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 applicability 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. During the IGF 2018 in Paris, France, participants agreed that the following statement makes sense and should be considered by all involved in rolling out, using and overseeing IoT devices, applications and services.

Internet of Things Global Good Practice

The Dynamic Coalition agrees that the general assumption that legislation alone is not 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 there is not yet on a common understanding on this. A proposed "ethical approach" should be "sufficient" from a civil society point of view, and "do-able" from a business point of view, and reasonable from a government perspective – in particular when considering good practice from a global perspective, which is to reflect an understanding of the world to be diverse, and need to be inclusive, by nature.

The following was concluded (see IGF 2018 report on the Open Meeting of the DC IoT):

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 justified 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 regulate where necessary while holding 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 potential 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 rapidly evolving, both in terms of numbers of deployed devices and in terms of functionality and functioning through broader sharing and relating of data ("Big Data") and decision making by machines (machine learning and artificial intelligence), 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. And with every consideration it is crucial to take into account that there is a growing amount of legacy systems on the Internet, still connected, not always in active use anymore yet still useable – for the good or for the bad.
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 IoT systems, products, and services taking ethical considerations into account from the outset, in the development, deployment and use phases of the life cycle, thus finding an ethical, sustainable way ahead using IoT to help to create a free, secure and rights enabling based environment: a future we want.

2. Towards an ethical framework for IoT 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 IoT products, systems and services around the world require:

A. Meaningful Transparency to users: understandable and clear terms of use, including an overview of what is tracked and 'why', and '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 them, 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 could compromise the security of an IoT deployment or which impact elements of innovation that are protected by Intellectual Property laws;; neither of those elements should negatively impact the ability of a user to have the needed information, in an accessible and understandable form, to make decisions about the use of a product.

B. Users' ability to understand and exert appropriate control of personally identifiable data produced by, submitted to, 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 and whether the data is generated at all, to being able to appropriately delete historic data, and 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 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 users 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 their 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 make sure that historic data are no longer related to individual accounts unless explicitly agreed otherwise ("the right to be forgotten" in practice – and effectively anonymized 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 and also from the perspective of potential physical damage or harm. Therefore, individual IoT devices, systems and the data related to the systems need to be secured adequately. In this it is important that the different actors in the value chain of IoT supported services all accept their responsibility: device manufacturers, access providers, application service providers, cloud providers, and the end user her- or himself. In this it is important to note that no responsibility can be dumped upon end users that relates to an unreasonable or unrealistic expectation of knowledge and care. An additional challenge raising from some IoT applications is the fact that the devices and systems may be in use for a long time during which the security requirements may change. A third element of concern is that devices may be "captured" and used to do harm to third parties, for instance as parts of botnets that are used to instigate distributed denial of service (DDOS)attacks. Good practice includes at least assessment of security impact of every part of an IoT system when developing or deploying, secure update-ability of software in devices, not delivering IoT objects with default passwords to end users, ensuring the ability to change passwords. Further development of approaches, methods and systems to increase the justifiable trust in IoT enabled environments is ongoing, and deserves regular stock-taking.
D. Privacy: All stakeholders in the Internet of Things value chain, including governments and industry, whether making direct or indirect use or 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 supporting mutual trust amongst human (individual or institutional) entities involved in loT systems and justified trust in their non-human system components: devices, applications and supporting operations. Justified 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, meaning that responsibilities are clear, and if someone responsible (person or organization) fails to live up to what is promised or required, they will be held 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 that stakeholders agree on this framework for transparency and accountability, with respect for current legislation and pre-empting evolution of the regulatory framework to reflect changes in values and needs of citizens. Stakeholders must also understand that additional specific commitments may be needed or useful for specific IoT applications.

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 them. Measures by stakeholders are to include actively 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 loT Good Practice ("Ethical loT") 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 outcomes (and failure) is clear.

loT deployment in the development context needs to be considered as it can help achieve specific development goals. Next to the necessary investment in infrastructure and openness of that infrastructure, availability of both licensed and unlicensed spectrum is needed.

4. Education and awareness

Related to loT, individuals should have the right to information on which they base their interactions with loT - 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 bases. It is important to ensure that all stakeholders are able to participate in the discussions, and it is up to governments, academic institutions and the private sector to help ensure user education. We call for other IoT codes of conduct and trust frameworks to explicitly take the principles expressed in this paper into account, and build upon it. In addition, we call for providing examples of practice around the world that help illustrate “good practice” (as recognized 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 going forward. During the IGF it was concluded that:

1. IoT good practice principles must factor in (at least) four primary goals: security (of data and in their own person), consumer trust (including privacy / ability to control their own data), meaningful transparency (no hidden consequences), and affordability (both to produce the technology and to access it).
2. It is the responsibility of the larger IGF stakeholder ecosystem to educate and engage with public / government sector stakeholders on the progress of these discussions.

It is also noted that:

- It is imperative to understand and take into account the cultural norms / biases as formulate IoT good practice principles.
- These principles need to be voluntary in nature but also include a mechanism to encourage the adoption of them in the creation and marketing of new technologies.
- The IoT good practice principles will both impact and be impacted by the evolution of other disruptive technologies (e.g. artificial intelligence) but, so too, the principles can help guide recommendations for best practices for these technologies.

Going forward, more work needs to be done on global approaches towards ethics and IoT, and global approaches to IoT Security.

In the full understanding that legislation alone will not be able to guide development, and may even hamper innovation (if too restrictive, aiming to prevent further damage to society and citizens), we call for industry and the technical community to comply with the IoT global good practice principles, and for all stakeholders to further "spread the word" and have a continued dialogue on good practice, considering the wider application context including Big Data and Artificial Intelligence.

This document is based on the input document to the Open Meeting of the DC IoT during IGF2018 in Paris, and reflects the outcome of the discussions during this meeting.For more information on meetings that have taken place in the past, and meetings planned, and on progress on this document, please go to **https://medienstadt-leipzig.org/dciot.**