Dynamic Coalition on the Internet of Things (DC-IoT)

Since the IGF in Hyderabad in 2008 , the Dynamic Coalition on the Internet of Things (DC-IoT) has engaged in debate at IGFs and at meetings in between IGFs on the usefulness of Internet of Things, its necessity to help address global and local societal challenges, and the challenges that need to be addressed in order to ensure the Internet of Things is developing in a way that serves people around the globe. This is through enabling them to realize the potential benefits and innovative applications that the IoT can provide while addressing the risks and concerns which can arise from new uses of data. At the IGF 2015, in Joao Pessoa the DC-IoT presented and discussed its first draft paper on Internet of Things Good Practice policies. This was followed by intersessional discussions, and a workshop during IGF 2016 in Guadalajara, and contains now the insights collected up to September 2017.

Over time we have found an agreement that legislation alone will not be sufficient to “guide” responsible development of IoT products and services, and therefore there is a need for "IoT going ethical" as the way to find a sustainable way ahead that would help create this "world we want our children to live in", or "a future we want" -as a practical definition of "ethical". At the same time it is recognized that we are not yet on a common understanding on what this and that a proposed “ethical approach” should be “sufficient” from a civil society point of view, and “do-able” from a business point of view – but progress was made. This progress was reflected in the IGF 2016 DC IoT meeting report, and now in the text below.

As in 2016, this paper does not represent the Dynamic Coalitions final position on the Internet of Things. It represents an overview of the current thinking, with the aim to further develop this position during the IGF meeting in 2017, moving towards a "rough consensus", global, multi stakeholder position on an ethical approach towards IoT development and deployment.

Internet of Things Good Practice policies

Preamble

A. The Internet of Things is a set of devices connected to the Internet interacting with each other and/or human actors, therefore, as a general matter standards and principles that are applicable to the Internet and society at large, are also applicable to the Internet of Things.
B. The Internet of Things is not just about objects, data collected and shared, and actions by those objects: it also has implications for people and society.
C. The Internet of Things, like the Internet, should be open to connect to and secure in its use.
D. To foster both innovation and user trust in the Internet of Things, like the Internet, a careful balance should be struck between regulation and space for innovation. This requires governments to hold back on regulation where possible, and industry to commit to self-regulation, where necessary, while recognizing that future useful/necessary applications as well

as limitations cannot be determined yet, today, in full. Please note that current existing legislation that does not (yet) take IoT into account may affect the legal ability to deploy IoT products and services;

E. There are important benefits from the Internet of Things to deal with a wide range of societal challenges, ranging from medical and health care, social care, and urban planning to agriculture, food chains, security and environmental sustainability. These benefits need to be explained and responsible development of IoT should thus be fostered and stimulated.
F. The Internet of Things is in its early phase and it is still evolving, though it has been around long enough for there to be some historical consequences. Therefore, not all of the technical and the governance issues have been considered yet. Especially, the issues of security and privacy will need to continue to be explored to ensure justified trust in the Internet of Things environment.
G. The Internet of Things, needs investments in innovation and deployment in order to develop. Investors like to know that their investments will lead to products and services that are not countered by governments (illegal) or markets (seen as unsafe, unwanted, unethical) or even subsidized/acquired by governments in response to specific societal challenges. We should consider how to enhance the potential for investment in both the IoT and the methods to assure its security and privacy.

1. Internet of Things Good Practice Principle

Internet of Things Good Practice aims at developing loT systems, products, and services taking ethical considerations into account from the outset, both in the development, deployment and use phases of the life cycle, thus to find an ethical, sustainable way ahead using loT helping to create a free, secure and rights enabling based environment: a future we want, full with safe opportunities to embrace.

2. Towards an ethical framework for loT Good Practice

Ethical values are the product of applicable law, cultural values, morals, and habits, and are globally rooted in outline in the Universal Declaration of Human Rights and the Sustainable Development Goals that were adopted by the General Assembly of the United Nations.

Good practice in loT products, systems and services around the world require:

A. Meaningful Transparency to users: understandable and clear terms of use, including an overview what is tracked, and the ‘why’, and the ‘how’ that information is used in IoT systems and how it is shared, with whom it is shared and under what terms. Transparency also includes "usability" as it doesn't help to have options if you do not know how to use those, and "accountability" as it is important to know whom to address in case of wrong use or abuse; It should be noted that the purpose of transparency is to provide sufficient information to allow users to make informed decisions about whether and when to use technology. There are limits to transparency in relation to specific details that if public could compromise the security of an IoT deployment or which may impact elements of innovation that might be protected by Intellectual Property laws; neither of those elements should negatively impact the ability of a user to have the needed information to make decisions about the use of a product.
B. User’s ability to understand and exert appropriate control of personally identifiable data produced by, submitted, or associated with an application. This is necessary for multiple reasons, ranging from essential privacy and other human rights to business and competition

reasons. This user control may be reflected in various ways, through an ability to direct where data is sent or stored, whether the data is generated at all, be able to appropriately delete historic data, be in control of security settings for the data. For instance:

a. Ability to turn off individual tracking (and how this can be done) where and when possible, in the highest level of granularity as practically possible." All or nothing" does not always fit here, depending on the specific application. Another option would be allowing users to control access to their own tracking data via sufficient and useable means.;
b. Enable the user to protect their personal data with a technology of choice such as strong public key encryption;
c. Ensure user awareness of data set correlation capabilities and its implications on user privacy;
d. Ensure user awareness of machine learning (and eventually possibly artificial intelligence) that may lead to change in behavior of IoT environments the user is confronted with;
e. Consider the ability to delete and export historic data: or at least makes sure that historic data are no longer related to individual accounts unless explicitly agreed otherwise ("the right to be forgotten" in practice - and data can still be used for business process innovation etc.);

C. Security: Security is an important and relevant concern for IoT both from a data perspective but also from the perspective of potential physical damage or harm.. Therefore, the security of individual loT devices, systems and the data related to the systems need to be secured adequately. An additional challenge raising from some loT applications is the fact that the devices and systems may be in use for a long time and the security requirements may change during that time. Good practice includes assessment of security impact of any part of an IoT system when developing or deploying, not deliver IoT objects with default passwords to end users, and ensure the ability to change passwords.
D. Privacy: All stakeholders in the Internet value chain, which includes the Internet of Things, including governments and industry, including both direct and indirect use and reuse of data, should comply with privacy and data protection norms and international law. In particular, any techniques to inspect, correlate or analyze Internet traffic shall be in accordance with privacy and data protection obligations around the world and subject to clear proactive legal protections. Good practice includes assessment of privacy impact of any part of an IoT system when developing or deploying with a clear understanding which data that relate to persons are collected, where they are stored and how they are used and shared.

3·Implementation and enforcement

An important element of loT Good Practice is its supporting mutual trust amongst all the components of loT systems: human, devices, applications, existing institutions and business entities. Trust is boosted by a recognition of personal needs; by transparency in how things are organized-namely in a way that clearly shows that relevant measures have been taken to meet those needs-; and by accountability in ensuring that responsibilities are clear, and if someone responsible (person or organization) fails to live up to what is promise or required, they will be made accountable, thus assuming a principles based front end (ethical, i.e. in line with Human Rights) and harms based backend (accountable).

In order to ensure long term relevance of the products and services under development, it will be key to establish a clear framework for transparency and accountability, with respect for current legislation and pre-empting evolution of the regulatory framework reflecting changes in values and needs of citizens.

Recognizing that active use and abuse of vulnerabilities in systems happen, as well as that IoT has become an attack vector for cybercrime and cyber warfare, good practice is to be pro-active in this understanding, as justifiable trust in the Internet and IoT is crucial in order for society at large to benefit from this. Measures by stakeholders are to include active monitoring networks and systems for abuse, and taking prompt action when vulnerabilities and/or abuse of infrastructures are discovered.

Ultimately, the combination of technologies applied according to IoT Good Practice ("Ethical IoT") should lead to products, ecosystems and services that are transparent for the user in terms of how they collect, store and share information, that give choice to the user in terms of adapting that to his or her appreciation of values (and legislation), and for which accountability for usages (and failure) is clear.

IoT deployment in the development context need to be considered as it can help achieve specific development goals. At the same time, attention should be paid to ensure access to IoT is available. Next to the necessary investment in infrastructure and openness of that infrastructure, both availability of licensed and unlicensed spectrum is needed.

4. Education and awareness

Related to IoT, individuals should have the right to have access to information on which these individuals base their actions with IoT - systems, - infrastructures and utilities. This information needs to be provided in a manner that is accessible to the non-expert and may benefit much from Open Educational Resources and prosumer (i.e. both producer and consumer) knowledge base. It is important to ensure that all stakeholders are able to participate in the discussions, and it is up to both governments, academic institutions and the private sector to help ensure user education. In addition, we call for providing examples of practice around the world that help illustrate “good practice” as recognized to be so within a specific region and by specific stakeholders.

Road ahead

The Dynamic Coalition will continue to work on these issues with a goal of producing output for consideration during IGF 2018. The stakes continue to go up, and more influential players will further progress in the field. The G7 Ministerial Meeting in Torino (September 25 - 26, 2017) adopted in its Declaration a special section on a "G7 Multistakeholder Exchange on Human Centric Artificial Intelligence for Our Societies" (Annex 2) that says: "the economic, ethical, cultural, regulatory and legal issues linked to artificial intelligence [need to be] thoroughly researched and understood by policy makers, industry and civil society." AI and IOT are not the same, but very interlinked. The G7 announced its intent to start a "multistakeholder dialogue" on those issues but it did not outline how this will be organized. The Torino document has a strong support for the multistakeholder approach in Internet Governance and refers to the NetMundial Declaration on Principles for Internet Governance from Sao Paulo (2014).

For more information on meetings that have taken place in the past, and meetings planned, and on progress on this document, please go to http://www.iot-dynamic-coalition.org