

IoT: do we have a choice?

IFIP Position Paper

(version 10-09-2018)

1 Introduction

IoT is hot. Many experts and organizations are addressing the topic in policy statements, papers and conferences. There are many aspects to be looked at when talking about IoT. IFIP wants to contribute to the discussion by investigating what choices can or must be made regarding these various aspects. And by addressing the question what choices various stakeholders should have. This paper briefly lists the aspects and dimensions of the IoT. Then IFIP's position on some major questions and choices is presented. It concludes with an overview of (possible) contributions that are already made or can be made by IFIP and its member societies and by ICT professionals in general to the open questions.

2 Definition

More than one definition of the IoT exists. For the essence of this paper the definition is not the most important element. It was therefore decided to neither choose one from the list nor create one of our own to guide the discussion. A few examples of definitions are added in an annex at the end of the paper. It is important to note however that while the IoT can be seen as a global infrastructure several vertical domains for distinct applications can be defined.

3 Aspects and dimensions

3.1 Opportunities versus threats

Like every new technology also the Internet of Things offers opportunities for progress and application for beneficial purposes while at the same time it introduces or increases risks and threats. When addressing choices about various aspects, both sides will be considered.

3.2 Dimensions

As mentioned in the introduction, there are many aspects to be looked at when talking about IoT and discussing what choices can or must be made regarding these various aspects. In the current literature, many lists of aspects are a mixture of types of aspects. In an attempt to structure this, a three-dimensional model is proposed. The three dimensions would distinguish choices to be made:

- by whom (individuals and organizations)
- during which phase of the lifecycle of an IoT application
- about which issues.

3.2.1 By whom

Choices are to be made by individuals and by organizations. An individual can be in the role of ICT professional developing IoT infrastructure or IoT applications or in the role of a user of IoT. Organizations can be in the role of user, of ICT industry developing IoT hardware and software or of authorities / regulators responsible for policies, standardization, legislation and other types of regulation.

3.2.2 Phases of an IoT lifecycle

Many lifecycle phases of products, systems and applications can be found in literature. Generally speaking the following phases can also be distinguished for an IoT application:

- Analysis / design;
- Development / production;
- Operation / maintenance;
- Disposition.

3.2.3 Issues

The broad spectrum of issues to be considered includes:

- Technical issues
- Legal issues (including liability)
- Ethical issues
- Education, training, awareness
- Usability and accessibility issues / freedom of choice and personalization issues
- Environmental issues
- Privacy issues
- Risks, Security, Resilience
- Impact on persons and society
- Professionalism / duty of care

4 IFIP's position on major questions and choices

This position paper is not a series of positions on the technologies in the Internet of Things but it is a series of statements about choices that can be made and / or should be made and that should be enabled by technologies and / or policies. As a federation of societies of ICT professionals, for our positions we take the perspective of a human centred IoT: *"A human centred IoT would imply an environment where IoT will empower people and not transform them into hostages of technology"*¹.

The most elementary choice is the question "can I choose not to use an IoT?". The answer to this question is not straightforward for all cases. There may be arguments e.g. for national security or environmental reasons to limit the choices. In the following paragraphs this and a number of other questions will be addressed. In each paragraph IFIP's position on a variety of aspects is presented and substantiated.

¹ EC Staff working document "Advancing the Internet of Things in Europe", April 2016, <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe>

The paragraphs are following the dimension “By whom” (see paragraph 3.2.1).

4.1 ICT professional

- I. **IFIP’s position is that an ICT professional should have sufficient professional and ethical competencies to make the right choices when designing, developing, implementing, operating or managing software / hardware as part of an Internet of Things that is able to offer choices to its’ users.**

Having sufficient professional and ethical competencies is a general requirement for ICT professionals. However, in an IoT environment this is especially important because users may not be aware of the fact that choices are, could or should be possible. Users also may not be in a position to demand choices or to influence the usage of collected data. Therefore, the professionals should see to it that such choices are embedded and offered. The constraint of course is that also an ICT professional may not be in a position to decide upon the design etcetera. This means that a condition for making this work is to have professional and ethical competencies not only embedded in the codes of ethics of societies of professionals but also in companies’ policies. And to have a work environment that is supportive of putting these policies into practice.

- II. **IFIP’s position is that ICT professionals have a choice to educate / inform users on both the potential benefits and the risks of the Internet of Things the users are confronted with.**

Users should be informed about the benefits and risks of Internet of Things applications they use. If the owner / developer of such applications does not (sufficiently) inform the users, ICT professionals have a choice to do this, for instance via research papers and publications. In order to be able to do this, there should be no legal liability when publishing such results.

4.2 User

Both individuals and organizations can be in the role of user.

- III. **IFIP’s position is that users at least must have a choice to switch of the connection / not use the smart part of smart devices. In other words, users should have an opt in or opt out choice.**
- IV. **IFIP’s position is that it supports the possibility to empower users in such a way that they can control and personalize the behaviour of smart objects and associated applications through appropriate design tools even if they do not have programming knowledge.**

For example, if a smart meter gives the energy company full insight in the user’s energy consumption, the user should have the option to not provide this information. This means that policies / regulations / legislations should allow for this and also the technology / devices should make this possible. Users should be aware of the consequences of both the opt in and opt out choice.

There may be applications or circumstances where it is not possible or desirable to give users an opt in or opt out choice, for instance in cases where national security is at stake. When this is the case, it should be clearly explained to users.

- V. IFIP's position is that users should inform themselves about the various aspects (benefits / risks) of the devices that are connected in the IoT they are using.**

While ICT professionals and ICT industry have a choice, or actually an obligation, to educate / inform users, these users have a choice, or also perhaps an obligation, to inform themselves. This can be by simply reading the information provided or asking for information if that is not provided. A condition to help users is the availability of "a set of the right questions".

- VI. IFIP's position is that it should be encouraged to involve users in the design / development of IoT (applications).**

Users are not only passive users but are also often people who possess knowledge and can contribute in the design/development of IoT. Having a say – if possible, in the design process would be one way to make them more active.

4.3 ICT Industry

- VII. IFIP's position is that the ICT industry providing IoT applications should inform users about the benefits and potential risks.**

This should not be a choice but an obligation. It has to be clear for users for which purposes data are collected. A mechanism needs to be in place to assure the security and protection of such collected data and providers should inform users about these mechanisms. It should also be made clear what the consequences of either choice (opt in or opt out) are.

- VIII. IFIP's position is that the ICT industry should not develop IoT applications that provide data that can be used without the owners of the data knowing about the use or consenting to it. The ICT industry has a choice not to do this.**

Owners of data, both personal data or data that can be linked to persons in an indirect way, should know who is doing what with their data and they should have the right to give consent for such usage. This may not be possible in all cases but that should then also be clear.

4.4 Authority / regulator

- IX. IFIP's position is that policymakers / regulators should take into account the interests of users when regulating the use of (personal) data (including data that can be linked to a person in an indirect way e.g. via home, car, etc).**

Policymakers / regulators have a choice to balance the interests of various stakeholders in the applications and their data. It is important that policies and regulations provide the conditions for the choices that users and providers can or should be able to make.

5 Possible actions

IFIP, its member societies and their members can contribute to solve the “choice problems” addressed in the previous chapter. What can be done:

- Check / promote the presence of the professional and ethical competencies issue
 - in codes of ethics of professional societies
 - in companies’ HR policies
- Provide a “set of the right questions”
- Promote the position statements to the professionals, users, industry and authorities.
- Research the benefits and risks of the various Internet of Things applications
- Increase research of those aspects that are insufficiently addressed and / or that are gaining more and more importance. Examples could be:
 - With the increasing number of IoT devices will there be energy to run all of them? IoT is requesting the production of low power devices, that means the use of optimisation techniques, and the direction is to have dedicated devices to each need or function.
 - With the increasing number of IoT applications, ethical (privacy, surveillance etc) and security issues are becoming more and more important due to the use, design and implementation of such applications.

6 Annex. Definitions

ITU

According to ITU-T Y.2060:

“Internet of Things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting physical and virtual things based on existing and evolving interoperable information and communication technologies.

Thing: an object of the physical world or the information world, which is capable of being identified and integrated into communication networks.

Device: a piece of equipment with the mandatory capability of communication and the optional capabilities of sensing, actuation, data capture, data storage, and data processing.”

Wikipedia

(https://en.wikipedia.org/wiki/Internet_of_things (14 August 2017, 21:22 Amsterdam, slightly adjusted)

*“The **Internet of Things (IoT)** is the inter-networking of physical devices (also referred to as “thing”, “object”, “connected devices” or “smart devices”) such as vehicles, buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. The IoT allows objects and their environments to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants,*

smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure."

Gubbi et al, 2013, p. 1647

"The worldwide network of interconnected objects uniquely addressable based on standard communication protocols." and "Our definition of the Internet of Things for smart environments is: Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with Cloud computing as the unifying framework."

Gubbi, J. Buy, R. Marusic, S and Palaniswami (2013) Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), pp 1645-1660

Preliminary draft