Internet of Things

Commission Staff Working Paper on Early Challenges regarding the "Internet of Things"

SEC(2008) 2516

Joint ANEC/BEUC answer to the consultation

BEUC Contact: Emilie Barrau – legal@beuc.eu
ANEC Contact: Chiara Giovannini chiara.giovannini@anec.eu
BEUC Ref.: X/068/2008 – 27/11/08
ANEC Ref.: ANEC-ICT-2008-G-062
BEUC, the European Consumers' Organisation, www.beuc.eu
ANEC, The European Consumer Voice in Standardisation, www.anec.eu

Summary

This paper aims at commenting on the aspects of the Commission Staff Working paper on the Internet of Things relevant from a consumer point of view.

ANEC and BEUC recognise that, though more a concept than a reality, the Internet of Things has the potential to modify the existence of European citizens' everyday life in terms of quality of life. However, we believe that the possible negative impacts should also be addressed in the future European policy on the Internet of Things. For instance, its various components/elements - such as tags, readers, sensors, mega databases -… might have a big impact on energy consumption.

ANEC and BEUC are equally concerned by the challenges that the IoT raises in terms of new threats to consumers' fundamental rights, of which the protection of privacy and personal data, to security but also regarding uncertainties on the impact on human health such as the level of exposure of people to multiple sources of electromagnetic fields (EMF).

Consumers need confidence to fully embrace the Internet of Things in order to enjoy its potential benefits.
ANEC and BEUC call for the following core consumers' principles to be adopted by the future European policy when designing and developing for the Internet of Things to be adopted and recognised by the future European policy on Internet of Things:

- Openness
- Interoperability
- Neutrality
- Trust
- Transparency
- Protection of privacy and fundamental rights
- Security
- User control
- Representativeness
- Respect of European values
- Liability and accountability
- Respect of the environment
- Health/safety
- Reliability

The Internet of Things needs to be built in such a way as to ensure an easy and safe user control. Consumers need confidence to fully embrace the Internet of Things in order to enjoy its potential benefits.

We are convinced that the only way for the "Internet of Things" to become a reality is by becoming the "Internet for People".

This joint ANEC/BEUC paper aims at commenting on the aspects of the Commission Staff Working paper on the Internet of Things relevant from a consumer point of view.

--°--

PRELIMINARY REMARKS ON THE INTERNET OF THINGS

We would like to congratulate the European Commission for this open consultation that demonstrates Europe's pro-activity in shaping a better future for European citizens.

While we understand that the Internet of Things (IoT) is still to a very large extent a concept or a vision rather than a reality, we would like to point out that the name "Internet of Things" in itself misleading - in particular for non-experts such as citizens - as it will not only link things or objects but also people.

ANEC and BEUC recognise that the IoT will bring about new opportunities and new societal services that will improve the quality of life of European citizens.

We would welcome though if the "huge benefits"[1] claimed by the European Commission in this paper could be documented with further details. We also call on the Commission to give the aspects that may be linked to concerns more consideration. For instance, tags, readers, sensors, mega databases… might have a big impact on energy consumption. Has the Commission fully assessed what the overall energy consumption of the IoT components will be? Similarly, as regards recycling, the disposal of RFID tags will create waste management difficulties that equally need to be considered.

We also regret the lack of reference to ethics, dignity and human relationship aspects in the examples on e-heath and medication. We would urge for a European Ethics Committee to be created and consulted ex-ante on Internet of Things applications raising potential ethical risks. Also, the digital divide issue should not be forgotten especially as consumers will be more and more dependent on the Internet/new technologies for exercising fundamental rights such as e-voting.

ANEC and BEUC are concerned by the challenges that the IoT raises in terms of new threats to fundamental rights, of which the protection of privacy and personal data, and the right to security are key. We would also like to highlight uncertainties on the impact on human health such as the level of exposure of people to multiple sources of electromagnetic fields (EMF). We are calling for the "precautionary principle" to be applied to the deployment of IoT systems.

Many challenges need to be overcome and risks still need to be assessed and addressed.

[1] Staff working paper – page 4.

Policy Challenges in RFID Architectures

While we believe that RFID will be an important element of the IoT, ANEC and BEUC would like to recall that RFID applications are still in their infancy – as to a very large extent only pilot projects are running - and that consequently the experience gained from RFID applications has to be put into that perspective.

When it comes to the architecture of the IoT, we should learn from the Internet experience i.e. that "*mismatches between original design goals and current utilisation are now beginning to hamper the internet's potential*"[2].

Core consumers' principles

ANEC and BEUC would like to stress the importance that the design of the architecture of the IoT will have on European society. As consumers' organisations, we believe that – at the very least - the following principles are essential to the future development of the IoT and should be formally adopted and respected:

- *Openness*
  The IoT should be open to all – as the current Internet is.
- *Interoperability*
  In an interconnected world, interoperability of the various technologies and services is key.
- *Neutrality*
  Network neutrality is vital. An Internet without restriction on access to certain content and applications, or limitation on the types of equipment that can be attached to the network.
- *Trust*
  The IoT will only be used if it can be trusted by consumers.
- *Transparency*
  Especially when it comes to governance.
- *Protection of privacy and fundamental rights*
  Privacy and personal data protection are fundamental values.
- *Security*
  Security of the components and of the overall structure of the IoT.
- *User control*
  Consumers should be fully informed about the impacts of IoT applications and should remain in control.
- *Representativeness*
  Representation of governmental authorities, civil societies and consumer organisations in the decision making process needs to be ensured.
- *Respect of European values*
  Fundamental values such as democracy and ethics, enshrined in European law, should be respected.
- *Liability and accountability*
  Chains of responsibility should be clearly established and remedies must be available.

[2] Bled declaration - http://www.future-internet.eu/fileadmin/documents/bled_documents/Bled_declaration.pdf

- *Respect of the environment*
  The environmental impact of IoT applications and components should be minimum in terms of energy consumption and waste management.
- *Health/safety*
  IoT applications will lead to increased levels of exposure of consumers to multiple sources of electromagnetic fields (EMF) emissions. Legislation and standards should always ensure the highest level of consumers' health and safety protection.
- *Reliability*
  Where critical appliances are in operation in a IoT system (e.g. healthcare devices, heating systems, etc) means of reporting the failure, providing support or providing back-up power should be provided.

User control

Consumers – but also businesses – hardly trust what they cannot control and/or what they cannot understand. User control is linked to trust and acceptance of the IoT. Consumers should remain in control and should decide who should have access to their data and under which conditions. However, this control should be easy to exercise and should not burden consumers with endless requests.

Therefore, the IoT needs to be built in such a way as to ensure an easy and safe user control. We believe that the best way to get to this result is by implementing privacy and security by design.

Security

We support the focus on new security aspects. Technical as well as legal means will be needed to ensure secure exchange of information through the IoT – in particular when this has an impact on consumers' privacy.

Privacy and Data Protection

From a consumer perspective, data protection and privacy is one of the major challenges of the IoT. Above all, the risks of identification and profiling of consumers should not be underestimated.

Due to mass storage technologies and the increasing connectivity of databases, the Internet of Things will exponentially increase the possibilities of tracing and tracking consumers. The multiplication of information collection from objects, readers, tags, sensors… everywhere – from the workplace, through public transport, and within individuals' homes will facilitate this operation. The European Commission acknowledges that the first visible signs of the IoT are RFID and Near Field Communication (NFC)[3]. It is therefore important to set up the right framework and address the relevant challenges already today. We therefore are looking forward to the upcoming RFID recommendation[4]. We further support the call for a new consumers' right - "the right to the silence of the chip" - made at the French Presidency conference on the Future of the Internet[5].

---

[3] Staff working paper – page 4.

[4] Please refer to ANEC/BEUC comments on the draft recommendation - X/029/2008/ ANEC-ICT-2008-G-017 – April 2008.

[5] Speech from Eric Besson, French Minister, at the French Presidency conference on the Future of the Internet, 8 October 2008 Nice.

ANEC and BEUC strongly call for the data protection principles (data minimisation, lawful and fair collection, proportionality, finality, accuracy and transparency, right of access and rectification, confidentiality and security of processing) to be fully respected and implemented in the technology when building the IoT. Therefore, we fully support the European Commission when it emphasises the necessity to "*ensure that the fundamental rights of individuals/citizens to privacy and data protection [...] are adequately captured in the design and functioning of the Internet of Things*"[6].

However, we are unsure that self-regulation is the best way to achieve guidance on how to apply data protection rules to new technological developments. We fear that in a self-regulatory environment there is not enough pressure on industry and/or other parties to set themselves high standards. We feel that a mandatory approach would be required given the possible far reaching impact on privacy both of individuals, business and all other parties.

At the same time, the impact of the IoT on citizens may be wider than just privacy – as it will have an impact on human relationships – how people interact with one another - and on the perception of our society. This wider dimension would need to be carefully assessed.

Identity Management, Naming and Interoperability Requirements

ANEC and BEUC believe that identity management – together with other technical solutions - will foster consumer protection. In this context, we call for the endorsement of the PRIME principles[7] when designing identity management mechanisms:

1. design must start from maximum privacy;
2. explicit privacy governs system usage;
3. privacy rules must be enforced, not just stated;
4. privacy enforcement must be trustworthy;
5. users need easy and intuitive abstractions of privacy;
6. privacy needs an integrated approach;
7. privacy must be integrated with applications.

When referring to mandates to be issued for the elaboration of standards to support public policies, only European Standards organization (ESOs) and not Standards Developing Organisations (SDOs) should be mentioned, according to the existing legal framework. The principle of openness and transparency should always be respected in developing standards. It is in this regard essential to establish the most appropriate mechanisms for involving consumers' representatives in the standards making processes, if relevant for them.

Fostering Innovation and Research

We are sympathetic towards the Commission views as regards open standards, open architectures, user-friendliness, competition and interoperability. We support the adoption of interoperable standards for the technologies that will be applicable to the IoT. Proprietary solutions could lead to companies 'owning' the infrastructure to dictate preconditions, leaving consumers financially or physically 'tied-in' to a particular system. It is therefore essential for standards to ensure consumers can use an IoT application or service without having to buy a specific software or system.

---

6 Staff Working Paper, page 12.

7 Privacy and Identity Management for Europe (PRIME) project was a FP6 project that aimed to develop a working prototype of a privacy enhancing Identity Management System - https://www.prime-project.eu/

As referred to in the staff working paper, elderly and people with disabilities are vulnerable consumers that have specific needs. The use of IoT applications must bring to the latter real benefits. Of course, compatibility between mainstream applications and assistive technology, even legacy ones, should be ensured.

As mentioned in the Bled Declaration[8], Research & Development should help "*jointly designing, developing and experimenting technologies ensuring the robustness and security of the networks, managing identities, protecting privacy and creating trust in the online world*".

ANEC and BEUC calls for more public research projects on privacy and transparency enhancing technologies (PETs/TETs), on tags that can be deactivated and reactivated by an authorised party, on multiple digital identities, encryption, authentication and other technical means. On the other hand, existing projects results should also be used, in particular the results of the Safeguards in a World of Ambient Intelligence (SWAMI) report[9].

Standardisation

We share the Commission's opinion on the use of industry fora and consortia deliverables that should not be made at the expense of quality and democracy. From a consumer point of view, the lack of transparency and consensus involved raises concerns because they impede proper consumer participation and could lead to the adoption of non-open standards. Therefore, we believe that a balance between efficiency and openness must always be maintained.
We call for the application of good governance principles. Standards alone should not be used to address consumer issues as this approach tends to shift decision-making from democratic institutions to standards bodies where consumer representation is not balanced.

Standards should be widely available to all interested parties and not be used as a means of market segmentation. Therefore, standards should preferably be free of Intellectual Property Rights or on FRAND basis.

Standards could also be used to address the health, safety and privacy concerns raised by IoT applications.

NEW CONSIDERATIONS - HEALTH, SAFETY, ENVIRONMENT

In ANEC and BEUC's opinion, a new section on health, safety and environment aspects of the IoT should be added.

Safety

Safety of the IoT system and appliances is of paramount importance. For example, if the intelligent house has to carry out tasks automatically and intelligently, it must be done safely and the consumer needs to know this.

The inherent safety of the device as a stand-alone appliance or application is covered by

[8] Bled Declaration – http://www.future-internet.eu/fileadmin/documents/bled_documents/Bled_declaration.pdf
[9] http://ec.europa.eu/research/fp6/ssp/swami_en.htm

the existing safety standards[10] and in many cases this device would be considered as an "unattended" appliance. To ensure the safety of the system as a whole, additional safety measures should be developed for the safety of the device when controlled and operated as an integral part of a IoT system.

Health

In addition, many components in a IoT system will be used in close proximity to each other and radio devices may share frequency bands. The Electro Magnetic Compatibility and Low Voltage Directives and standards do not always address close proximity use. Therefore it will be necessary for such devices to either have better limits than the minimum required by the directive or the inherent limitations of such devices should be made clear to the consumer and installer. Some components such as heart pacemakers, wheelchairs and other medical equipment will require special attention in this respect for possible interferences.

ANEC and BEUC call for new electromagnetic fields EMF exposure assessment procedures for testing compliance with safety guidelines and further research to assess potential health risks of IoT technologies together with exposure assessment procedures. In the meantime, the "principle of precaution" to the deployment of the IoT should be applied.

Environment

The aim would be to achieve products that are environmentally neutral or made of decomposable materials. In particular, the use of some chemicals in IoT products should be reduced[11]. Low energy consumption products are to be welcomed.

END

[10] CENELEC EN 60335-1: safety of domestic appliances (Low voltage directive).

[11] Restriction of use of certain hazardous substances in electrical and electronic equipments (ROHS) Directive 2002/95 EC.