. Over the last few years, in many countries there has been a growing “techlash” as Internet users have learned how their data and the services that collect it can be misused.

- What do you think most accounts for this lack of trust?
- What can Internet companies, Internet users, and governments do to increase trust in applications and services that combine the Internet of Things, Big Data, and Artificial Intelligence?

- I think is good and interesting that the majority of people are thinking in how their governments, they cheat in the end, those harmed by an act of surveilllance or pedophilia are the affected themselves. It is everyone's responsibility to demand good security standards in the devices and the necessary audits to ensure the security that the device gives us
- Hidden agendas, interests that go against common good
- Lack of accountability
- n/a
- Internet platforms irresponsible attitude.
- Lack of digital literacy and that these platforms, and Internet more generally, has become so integral to our lives. Colelction of my data might not have been a big deal in 2005, but by 2015 it starts to become a big deal since we are living our lives online to a greater degree.
- Government use data to surveillance citizens. More and more fraud with e-commerce websites data leak incidents.
- · Major firms competing for the AI market share include Google, Microsoft, Nvidia, IBM, Intel, Facebook, Samsung and Amazon web Services.
  · Major drivers for the AI market are the growing big data, increasing adoption of cloud-based applications and services, and a rise in demand for intelligent virtual assistants.
  · Essential challenges facing the AI market include concerns relating to data privacy and the unreliability of AI algorithms.
  · Public cloud adoption is increasing along with the gainintrustin public cloud.
  · The complexity of the IoT system requires essential rules on data management, security, latency and reliability issues.
  · IoT requiresAI as a companion.Since,IoT will produce a treasure store of big data that will need to be intelligently analyzed with machine learning to draw meaningful insights for businesses.
- Understanding the processes involved and mostly access to terms and conditions are too long and fine to read or spend time on. Short and simple that will attract understanding and build trust at the same time
- Lack of communication
- Misunderstanding of the real purpose why data should be collected
- Most users want to be in charge to control and know where their data go to. The lack of trust arises when users find out that their data is going to places they don't want, through certain entities that they have not authorised to do so.

- What can Internet companies, Internet users, and governments do to increase trust in applications and services that combine the Internet of Things, Big Data, and Artificial Intelligence?

- generate more space for reflection, invite young people to participate in ethical debates regarding specific technologies, propose scenarios and decide through consensus how the software should act in a given situation or scenario. For example, before an imminent scenario of shock and accident, who to kill? In front of a drone border scenario, the drone must shoot? when? In a scenario of medical operations remotely, if the link goes down, which connection do I give priority to? How do I determine routing rules on the internet based on the application? Are there priority applications, life or death? What happens before a Denial of Service, and why protocol are passing the data of the teddy bear camera?
- Be truthful
- put forth enforceable regulations bringing accountability to the next step and blocking any market leverage effect.
- That's not their real agenda

- n/a
- completely change their "contract" with the users and guaranteeing the respect of the privacy 100%
- Transparency
- They need to talk about norms together. Don't regulate the law before technology development.
- connect with the inventors and understand the overall purpose of building applications or services..... have relationships with them through partnership programs
- Town hall meetings, newsletters and follow ups
- Shortened the terms and conditions if usage. Regularly run survey on the trust users place on the service
- Have a strong Ethical Guideline that they adhere to. Use new technologies like Blockchain to securely store data in a trusted fashion (data is stored in many trusted places hence making it difficult for hacking or illegal access)
- Maybe a centralized blockchain system ?
-

V. Survey respondent

Region/Country

Africa *
Asia Pacific *****
Europe *****
Middle East
North America
Latin America and the Caribbeans ***

Countries:

Barbados, Bulgaria, Burkina Faso, China, Germany, India, Singapore, Uruguay, Vanuatu, Sweden, Switzerland, Taiwan

Stakeholder group

Civil society *
Technical Community ***
Government **
Academia ***
Other *** (private sector, Government-linked non profit organisation)

Any other comments or input on you wish to share?

- A special event is only targeted for parliament members and do not mix with any other stakeholders. the training should be coordinated by UN body

The BPF wishes to thank the survey participants for their contribution:

Nicolas Fiumarelli (Youth IGF Uruguay), Petar Mladenov, Giacomo Mazzone, Ying-Chu Chen, Dr.N.Sudha Bhuvaneswari, Dalsie Green Baniala, June Parris, Christine Tan, Yinxuan Yang, and the participants who preferred an anonymous submission.