The Internet Governance Forum

Meeting of the Dynamic coalition on the Internet of Things

Meeting report, Thursday, 12 November 2015, 09:00 – 10:30

Since the 3rd Internet Governance Forum (IGF) meeting in Hydrabad (2008), IoT has been on the agenda for multi-stakeholder discussions of all IGFs, We came to understand that the way forward is to be found in taking ethical considerations into account from the outset, both in the development, deployment and use phases of the life cycle, thus to find a sustainable way ahead using IoT helping to create a free, secure and enabling rights based environment. In 2015, this has resulted in a draft Statement of IoT Good Practice that has been put out for public comment during August 2015, and can be found at http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-the-internet-of-things-dc-iot-4/. Earlier reports on the work can be found the DC IoT website at http://www.iot-dynamic-coalition.org/.

The DC IoT workshop focused on 5 key ideas that are reflecting our current thinking behind the IoT good practice paper, working towards a common appreciation in 2016. The session explored what "ethical" actually means in this global context, how we could come to a commitment to such an ethical approach, and what else may be important in this.

DC IoT Chair:	Maarten Botterman
Moderator:	Avri Doria
Remote moderator:	Sandra Hofenrichter

Contributors (in order of speaking):

- Maarten Botterman, Netherlands, Chairman Public Interest Registry (technical community)
  Introducing the draft IoT good practice declaration
- Wolfgang Kleinwaechter, Germany, Professor Arhus University (civil society)
  History of DC IoT and thoughts on ways forward

Panelists:

- Carlos A. Afonso, Brazil, Boardmember CGI (civil society)
- Megan Richards, Belgium, Principle Advisor European Commission (government)
- Jari Arkko, Finland, Chairman IETF (technical community)

- Max Senges, USA, Google lead on IoT policy (business)
- Joe Aldaheff, USA, VP Global Public Policy and Chief Privacy Officer ORACLE, Chairman ICC Digital Economy Commission (business)
- Sergio Paulo Gallindo, Brazil, President of BRASSCOM (business)
- Olga Cavalli, Argentina, representative of ITU-T WS 20 on IoT (government)
- Sebastian Bellagamba, Regional Director for Latin America of ISOC (technical community)

Summary

With about 80 people in the room, the discussion on the draft IoT good governance paper was well received, and whereas it was made clear that the paper was indeed a starting point requiring more dialogue, it was seen as a useful starting point.

A number of observations were made across the board, and in particular it was made clear that it is important to distinguish the specific IoT application, before becoming more specific than “generic”. IoT applications can vary in terms of:

- Privacy sensitivity;
- Security level required, not only for protecting data but also for avoiding unauthorized tampering;
- Safety level required, much depending on the type of application and sector.

Overall, IoT was seen as “coming” and “promising”, also important to ensure developing countries can and will benefit from IoT applications, such as in agriculture and disaster warning systems. It was proposed to develop an annex to the declaration with examples of good practice in a variety of applications.

In terms of networking, it was recognized that IoT functionality should not be fully dependent on networks working, as networks are not fully fail proof, by definition. So it is important not to become totally dependent on on-line systems, all the time.

In terms of “ethical” it was remarked that this is a concept that needs to get better explained. IN the end, a proposed “ethical approach” should be “sufficient” from a civil society point of view, and “do-able” from a business point of view. This requires an active multistakeholder dialogue.

In terms of “making people aware” it was pointed out that “meaningful transparency” also met that people should not be expected to be technical experts. One way of dealing with this is using simplified codes (like washing labels), and clear language reference sites, like a “Wikipedia for IoT”. Another important factor is for users to have choice, and ownership, and where this is not possible for business to commit to “fairness” – again a concept to be further developed over the coming year.

Overall, all participants seem to agree that IoT is coming, and that law alone will not be sufficient to “guide” responsible development of IoT products and services. It will need action from all stakeholders, and the dialogue facilitated by the dynamic coalition will help find a way forward that will help create “a future we want”.

Panel – issues discussed

>> MAARTEN BOTTERMAN: Going back to the 3rd IGF in Hydrabad (2008), the Internet of Things has been subject to debate during the IGF, as it was considered by multiple stakeholders as one of the “game changers” towards the future of the Internet. With the formal inauguration of the Dynamic Coalition during the IGF in Nairobi (2011) this relevance was confirmed, and the discussions between a wide range of stakeholders has continued, since.

Today, we are at a point where the Internet of Things (or: IoT) is increasingly impacting our society by collecting and sharing data as input to services, as well as acting based on feedback from sensors and/or instructions provided by users.

For the first time, DC IoT has tabled a (draft) IoT global good practice paper, with the intent to further develop this with the IGF multistakeholder community towards a IoT good practice declaration, aiming at rough consensus towards the end of 2016. Ideas behind this declaration have also been presented for feedback.

Subtitle of the session is: “How to prevent needing more regulation”. As developments go very fast, it is impossible to pre-empt outcomes and legislation may stifle innovation in ways that are contrary to the interest of society or unnecessarily hindering business. It is noted that legislation is already there, and even if not designed for IoT it does apply to society, thus also to IoT. As legislation today is not reflecting an increasing digitization of society as happens with a wealth of connected objects, observing, sharing data and taking action, the ways implementation of specific legislation has been foreseen may unnecessarily hinder innovation, development and deployment. Now: it is clear that IoT as such can be intrusive, and in order to “protect” society it is therefore important we can find a way forward in which business commits to self-police by “acting ethically from the outset” and civil society helps defining how a sufficient ethical commitment would look like, and how keeping to such a commitment can be assured. Governments and the technical community play an important role in implementing this. We need to find a sustainable way ahead using IoT helping to create a free, secure and rights enabling environment and to stay close to the sustainable development goals it's about a future we want.

It is clear we need to to establish a framework on transparency and accountability with respect to current legislation but also preempting changes in values and needs of citizens in such a way we can move ahead responsibly, together.

>> WOLFGANG KLEINWAECHTER: We see a wave of discussions on Internet of Things since one or two years. It's really exploding now the debate, but it's not new. So the first discussion around the Internet of Things emerged from the discussion about the ID chips in the year 2000, 2001, 2002.

Initially the question was: “If we link objects to the Internet, what does this mean? Is this a new Internet, or is this just on top of the existing DNS system a new application, new services?” In the year 2006, 2007, 2008, 2009, the discussions developed further, growing towards the understanding that the Internet of Things if it comes to the issues of governance or regulation is nothing else than another service on top of the existing Internet, just like search engines or social networks.

And the question was then with regard to regulation: “Do we need a special mechanism, special regulation for Internet of Things like we have for the DNS.” Some people proposed to introduce something like an ICANN for the Internet of Things dealing with the ONS, Object Naming System, others proposed to just use the existing mechanism and existing regulations to identify what is needed and then to find arrangements, guidelines or whatever that are based on the existing mechanism and the existing regulations. The dynamic coalition has been instrumental in this discussion.

The second main contribution this dynamic coalition made to the debate is having put the discussion in the multistakeholder context. Even today, we still find a lot of discussions to find place within silos and from individual perspectives. All stakeholders discuss the issues within their own circles, or their own sector, and more needs to be done to truly make this a multistakeholder dialogue, up and beyond the discussions in the dynamic coalition itself.

Stakeholders come together when discussing smart cities, yet these circles do not connect to the global Internet Governance debate. Same it true for the debate in Internet of Things in transportation and traffic, and on industry 4.0: all in isolation.

The challenge for the future is to pull the people not only out of their stakeholder silos, but also out of their sector silos and to organize a debate which is integrated both horizontally and vertically brings the stakeholders into debate which is base the on existing mechanisms, so the basic question do we he need new regulation. The basing answer is no, but we have to double check existing legislation and identify where we have probably to bridge some elements and the final point is the so called ethical dimension, which is our discussion tomorrow morning.

With regards to Human Rights we can learn something from the debate in ICANN on whether Human Rights is relevant for names and numbers. And the answer is, yes, it is relevant, but ICANN is not a Human Rights organization, nevertheless whatever ICANN does, it has to respect Human Rights. This seems a good guideline also for the Internet of Things. Whatever is introduced in new technologies, services and applications, Human Rights have to be respected. We operate in an existing body of international Human Rights legislation, and nobody has the right to violate Human Rights. This will be an important new area for discussion which needs more clarification and the dynamic coalition is very well positioned to facilitate this discussion.

>> AVRI DORIA (Moderator for panel and participants’ discussion): The five questions that we have sent to the panelists for their initial contributions are (for the record):

1. In order to develop the Internet of Things in a sustainable way, developers and deployers need to commit to an ethical approach taking into consideration that the IoT is really about people and how it affects people.
2. Good practice in IoT products, ecosystems and services requires meaningful transparency to users and user control of data produced by and associated with an application, insuring security and respect for privacy.
3. Products that can be connected to the Internet should come with a clear indication of what data gets collected, where the data is stored and what are the conditions, what the conditions for access are.
4. Stakeholders should work together to insure consumers, citizens have a choice when wanting to obtain current and popular services.
5. In order to establish a long-term relevance of IoT products and services, it will be key to establish a clear framework on transparency and accountability and preempting changes in values and needs of citizens.

We have asked each panelist to speak three maximum five minutes. Find below the core messages from the speakers:

>> CARLOS AFONSO (Board Member of CGI, Brazil) pointed out that with the abundance of unique address space in IPv6 a small provider potentially can address anything in the world. This makes it possible that all objects have public addresses, rather than being behind one public address or carrier grade network. This has consequences for privacy and data protection. He suggested that the issues arising are similar to those we started asking when the Cloud appears. The same questions which might be asked from Cloud providers, and in the past, from Internet service providers as well, is that that we are on the verge of another big bang. Hence we really have a big challenge in this dynamic coalition.

>> OLGA CAVALLI: (Member, ITU Study Group 20 on IoT) Olga is participating in the ITU Study Group 20 on IoT, representing Argentina. The work of ITU SG20 is the development of standards that refer to Internet of Things technologies to address urban development challenges. Commending the work of the dynamic coalition for their work and documents produced Olga supported the proposal that the ethical approach should be inclusive in the sense that knowledge and technology should be developed including interest and industries from Developing Countries. Developing Countries should not just be consumers in, but should be encouraged to produce knowledge, products and services locally so we enhance the knowledge of our own companies, also about the good practice related with where the data is stored. That is something that it's important. Information about where the information is stored, how is it managed, the local security and privacy regulations should be taken in consideration and respected, about the products that could be connected in the end, in the Internet that could come with a clear indication about the data that gets collected. It should be important to consider the language barriers for many small or medium enterprises in Developing Countries, especially those who are not English speaking countries, the language can be a huge barrier, so all of this information and manuals and codes should be available in several languages. Last but not least: stakeholders should work together to insure consumer citizens to have a choice when wanting to obtain current public services. The challenge in Developing Countries is helping the ecosystem of the industry is to develop locally, to create knowledge and value added at the local level, at the local companies. Latin American countries run their economies mainly through small and medium enterprises and for a small or medium enterprises it's not so easy to participate in this global definition of standards. The clear framework of transparency and accountability should have all of this considerations.

>> MEGAN RICHARDS (Principal Advisor to the European Commission, DG CNECT):

The European Commission is actively developing the Digital Single Market strategy, which Vice President Ansip responsible for, along with Commissioner Oettinger. Development of the Internet of Things will be an important aspect in developing the digital single market and its environment should be supportive for IoT development.

An important step in this was the creation of the Alliance for Internet Of Things Innovation (AIOTI), launched by Commissioner Oetinger (responsible for "Digital Economy and Society") in March this year (2015). AIOTI brings together a group of experts from all different areas looking at issues relating to the Internet of Things, divided in a number of working groups.

WG 1: IoT European research cluster

WG 2: Innovation Ecosystems

WG 3: IoT Standardisation

WG 4: Policy issues

WG 5: Smart living environment for ageing well

WG 6: Smart farming and food security

WG 7: Wearables

WG 8: Smart cities

WG 9: Smart mobility

WG 10: Smart environment (smart water management)

WG 11: Smart manufacturing

These working groups are looking at a number of issues relating to the Internet of Things, particularly in in Europe, and in a global context. And they are looking in particular at issues relating to numbering, standards, spectrum, Net Neutrality, and the influence and impact of those issues.

There are also different EU fora looking at ethical issues relating not only to Internet of Things but also research, and ethical issues are very important and taken very seriously.

In terms of the IoT research activities, in the last call for proposals under the Horizon 2020 programme nine projects related to Internet of Things were selected and will be starting in January 2016, with EU funding of $50 million and some of these include aspects relating to ethics impact on people, et cetera. In the work programme for 2016 2017, there is 100 million Euros allocated to research in these areas as well. The European Commission is interested in working with other parts of the world, and supports this actively.

>> JARI ARKKO (Chairman IETF): The standards organisations have done work to standardize various protocols in the IoT space. However, at the application and data format layers we have far less interoperability than we should have so there is still much work to be done there. Also we obviously need good answers with regard to security and privacy. If we do not get this right, we are risking another Snowden moment or Snowden on steroids moment later. The latter is well covered in the principles. The former requires some aspects of user control such as practical ability to store data in a specific location. Items 13 and 14 talk about transparency, about terms of use not only to what gets tracked and by whom and user control. This is good, yet it stops short of covering some challenges that we may actually be facing as well: we may need to transforming the optics around us and move towards something completely new. In particular we will see a change in the concept of ownership. Do you own the control

software in your joint attracter or are you licensing it? Can you modify your car (John Deere tractor), are you buying the service, physical object, both, what. If the object consists physical parts and services that run on the network, under what conditions did you buy those things or good you buy those things and how long will they be available? This aspect needs to be fleshed out more, as it is currently underserved in a paper that talks mostly about data and tracking right now. There may also need to be attention for, for instance, ownership, control, composition of the thing that you own, and service agreement.

>> MAX SENGES (Google Internet Policy and IoT research programme): Google has high interest in IoT, and is working on developing it - exploring and boot strapping like everybody else. Google is large, and especially Alphabet, so the disclaimer is that Max is only talking from his position within Google – not on “all positions within Google”.

Google and Carnegy Mellon university, Cornell University, the University of Illinois and Standford are working together on the preparation of an IoT expedition and open innovation programme. It is the intent to bring in potential industry partners from around the ICT spectrum from 20 November 2015, onwards, to join and build a coalition that is set on openness principles. The initiative is intended to create a basis that brings us together for the Internet of Things, Systems and protocols and especially interoperability amongst these different pieces is one of the key goals, the expedition set its bill to develop something like a LAMP stack for IoT, meaning we don't want to set the system, but at least a system in which you can have modules that can be interchanged. It's important that you have a standard you can deploy easily and to address the point of making the IoT applicable to developing and emerging countries.

The idea is to develop a package “IoT in a box” that you can bring to universities and hacker spaces around the world. Having that said, we are just one year into the operations, so we invite everybody to come and speak to me and to the colleagues from the universities, but it is early stage. Systems and protocols especially and schema to address and speak between the different things are one of the research and development areas. Another priority is that there a lot of things and ensembles of things that don't have screens and key boards yet do require a human computer interface that is fairly universal as the second aspect. Third, or maybe first priority, is privacy and security

And the third, or maybe the first if we wouldn't have stressed it already so much is privacy and security which really needs to be thought of from the very beginning (including identity management). This may not have been up front when originally developing the Internet, yet it needs to be up front right now.

Last but not least is the need to address safety. Now, the Internet of Things comes into the physical realm and our cars, our houses, all of that add a new component that is safety – also key to the success of IoT.

>> JOE ALDAHEFF: For IoT, we do not need new regulation but we may need to check and see whether current regulation is implemented in a way that serves the purpose of the law. From a business point of view, there is really no objection with the concepts related to ethics, privacy and security. They are logical extensions of the current conversation. The challenge is to make ethical values practically applicable, as ethical values are abstract, as such. It is important to consider the specific application: it makes a huge difference considering wearables or industry logistic applications.We need to rethink the principles in the terms of the application in their construct.

The other challenge is that a one to many or many to many process may not be susceptible to complete individual control or even to multiple individual control. So fairness models may need to be developed in those contexts as the level of the individual preference cannot always be honored, especially in IoT like street sensors et cetera.

Another distinction that is important to make is whether specific IoT applications deal with personally identifiable information. Large chunks of IoT that have no personally identifiable information. So whereas certain practices are applicable in cases where personally identifiable information is implicated, they may be unnecessary in other application and may add overhead and constrain innovation needlessly.

It is also important to be careful with specifying technology as opposed to just using technology as an example. So highlighting PKI without saying including PKI is problematic because five years from now PKI may not be the flavor of the day and we don't want to lock ourselves into a practice that is limited to a technology. This will need to be reflected in a good practice document, carefully.

Very important is to also not to expect people to be experts: applications for consumers should be easily understandable, both in their working and impact. Don't confuse people with excessive information they cannot deal with – offer comprehensible info only. Again: as simple as can be, and not simpler. Use fairness models to supplement it.

Disclosure and control should be reasonable and useful both from an individual and a commercial perspective. A multistakeholder process would allow to have all of the points of view factored in so you can figure out what is commercially practicable while still actually managing and maintaining fundamental rights related to privacy and issues related to security.

Finally, it is good to talk about "good practice" rather than "best practice" as there may not be one single best way forward, because this may not be a one size fits all environment. Frameworks are to be consistent to the same set of principles, but how they get articulated at the next level of detail may have to vary across uses and that's something we should probably consider how to address in the practice framework, which may be the set of the principles that is the binder, not going to the specific implementation scenarios.

>> SERGIO PAULO GALLINDO (President BRASSCOM): Brasscom is an association of ICT companies the largest operating in Brazil. I am going to address the accountability issue and it's a mixture of the discussions we are having in the ocean as well as my own thoughts.

IoT is a new technological and business wave that promises to integrate individuals in the physical way into a digital and reactive reality through the Internet. To achieve this a promise massive amounts of data will be gathered by sensors, stored and processed by Cloud based infrastructure, using big data techniques to produce meaningful information for wide variety of purposes. Specialized software or expert individuals should be able to affects the physical world or the biological world through actuators or several mechanisms. Ethics in this can be seen as high level values or law principles not necessarily attached to any jurisdiction that should be observed as a minimum standard by all actors involved in IoT and should hopefully influence expected and desirable upcoming legislation in various countries.

As much as new technologies and business models are desirable, both from an economic point of view as well as for the sake of public welfare, protection of individual rights shall be promoted by companies and Governments. Such a balancing act evokes a notion of civil responsibility in law condition or law of torts in common law, accidents or damage, whether material or moral shall be avoided in the first place and compensated in case of occurrence.

A great deal of discussion is being undertaken in Brazil these days about protection of personal data, consent relative to processing of such data, and consent. As I see it, consent is embedded with an underlying contractual relationship in which data is relinquished by its owner as a quid pro quo for a service of some sort or benefit of some sort.

In line to such understanding, consent is given for a purpose, and can be explicit or tacit or implied. In the latter case, interpretation of implied consent purpose shall be very narrow given its context, it is context based. The relationship between the data subject or the owner of the personal data and the data controller is a consumer to enterprise relationship.

Under Brazilian life the objective of product liability in common law system and the data controller shall respond for deviation of purpose in using the data as well as failure to protect the data in light of unauthorized leakages. The data controller might contract other data processors. Given the level of expertise of various companies it is conceivable that chains of subcontractors will emerge in collaboration to deliver IoT systems and applications.

Relationship through the chain of subcontractors is an enterprise based contractor one. Hence, contractors shall respond in accordance with the terms and conditions under which they are contracted for as well as for the duty to protect the data. A traditional subjective civil responsibility or the negligence status seems adequate principle for such relationships, however, such assessment might be argued in light of possible application of objective civil responsibility or strict liability standard relative to duty or protecting data.

Relative to IoT, one is questioning how such concepts can be applied over things, and the reality is they cannot. A thing is not able to autonomously respond for any damage, however, IoT is a kind of system and application, most likely delivered as a service. Behind the collection of connected things there ought to be a company or interpreter responsible for it, and hence the responsible party.

What is new in IoT is a possibility to interfere in the physical or biological world through actuators commanded by experts or even by commands automatically generated by software. Under such circumstances emerges civil responsibility for damages caused by wrong actuations or emissions,that is when a particular needed expected action is not taken.

We shall welcome IoT given the enormous benefits it will bring and the potential for further economic development and growth. It is thus recommended that companies take a preventive approach adopting principles such as privacy by design and safety by design.

>> SEBASTIAN BELLAGAMBA: The ethical approach makes sense, and to work towards the world we like our children to live in puts the user in the centre of the discussion of IoT which is important.

IoT holds promise as a tool in achieving the United Nations Sustainable Development Goals and it's a very key part of that. In order to unleash all of the potential of IoT, we identify some challenges that have to be worked in order to get it right. Information Society has put out a document on this that can be found at www.informationsociety.org/iot.

Security is important, and it is really about trust. One of the things that we identify as a big challenge for the Internet in the coming years is not only to get people on line, I mean, the rest of the world that is not online, but how we work with this undermining of trust that some privacy challenges are bringing to the people that are already connected. We should avoid this becomes a big issue for IoT in the future, as we could be facing a “Snowden on steroids” and that's something that we are desperate to prevent. So users need to be able to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology becomes more pervasive and integrated into our daily lives.

The interconnected nature of IoT devices means that every secured device connected on line potentially affects the security and resilience of the Internet global, and that's another thing that we have to consider. In privacy, the Internet of Things is redefining the debate about privacy issues. Implementations can change the way personal data is collected, analyzed, used and protected so something has to be done in this regard.

Interoperability and standards is another key challenge. A fragmented environment of proprietary implementations will inhibit values for users in the try, and I the use of generic open and widely available standards as technical building blocks for IoT devices and services such as the Internet Protocol will support greater benefits innovation and economic opportunity. There is a lot of legal regulatory and rights issues that has to be considered.

The emerging economy in Developing Countries can and should realize the potential benefits of IoTs. The unique needs and challenges in implementation in less developed regions will need to be addressed including infrastructure readiness, market incentives, technical skill requirements and policy resources.

Last, but not least: no stakeholder can achieve all this by itself: we need a collaborative multistakeholder approach.

>> AVRI DORIA: Thank you very much. I want to thank all of the panelists for not only the contribution they brought to the discussion, but for actually sticking to the time limits we had because it was really important that we get the contributions from the other participants in the room. First questions?

>> AUDIENCE: (Joseph Amadu from Ghana):

Question 1: how would the IoT inch challenged our lives, especially in Developing Countries?
Question 2: what impact will IoT have on sustainability?
Question 3: How safe is IoT?

>> AUDIENCE: (Sana Gitu from Nigeria):

I'm trying to find out the choices between rights, access, quality of education because when you are talking about having a whole lot of things to do with Internet of Things with unique identifiers. Can we now use IPV6 to create global registry for both machines and human beings?

>> AUDIENCE: (Peter Dengate Thrush, New Zealand):

What will be the intermediation between the IP addresses and devices? Are we going to see domain names used in the IoT? Are we going to see it just machine to machine using IP address to other systems to that stack? Or are we going to have a multiple system where some domain names are used and if we are using domain names, one assumes they will be largely machine readable ones rather than human readable ones. How do you see that developing?

>> AVRI DORIA: Responses from the panel?

>> JARI ARKKO: There is no “one side fits all” answer on the question of the identifiers, so obviously for technical reasons we need IP addresses and in some cases we need domain names, but IoT is far larger than addressing a host either through an address or domain name. You will have databases that keep track of which things belong to which persons.

There will be various kinds of tabulation of information: IoT will probably be considered mostly in terms of that database which probably will be somewhere in the Cloud, depending on the specific application. And underneath the machinery, we will somehow figure out what addresses or domain names to use, but the user will not need to type your sensor's name on a browser.

>> MAX SENGES: How is IoT going to change our lives? This is really about how we are going to use it, and the impact it has on society is the ethical dimension. The current framing on this in the DC IoT draft document is not good enough, yet. The discussion would merit from being informed by the work by

Michael L. Dertouzos called “The Unfinished Revolution: Human-Centered Computers and What They Can Do For Us” from January 9, 2001 in which he asks for a new technology design paradigm, necessarily with an ethical perspective.

The way ethics are framed right now seems to focus privacy and data ownership yet should also include openness and making the technology accessible to people and really give them a right to work with it. Data ownership will ultimately need to be addressed. And right now it would be too early for the request for a report by the privacy rapporteur of the UN.

On the question re: safety: no technology or service is completely safe, but in Internet of Things what we are going to have to deal with is with level of safety, right, levels of safety, different safety levels. An application that just gathers data, let's say, from a vehicle and send that data for post processing relative to the quality or maintenance of the car is one level of commercial safety which has to be reasonable.

But what Internet of Things is bringing towards us is the possibility for actuation in the physical world. So if in the same car the sensors send the information to a data centre and that data centre processes the way the car is being driven, and sends a command to try to avoid a crash that is imminent, or the algorithm is wrong, the crash may be precipitated and the driver will suffer the consequences.

So what we need to actually consider is that there will be different levels of safety to be imposed on the types of applications that will be coming up. And that's the real value of the discussions about ethical principles because we have to differentiate from application to application the levels of commitments that the future providers will have to take with their consumers and they have to actually embed this from the inception of their designs to the delivery and operation of such applications.

So in short, is Internet of Things safe? No. But we have to strive to make it as safe as possible for the sake of us individuals.

>> OLGA CAVALLI: With regards to the connection with the physical world, IoT will have a major impact on traffic management and distribution of water and other goods in the city. In Latin America, there are huge cities with more than 10 million people gathering together every day for work and interacting, so the impact is expected to be substantive. In developing countries, agriculture is an important element of the economy, and it would be an interesting area to see how the Internet of Things can contribute to and empower that industry, yet the main “gain” for developing countries is in development of the knowledge and empowerment of cities, local SMEs and communities, learning and getting know how to do things on their own.

>> JOE ALDAHEFF: Let’s not apply personal information restrictions where personal information doesn't exist. And cars already have antilock brakes which actually process information on board. So we already have a learning curve here. This is not a new topic, just a topic we have to consider, and many problems that come up here have already been solved somewhere else.

There are huge potential benefits to a developing country. Here it's perhaps less about wearables and sensors as “toys” yet more about the how you might use a sensor in farming, because low cost sensors can tell what the water flow is in the river near the farm. A sensor can be put in the ground to better understand what the level of water table is, what the level of rainfall is, tying that to remote systems which can be fed through a non-Smart phone to tell you about what the weather patterns have been, what the possible crop benefits are, what the soil needs. A number of countries have already started putting these in place to help farmers increase the yields to improve food safety and security, in combination with other sensors and other information that is blended because we can't think of sensors in a vacuum. Sensors work with analytics and with other services, also allow them to know which markets are near them that may actually need the products they are growing to allow them to gain the economic benefit from their effort and industry.

In some ways we are only limited by our imagination. You can see this in terms of putting sensors on buses, so rural routes where the bus service is highly irregular, people can start to know when the bus is going to come by. Things like that can be small things that can transform lives significantly. We might want to consider adding an annex to the document to also help us flesh out our thinking on opportunities.

>> CARLOS AFONSO: It is clear that we are at the starting of a big bang in IoT, hence the expectations vary wildly. A good report from the European Parliament explores the issues from a societal perspective, and also highlights the importance of addressing the bandwidth issue. Sensors usually use bits per second only and don't need to be connected all of the time, yet with masses of things connected we will need to look into this. Also on other topics we need to do more, and we are only beginning to scratch the surface. This is true for “IoT going ethical” as well as for more concrete subjects like the role of PKI etc. The challenge is big.

>> AUDIENCE: (Mary Lynne Nielsen, IEEE).

IEEE is right now working on architectural frameworks for the IoT. If you haven't seen it or examined it in some of the standards questions you raised, I would strongly encourage you to look at that as well as frameworks for market architectures for buildings and home security. There is a great deal of detail at the IEEE that I think you would benefit from in examining this question. I encourage you to look at that or talk to me or come to our book about that.

Out of all of the speakers only one of you mentioned identity management, whereas this is very important when considering IoT: identity varies per role we fulfil, i.e. it is really about persona. We are working on this in the IEEE in partner well with the Pentara initiative, and think about for the fact that every device or tool you use, you are not one thing. Right now, here at this event, I would imagine that all of us are at any moment switching from being a participant to being an employee of our company and organisation and doing it seamlessly on one device. How do we approach that? What are the ethical implications of our varying persona on devices and how do we handle that?

>> AVRI DORIA: Thank you. And please join the dynamic coalition to make sure your ideas get in the right place over the next year. Next question?

>> AUDIENCE: (Allen Greenburg, Chair of the large advisory committee in ICANN). I'm a newbie on Internet of things I'm not a newbie on networking in general. My question is not on the ethical basis but a more basic one. Last night my phone in my hotel room said ready to connect as soon as network quality improves. We can't make our telephone system work all of the time. Why do we really believe that we are going to be able to do all of these things with ubiquitous functional networking that will be transparently useable by all of these little things?

>> REMOTE MODERATOR SANDRA HOFFENRICHTER:

I'm reading comment from Miguel Estrada. He said I think the kind of safety on the IoT can be closely related to airplane software. The thing here is not software, it is data storage. His question is what can be done with this data? Who owns the data? For what purposes it can be used, et cetera?

>> AUDIENCE: (Alessandro Zeleskr, Nokia??)

I have concerns about the Net Neutrality and the type of connection that it will be needed for IOT. And IoT not going to work but quality of services and prioritized connections. And I'm not only talking about remote healthcare or connected cars, but a lot of other new applications that are coming together with 5G networks. 5G networks will be by definition an application aware network. That will give to any application the network services that it will need to work properly. So the connections will have to be prioritized. So how to deal with this issue face to face, the discussions about Net Neutrality here around, and that it cannot be as exceptions, so healthcare as an exception, exception for this, exception for that that we are hearing in some rooms here..

>> AUDIENCE: (John Grosam from Bangladesh??)

Question 1 to my mentor, Mr. Jari Arkko: He already said that his challenge in business model during service is object. So is there any present solution we are trying to mitigate this type of, mitigate this type of service and object.

Question 2: Architecture is important. Based on this I have one question, will IoT actually work over Internet? Will it have own dedicated wide area network.

>> AVRI DORIA: Responses, please.

>> MAARTEN BOTTERMAN: Will our networks support IoT? IoT happens because of business reasons, it's something that begins to happen also because societal reasons. There is investments going on to make sure that this all works. We are already aware that the traditional connections will not be able to connect everything as it used to be, and spectrum is an element of that how do we deal with that, but there is also new technologies that will help make these things work ranging from lower networks in certain areas even up to drone networks in the more disbursed networks or satellite networks. So basically I think the answer is to be found in really thinking ahead of how we make these things work, and there is not a single way forward, but a whole patchwork and this is why we need to talk about it.

>> MAX SENGES: To deal with accountability, we need multistakeholder solutions and shared responsibility that is dealt with on a case-by-case basis. Fair practices is what we need, and basic, easily understandable information (like washing labels or creative comments) should be available for consumers. Maybe something like a Wikipedia style network that explains how things are used and organized would be excellent in that space.

We also need to make sure we are not dependent on networks, on being online. We need to think about fail-overs and make those IoT devices work, off-line as well. The light switch should work whether you are on or off line, otherwise we are going to be in a very strange world.

With regards to new or specific types of networks, it is good to welcome experimentation. Colleagues at Google develop an open source project called The Physical Web which has a Bluetooth low energy beacon ping the URL for a bus stop. So these use cases where you walk up to something and you just need to know when the bus comes, you certainly should not need to install a new app, et cetera. We should build on the architecture that we already have and the Web is working. It's a long time out there. It's a great success. So let's not reinvent the wheel and start with a new network and new technologies.

>> JARI ARKKO: The emergence of new networks specifically for IoT will be the result of pur economics. There will be general purpose services, and they will be used. Almost no application that we can think of would have the financial backing to implement their own networks worldwide. So obviously we need one Internet and small set of access networks around the world and that's the direction that is happening. What we are seeing actually is that while it's true that IoT is going to stress these networks, the networks are evolving. 3GPP and IEEE are evolving their network standards to be able to deal with much more traffic. I believe in the use of the general purpose networks.

At the same time we are aware that currently it is sometimes hard to get access in your home network and now you are telling me, well, all of these devices need Internet connectivity. That's a really big issue actually, and it is addressed with priority. Efforts are underway in various organisations to make automatic network loading process a little bit more reasonable or feasible and progress is being made as we speak.

>> MEGAN RICHARDS: Spectrum is an area that is of particular importance to address in the coming period in Europe. Whereas there is not a specific problem with spectrum and IoT yet, we do consider this an area of importance to ensure it will not become a problem.

Examples that are specifically focused on IoT is for instance the opening up of the 876 band and the 915 to 921 Mhz band for IoT in the UK by OFCOM, the UK regulator for telecommunications.

Net neutrality also comes with implications for IoT. The new Net Neutrality legislation in the European Union will be coming into effect early next year, and in line with that guidelines are being developed for its application, taking into account future implications for Internet of Things. The AIOTI has prepared a first draft report in its working group 3 (WG3) and it should be finalised soon. The AIOTI is certainly open to ideas and contributions.

>> JOE ALDAHEFF: There is no single answer to the question of data ownership. When there is a direct relationship with a device and it's a device that is carrying personally identifiable information, there is at a minimum concept of shared ownership of the data if not exclusive ownership of the data by the person. Yet this is a specific case.

There might be shared ownership because it could be that the service provider is also using the data for functions they are delivering to you so it might be a question of you both have rights to use data and the rights extend to certain things, and there the question is contractual simplification, because at the moment the terms related to that rationale between the parties is difficult to understand. When you get to things like the jet engine returning data home, you want that data to be secured and you want that data to have a limited set of accessibility and since it doesn't capture personally identifiable information that makes sense.

The regulator may also want to see that data from a safety perspective to make sure the plane is not going to fall out of the sky so there may be other people who have interest in the data. Let’s make sure we benefit from the wealth of experience that is already out there. This is an evolution, not a revolution, and I think we need to calm down a little bit and apply the lessons we have learned.

>> AVRI DORIA: Thank you. It was left to me to sum up, but there is no time for me left to sum up other than to say thank you to the panelists. You have given us an amazing amount to think about, and an amazing amount of work to do over the next year, so hopefully we will see you beyond the panel and in the dynamic coalition itself contributing.

Thank you to the participants on the floor. Your comments were very helpful. Hope to see you all on the dynamic coalition list. Please check out the references, and especially check out that second bullet on the INT guest Forum.org CMS surveys. Basically that takes this paper, it takes the questions, and it invites you to say how important any of these issues are and what you think about them. So it's a question for more input. Again, thank you. Thank you for maintaining time, and everything. You guys were perfect!

>> MAARTEN BOTTERMAN: Thank you, Avri for wonderful moderation.

>> AVRI DORIA: Thank you. (Concluded at 10:31).

Participate to the DC IoT

The Dynamic Coalition welcomes all that have an interest to help develop an IoT Good Practice document that would benefit from "rough consensus" from all stakeholders. Please sign up to the DC IoT mailing list, register for DC IoT meetings, or contact Maarten Botterman (maarten@gnksconsult.com) or Wolfgang Kleinwaechter (wolfgang.kleinwaechter@medienkomm.uni-halle.de) with ideas or suggestions, or if you would like to facilitate a DC IoT gathering.

- Read and comment on draft Declaration: http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-the-internet-of-things-dc-iot-4/ (or Google on IGF; IoT; review)
- Read and comment on the 5 basic ideas behind the Declaration: http://www.intgovforum.org/cms/surveys
- Read more about the previous work of DC IoT, and announcements for upcoming meetings: http://www.iot-dynamic-coalition.org/
- Sign up for the DC IoT mailing list: http://intgovforum.org/mailman/listinfo/dc_iot_intgovforum.org