IoT: do we have a choice?

IFIP Position Paper[1]

Final version 31-03-2019

1 Introduction

The Internet of Things (IoT) is a challenging topic. 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. The International Federation for Information Processing (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.

Most of the positions and questions also apply to other ICT areas (such as AI) and even to ICT in general. Nevertheless, it is useful to have focussed statements on specific areas such as the IoT in order to draw attention to the positions and questions and to follow up on them when working on a specific area.

2 Definition

There are many definitions of the IoT. 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. Furthermore, there is a considerable overlapping with the related concept of Cyber-Physical System (CPS). According to some perspective, all IoT systems are CPS, while some CPS might not involve Internet.

[1] This position paper was drafted by the IFIP Domain Committee on IoT. The first draft was discussed at the IFIP IoT 2018 conference and the IFIP GA 2018 meeting. The enhanced version was accepted by the IFIP Board in March 2019.

3 Aspects and dimensions

3.1 Opportunities versus threats

Statement I. Opportunities and threats

Like every new technology, 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. Some facets can have both, think for instance about security and safety. The IoT can offer new opportunities for monitoring safety on the one hand while introducing new security risks on the other. It may have an impact on employment and labour circumstances, again both on the positive and negative side. It has potential for improving people's life, think about personalized medicine, but may also infringe privacy. The preservation of the environment may be served by IoT applications while at the same time the energy consumption might be a burden on the environment. When making choices in developing, manufacturing and using IoT devices and applications, these choices should be well-balanced and based on appropriate knowledge and skills.

3.2 Dimensions

As mentioned in the introduction, there are many aspects to be looked at when talking about the 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, by organizations and by society as a whole. 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. Society define general acceptance principles and co-evolve in parallel with the new possibilities offered by IoT.

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 and evolution;
- Disposition.

3.2.3 Issues

The broad spectrum of issues to be considered includes:

- Technical issues

- Environmental issues
- Socio-organizational issues
- Personal and societal issues
- Security and Privacy issues
- Legal and Ethical issues
- Professionalism and Education issues

While these issues can be addressed and researched as stand-alone topics, also strong links between them are in place and these connections need to be taken into account when making choices. Technical issues can have an effect on the environment, both negative and positive. Technical issues have an effect on society and therefore socio-technical issues have to be addressed as well as personal and societal issues. And from there the link with security, privacy, legal and ethical issues and professionalism and education is obvious.

This paragraph provides some reflections on these issues giving a bit of background for the questions and choices addressed in chapter 4.

Technical Issues

The increasing number of devices connected in the Internet of things is increasing power consumption year by year, in such a way that in a near future there will be no sufficient power plants to provide the needed energy to run all IoT devices. We have also to consider that many energy sources are sources of pollution. To cope with this, it is becoming mandatory huge efforts to optimise the power consumption of IoT devices, from the small ones to big ones. The power consumption of some small devices can have an absolute small value, but as most of them are replicated thousands or millions of times, they also need power optimisation.

Power optimisation must be done in all levels of design abstraction, from the specification till the layout of devices, that more and more should be implemented using just one chip. At architecture level, for example, the use of modules dedicated to execute one specific approach, meaning that they will be smaller and fast than when the function is executed by a traditional CPU or GPU. These dedicated modules are being called “hardware accelerators”. In a SoC (System on Chip) based on hardware accelerators, only the ones that are being used in a specific moment will be power on, the others should be power off. The effect of having several modules shut down for a moment is called ‘Dark Silicon”. The power optimisation at physical design demands an optimisation of the number of transistors, as leakage power is related to the number of transistors.

This means that more and more the IoT devices must be dedicated ones (ASD – Application Specific Devices) and implemented by just one chip, in order to reduce power consumption. Software designers should also be aware of how to produce a software that will use less energy to run, by optimising the number of transitions (0 to 1 or 1 to 0) to perform a task.

Furthermore, with the increasing intelligence and autonomy of devices and sub-systems, complemented by hyper-connectivity, IoT needs to be considered at higher abstraction levels, in the context of complex Cyber-Physical Systems / Systems-of-Systems. Issues such as collective intelligence, and collaborative cognitive systems then naturally emerge.

Environmental issues

Having addressed the power consumption of IoT devices and the effect this may have on the environment in the previous paragraph, there are also other effects of the IoT on the environment. Not all negative, IoT applications can contribute to sustainability. IoT devices for instance can monitor energy consumption of household appliances (refrigerators, washing machines, etc) and warn if the energy consumption exceeds a certain level. And this kind of monitoring is not limited to households but also applies to industry. Another use of IoT connected sensor networks is protection against hazards such as water and air pollution. While such sensor networks already exist, the question is whether this can be taken to the next level by measuring pollution at the source. For instance measuring the pollution level of the waste water when it leaves your home or factory. That will lead to security and privacy issues, legal and ethical issues and societal issues.

Socio-organizational issues / Personal and societal issues

Our society is now dramatically influenced by the exponential increase in connectivity of objects, systems, organizations and people, leading to a hyper-connected world. In this context, IoT cannot be analyzed from a strict technological perspective but rather from a socio-technical perspective. Furthermore, as the number of devices and systems connected to Internet increases, there is an urgent need to address their organizational and governance structures, as well as their inter-relationships with other societal organizational forms. Complementarily, impacts on society and the emergence of new business models need to be properly addressed.

On the more personal side issues like usability and accessibility have to be investigated. And the questions of freedom of choice and options for personalization are not always easy to answer. The impact on individuals and society can be huge.

Security and privacy issues / Legal and ethical issues

These categories of issues include a whole lot of obvious questions: - who collects data; - where are they stored; - who has access to the data; - are they anonymized or can the data be linked to individuals (or companies); - who is responsible for the security of this information; - who decides what an acceptable risk level is; - how much control do users have with respect to their own data; - what is “your own data”, in other words, who owns the data; - what are the liability arrangements; - what can be legally enforced in terms of collecting data (think of the environment example of collecting information at the source about the pollution level of waste water); - who is responsible for decisions based on incorrect data. And there are undoubtedly more questions to be answered.

Professionalism and education issues

The final set of issues relates to all others. As written in the first statement, it is essential that choices are well-balanced and based on appropriate knowledge and skills. This means that professional behaviour is essential (which includes duty of care and ethical dimensions). But how can this be achieved, what are the means to reach that goal. Education is a “conditio sine qua non” in that respect. Education to be seen in a broad sense, including formal education, training, awareness, life-long learning.

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"*[2].

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.

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

4.1 ICT professional

Statement II. Competences

IFIP's position is that an ICT professional should have sufficient professional and ethical competences 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 competences 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 competences 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.

Statement III. Education of users

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, maybe even a duty, to do this, for instance via research

[2] 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

papers and publications. In order to be able to do this, there should be no legal liability when publishing such results.

Statement IV. Multi-disciplinary perspective

IFIP's position is that ICT professionals need to address IoT from multi-disciplinary perspective, thus exercising effective dialogue with many other knowledge disciplines.

In fact, IoT affects all domains and receives contributions from multiple knowledge areas. Effective systems and solutions shall result from a fluid dialogue between different knowledge domains, which requires proper openness from the new generation of ICT professionals.

4.2 User

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

Statement V. User opt in / opt out choice

IFIP's position is that users at least must have a choice to switch off the connection / not use the smart part of smart devices. In other words, users should have an opt in or opt out choice.

Statement VI. User control and personalization empowerment

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.

Statement VII. User obligation to get informed

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".

Statement VII. User involvement

IFIP's position is that involving users in the design / development of IoT (application) should be encouraged, materializing processes of co-creation / co-innovation.

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, as well as in the assessment of solutions – would be one way to make them more active.

4.3 ICT Industry

Statement VIII. Industry to inform users

IFIP's position is that the ICT industry providing IoT applications and systems 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.

Statement IX. Industry responsibility in IoT development

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

Statement X. Policymakers / regulators to balance interests

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, it's 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 and systems
- 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.
    - New organizational and governance models; towards collaborative societies / ecosystems of smart systems.

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

Related concept of CPS:

NIST
"Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas."
https://www.nist.gov/el/cyber-physical-systems

NSF
Cyber-physical systems (CPS) are engineered systems that are built from and depend upon the synergy of computational and physical components.
https://www.nsf.gov/pubs/2013/nsf13502/nsf13502.htm