

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

Since the IGF in Hyderabad, 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. At the IGF 2015, in Joao Pessoa the DC-IoT presented and discussed its first draft paper on Internet of Things Good Practice policies.

During the session we found agreement that law alone will not be sufficient to “guide” responsible development of IoT products and services and 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 was 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 2015 DC IoT meeting report, and now in the text below.

As in 2015, 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 towards the IGF meeting in 2017, further moving towards a "rough consensus", global, multistakeholder position on an ethical approach towards IoT development and deployment.

The paper presented below is a further iteration of the paper presented to the IGF in 2015, taking into account the comments during the on-line commenting period, the results of the dialogue during the DC IoT meeting during the IGF 2015, and the further results during the dialogue at EuroDIG 2016 in Brussels.

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, 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.
- C. The Internet of Things, like the Internet, should be open, secure and accessible to all people.
- 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 social care, to agriculture, food chains, security and environmental sustainability, and its development should thus be fostered and stimulated.
- F. The Internet of Things is in its early phase and it is still evolving. Therefore, not all of the technical and the governance issues have been considered yet. Especially, the issues of security and privacy will need to be considered to ensure the 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).

1. Internet of Things Good Practice Principle

Internet of Things Good Practice aims at developing IoT products, ecosystems 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 IoT helping to create a free, secure and enabling rights based environment: a future we want, full with opportunities to embrace.

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 expressed in outline in the Universal Declaration of Human Rights and the Sustainable Development Goals that are adopted by the General Meeting of the United Nations.

Good practice in IoT products, ecosystems and services around the world require:

- A. Meaningful Transparency to users: understandable and clear terms of use, including an overview what is tracked, and why, and how that information is used in IoT ecosystems and how it is shared with other companies or institutions 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;
- B. User control of data produced by or associated with an application. This is necessary for multiple reasons, ranging from 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 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. In addition, it is clear that unless all people and objects around turn off tracking, "collateral tracking" may still happen;
 - 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 machine learning (and eventually possibly artificial intelligence) that may lead to change in behavior of IoT environments the user is confronted with;
 - d. Consider the ability to delete and export historic data: or at least makes sure that historic data are no longer related to individual accounts ("the right to be forgotten" in practice - and data can still be used for business process innovation etc.);
- C. Security: IoT devices may have real, physical world connection and therefore, the implications of security may have physical or kinetic consequences. Therefore, the security of individual IoT devices, systems and the data related to the systems need to be secured adequately. An additional challenge raising from some IoT 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.
- D. Privacy: All stakeholders in the Internet value chain, which includes the Internet of Things, including governments and industry, including direct use and reuse of data, should comply with privacy and data protection norms and international law. In particular, any techniques to inspect or analyze Internet traffic shall be in accordance with global privacy and data protection obligations and subject to clear proactive legal protections.

3. Implementation and enforcement

An important element of IoT Good Practice is its supporting mutual trust amongst all the components of IoT ecosystems: 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") 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 the evolution of the regulatory framework reflecting the changes in values and needs of citizens.

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 be educated or at least have access to information on which these individuals base their actions with IoT - systems, - infrastructures and utilities. This education and proliferation of information needs to be done in a manner that is accessible to the non-

expert and may benefit much from Open Educational Resources and prosumer knowledge base. It is important to ensure that all stakeholders are able to participate in the discussions.

Road ahead

The plan of the Dynamic Coalition is to continue to work on these issues during 2016 and 2017 with a goal of producing output as output for consideration in 2017. We invite feedback on IoT Good Practice during a number of workshops, and on-line, during the coming year.

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>