ANEC reply to European Commission public consultation on

"The Internet is gearing up for the next technological revolution: communication with and among objects. How would you envisage the "governance" of such an "Internet of Things" (IoT)?

The Internet of today offers access to content and information through connectivity to web pages and to multiple terminals (e.g., mobiles, TV). The next evolution will make it possible to access information related to our physical environment, through a generalised connectivity of everyday objects. A car may be able to report the status of its various subsystems using communicating embedded sensors for remote diagnosis and maintenance; home information about the status of the doors, shutters, and content of the fridge may be delivered to distant smart phones; personal devices may deliver to a central location the latest status of healthcare information of remotely cared patients; environmental data may be collected and processed globally for real time decision making.

Access to information relating to our surrounding environment is made possible through communicating objects able to interact with that environment and react to events. This makes possible new classes of applications such as smart homes with automated systems to monitor many aspects of daily living, smart grids and intelligent energy management, smart mobility with better control of traffic, or smart logistics with the integrated control of all processes in the entire distribution chain. There are endless examples of this evolution of networked devices, also known as the Internet of Things (IoT).

The Internet of Things holds the promise of significant progress in addressing global and societal challenges and to improve daily life. It is also a highly promising economic sector for sustainability, growth, innovation and employment. But it is likely to have a profound impact on society, in areas like privacy, security, ethics, and liability. The policy challenge is to assess the right trade-off between the potential economic and societal benefits and the control that we want to retain over an environment where machines will gather, exchange, process and store information automatically. The effects on our private and public space require that people and their governments debate the appropriate governance and management of the Internet of Things in the future. To this end the European Commission envisions a recommendation addressing the main issues, of which a number are outlined in the questions below.

The purpose of this consultation is to solicit the views of a wide range of stakeholders and the public at large.

ANEC replies in red.

Questions marked with an asterisk * require an answer to be given.

Section 1: Privacy

The information collected by identifiable smart objects supports innovative Internet applications but may also reveal information on individuals, their habits, location, interests and other personal information. This also applies to persons whose social identity is not known, but might be indirectly revealed (e.g., location, combination of data sources).

The Internet of Things may increase privacy issues also because smart objects may exchange data automatically, potentially without involved humans being aware of it. Automated decisions may create a perception of loss of control (or lead to actual loss of control) because one of the main goals of the IoT is to give some autonomy to the objects for automated decisions. Decisions taken by machines or applications based on sensed data might not be transparent to the "data subjects"[1] and therefore create the sense of loss of control.

NB: the objective of the questions below is to identify how far IoT system deployment requires (or does not require) to adapt/precise/qualify our approaches and principles to safeguard data protection and privacy of citizens.

[1] The human beings impacted by the processing of these data.

Questions:
- Bearing in mind that important benefits for society as a whole, such as in smart transportation systems, smart cities, pollution control, and sustainable consumption, are to be expected with IoT systems, it may be acceptable that data are used beyond the sole purpose of the application (e.g., for a service provider to run statistics on your smart meter usage).
Strongly agree Agree Neutral Disagree Strongly disagree

- I do not expect any benefit from IoT applications.
Strongly agree Agree Neutral Disagree Strongly disagree

- Traditional data protection principles include fair and lawful data processing; data collection for specified, explicit, and legitimate purposes; accurate and kept up-to-date data; data retention for no longer than necessary. Do you believe that additional principles and requirements are necessary for IoT applications?

NB: in case your answer is "agree"/"strongly agree", please specify what additional principles should be addressed in free text box below.
Strongly agree Agree Neutral Disagree Strongly disagree

Right to be forgotten and right to the silence of the chip: In addition to the so-called 'right to be forgotten', i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes, we

would like to suggest to also work on the so-called "right to the silence of the chip" in a IoT environment.

Transparency principle/data use traceability: with high levels of networking (ie not hub and spoke data collection), with access to data at the periphery, coupled with the significant step up in central processing and data mining (Big Data) needed to bring all the potential value of IoT to fruition, there needs to be a balance between the wide spread use of data on IoT for value creation with the individual's perspective (IoT for People/IoT4P). A key IoT4P attribute needed to address both the consumers' and public interest will be the principle of data use traceability so that consumers and the public can find out who is using their data and for what purposes.

- Data Protection Impact Assessments (DPIA) are contemplated for the deployment of applications involving [1] personal data. IoT-based applications require to develop IoT-specific DPIA guidelines.
[1] A DPIA consists in methodology and tools making it possible to verify that an on-line application satisfies with all the regulatory and legislative requirements governing the handling of personal data, before launching the application.
Strongly agree Agree Neutral Disagree Strongly disagree

Please insert comments here, if you wish – maximum 10 lines

Privacy by design and by default: Design privacy from the very beginning in the development of technologies is essential to ensure that consumers' personal data protection rights are respected in an IoT environment. As far as the protection of vulnerable consumers' rights such as children, we would like to suggest to make mandatory the highest level of personal data protection settings when consumers interact with the specific technology ("privacy by default"). From a consumer perspective, data protection and privacy is one of the major challenges of the IoT as the risks of identification and profiling are a real deterrent for consumers.

Section 2: Safety and Security

Just as we need to protect against security attacks in the existing Internet, we should also consider information security and safety implications in the Internet of Things. Within the IoT autonomous objects may act on behalf of people and they will also need adequate protection against false requests for information and protection against unauthenticated commands.

At a minimum, the confidentiality, integrity and availability of IoT data and services must be safeguarded. User authentication, device and data authenticity, and data quality must be ensured. At the same time the data source has to be trusted, while unauthorised modifications of the data have to be prevented.

NB: below questions are to be understood as applicable to data managed by autonomous systems and objects controlling your environment, e.g. the devices in

your home, devices controlling your health status, devices controlling status of your car… which are processed, collected or transmitted without requiring any direct action from you. The aim is to derive how these novel usages drive information security and personal safety requirements.

- Guidelines and standards should be created to ensure data confidentiality, integrity and availability.
Strongly agree Agree Neutral Disagree Strongly disagree

- Guidelines and standards should define policy enforcement principles and requirements.
Strongly agree Agree Neutral Disagree Strongly disagree

- Data life cycle management in the IoT infrastructure includes data creation, processing, sharing, storing, archiving, and deletion of data. Guidelines should be developed to ensure secure and trusted data life cycle management.
Strongly agree Agree Neutral Disagree Strongly disagree

- Guidelines should be created to determine reliability of data and to verify the authenticity/source of data (data provenance).
Strongly agree Agree Neutral Disagree Strongly disagree

- Autonomous control systems whose behaviour may have safety implications (e.g., decisions taken for a car, or made with sensed health data) should be regulated by generic IoT policy principles.
Strongly agree Agree Neutral Disagree Strongly disagree

- The development of guidelines to respect safety and security requirements should be kept to a minimum in view of not compromising the economic viability of IoT applications.
Strongly agree Agree Neutral Disagree Strongly disagree

Please insert a comment here, if you wish – maximum 20 lines

We concerned by the challenges that the IoT raises in terms of 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.
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 the existing safety standards 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.

Section 3: Security of critical Internet of Things supported infrastructures

Political, scientific and industry representatives have repeatedly expressed concerns about the protection of (network supported) critical infrastructures and their dependencies. The risks of possible abuses of and attacks to communication resources and information flows can threaten information security of public utility installations necessary for the well-being and health of citizens.

Thus, it may be considered that the Internet of Things which is expected to allow the connection to the Internet of some 25 billion devices by 2015 and 50 billion devices by 2020 needs more stringent and mandatory information security measures when its services are related to critical infrastructures.

- The future architecture of the Internet of Things may determine accessibility to information and information flows for unwanted intruders. Such future architecture should be based on reference design principles.
Strongly agree Agree Neutral Disagree Strongly disagree

- Public sector role is crucial in driving the definition of the security of future architecture for the IoT.
Strongly agree Agree Neutral Disagree Strongly disagree

- Policy makers should provide guidance on security-by-design and applicable security technologies.
Strongly agree Agree Neutral Disagree Strongly disagree

Please insert a comment here, if you wish – maximum 10 lines
Any guidance developed for safety and security requirements applications must be comprehensive and ensure accessibility for people with disabilities and older people, especially when IoT services are relating to eHealth applications.

Section 4: Ethics - Group 1 – ethical issues

Objects taking decision autonomously without any user intervention, without possible user awareness and "on user behalf" may be perceived as challenging ethical values like the sense of identity, user consent, fairness.

NB: This group of questions focuses on key human values with ethical implications, i.e. values likely to be challenged, ending in "value conflicts" and tensions.

- Identity: IoT applications pose threats to the protection of an individual's identity.
Strongly agree Agree Neutral Disagree Strongly disagree

- Identity: IoT applications could change our sense and definition of personal identity.
Strongly agree Agree Neutral Disagree Strongly disagree

- Autonomy: Insofar as possible, IoT applications should operate under "explicit consent" by its users as with other ICT applications.
Strongly agree Agree Neutral Disagree Strongly disagree

-Autonomy: It is not possible for IoT applications to operate under explicit consent; alternative solutions to safeguard autonomy should be sought.

NB: if your answer is "agree"/"strongly agree", please specify possible approaches in free text box below.

Strongly agree Agree Neutral Disagree Strongly disagree

- Autonomy: IoT applications could interfere with individuals' autonomy when decisions are taken by autonomous systems.
Strongly agree Agree Neutral Disagree Strongly disagree

- Fairness and social justice: Current developments of IoT applications need to take into account the different capacities, constraints, needs and expectations of individuals.
Strongly agree Agree Neutral Disagree Strongly disagree

- Trust: I am concerned about the governance of the quantity of data that will be resulting from the interaction of objects, i.e.how they are used, stored, accessed, by whom.
Strongly agree Agree Neutral Disagree Strongly disagree

Please insert comments here, if you wish – maximum 10 lines

We would urge for a European Ethics Committee/WG 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.

Section 4: Ethics - Group 2 - procedural issues

NB: This group of questions focuses on the procedural, regulatory aspects for ensuring or at least taking care of ethical aspects in the design and deployment of IoT.

- Governance of ethical considerations in IoT: It would be sufficient to establish an "IoT ethical charter" outlining the ethical principles to be respected by any relevant entity when designing, developing and deploying IoT technologies and applications.
Strongly agree Agree Neutral Disagree Strongly disagree

(a) If you agree, please identify key ethical principles which you consider should be part of such charter:
Please state here- maximum 10 lines
(b) Who should be involved in the definition of an "IoT ethical charter"?
Please state here – maximum 10 lines

Please insert comments here, if you wish – maximum 10 lines
We believe that more then a Charter, which we interpreter as a non-binding document, is needed, in order to ensure effective consumer protection from an ethical point of view in the IoT. We suggest for relevant current legislation to be revised to be adapted to the IoT challenges. We are particularly worried by the lack of implementation/enforcement mechanism in the proposed Charter.

Section 5: Open object Identifiers and interoperability

The Internet of Things must be able to identify each and every connected object by its identifier. Industry predicts that the world's nearly 5 billion mobile phone subscribers today may be surpassed by 50 billion connected non-phone devices in 10 years.
Closed solutions that constrain the identification of the connected object may lead to "locked" markets, making it difficult to penetrate for competitors.
Openly accessible identifier solutions may allow smart devices to be used for different applications and be operated by multiple service providers, with unbundling between information and device. The design of an identification, addressing and naming scheme may ensure the identification of a particular object and provide non-colliding addresses in a global scheme with object discovery and resolution capabilities.

NB: the goal of below set of questions is to identify the minimum set of interoperability requirements applicable to objects naming and addressing to support competition and consumers choice.

- A number of use cases and business scenarios will require sharing a given IoT platform between multiple service providers.
Strongly agree Agree Neutral Disagree Strongly disagree

-A number of use cases and business scenarios will require access to multiple IoT platforms by a single service provider.
Strongly agree Agree Neutral Disagree Strongly disagree

- The Internet of Things identifier policy should promote business models for open interoperable platforms.
(other option: vertically integrated business models.).
Strongly agree Agree Neutral Disagree Strongly disagree

- To preserve competition, IoT identifiers should be openly accessible (e.g., like an url name or telephone number).
or

The use of closed identifiers that belong to the service provider (e.g., the SIM card on the mobile phone) is a better option.
("strongly agree"/"agree": openly accessible identifiers are the better option "disagree"/"strongly disagree": closed identifiers are the best option").

Strongly agree Agree Neutral Disagree Strongly disagree

- There are other conditions than open identifiers that need to be satisfied to ensure IoT platform interoperability.
Strongly agree Agree Neutral Disagree Strongly disagree

- There is a need of unique identifiers for the IoT and of an organisation allocating them.
Strongly agree Agree Neutral Disagree Strongly disagree

Please insert a comment here, if you wish – maximum 10 lines

Data portability is a key consumer concern. This relates not only to the issue of technical compatibility and interoperability of systems but also contractual barriers for the provision of the service. As far as interoperability is concerned, standardised data format could ensure the migration of data from one service to the other.

Data security is another main consumer concern as at present cloud computing services do not need to respect any minimum security standards nor to be independently audited on a regular basis to ensure compliance. It is likely that those shortcomings will be amplified in a IoT environment and should therefore be addressed.

Section 6: Governance - part 1

The current Internet has been created with design principles and characteristics that made its success possible as a unique global infrastructure, which has in turn driven the quest for globally accepted governance principles. The IoT may represent another infrastructure layer, with capabilities for interfacing and interacting with the physical world. Therefore, and in addition to the above outlined topics (security, privacy, ethics, interoperability), it may be argued that these additional aspects go beyond the bounds of what is considered Internet Governance, in relation to aspects such as:

1. Implementation, maintenance and development of the IoT physical world infrastructure (Internet linked or Internet-independent) characterised by edge devices, networks infrastructures and service capabilities with associated control functions (main aspect is design principles and responsibilities in making sure they are respected).
2. Environmental disruption and impact associated with deployment and maintenance of fixed position IoT object-connected devices, systems and networks, and the end-of-life recycling or disposal of devices, systems and networks; exacerbated by an

expected exponential growth in use of object-connected and other edge-technology devices.
3. Functionality and performance demands in relation to physical world interaction that may have an impact on critical safety and critical business functions.

NB: the goal of below set of questions is to identify key IoT deployment and operational aspects related to public policy concerns and under which framework these should be addressed

- There is one Internet, with resources globally available. There should be one IoT (other possibility: multiplicity of IoT silos without interoperability per application domains).
Strongly agree Agree Neutral Disagree Strongly disagree

- In general, IoT physical world infrastructure is an issue for IoT Governance.
Strongly agree Agree Neutral Disagree Strongly disagree

- Potential environmental disruption due to IoT technologies is an issue for IoT Governance.
Strongly agree Agree Neutral Disagree Strongly disagree
- Collective issues of IoT device deployment (functionality, reliability, safety) are issues for IoT Governance.
Strongly agree Agree Neutral Disagree Strongly disagree

- Governance addressing infrastructure and functionalities of the IoT are already covered by the Internet Governance framework.
Strongly agree Agree Neutral Disagree Strongly disagree

Please insert a comment here, if you wish – maximum 10 lines

Section 6 - Governance - part 2

Similarly to the Internet Governance, the development of an IoT Governance framework may require to engage multiple stakeholders to come up with generally agreed principles and implementation methodologies.

A framework for IoT Governance may also consider different enforcement approaches, including soft approaches (co-operation, co-ordination, co-regulation) or harder approaches (regulation, mandated standards).

- A multi-stakeholder platform is needed to address IoT Governance issues.
Strongly agree Agree Neutral Disagree Strongly disagree

- Existing multi-stakeholder platforms (IGF, OECD, IETF, ITU…) are suited to address IoT Governance issues.

If the answer is "disagree" or "strongly disagree", please give your views in free text box below as to what the optimal IoT Governance multi stakeholder platform should be.
Strongly agree Agree Neutral Disagree Strongly disagree

- Soft approaches are the most appropriate to implement an IoT Governance Framework.
Strongly agree Agree Neutral Disagree Strongly disagree

- Hard approaches are the most appropriate to implement an IoT Governance Framework.
Strongly agree Agree Neutral Disagree Strongly disagree

- A mix of hard and soft approaches are the most adapted to implement an IoT Governance Framework.
Strongly agree Agree Neutral Disagree Strongly disagree

Please insert comments here, if you wish – maximum 10 lines

We 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 and Reliability

Section 7: Standards for meeting policy objectives

Whilst ICT standards are primarily industry driven, standards may be an important tool to achieve policy objectives.
The international nature of the IoT development is likely to require a global standards approach. The nature of the IoT development also demands attention to wide ranging standards and differing types of standards, including technical, application, quality and compliance standards as well as regulation in relation to resources such as the electromagnetic spectrum, energy and so forth. This range and diversity in standards further suggests the need for a reference framework for IoT standards.

NB: the goal of below set of questions is to identify Key IoT standardisation drivers.

- The policies addressed under an IoT Governance framework need to be implemented with the development of global standards.
If the answer is "strongly agree" or "agree", please shortly indicate policy requirements needing global standards in free text box below.
Strongly agree Agree Neutral Disagree Strongly disagree

-IoT Governance should have a role in determining a reference architecture for IoT standards.
Strongly agree Agree Neutral Disagree Strongly disagree

Existing standardisation frameworks (e.g., M2M) should be considered as reference framework for further IoT standardisation.
Strongly agree Agree Neutral Disagree Strongly disagree

Please insert comments here, if you wish – maximum 10 lines

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 formal standards to ensure consumers can use an IoT application or service without having to buy a specific software or system. Standards could also be used to address the accessibility, health, safety and privacy concerns raised by IoT applications. We call however for the application of good governance principles. Standards should be developed with full and consumer participation.