EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

Sustainable and Secure Society
Trust and Security

REPORT ON THE PUBLIC CONSULTATION ON

IOT GOVERNANCE

[16/01/2013]

This document does not represent an official position of the European Commission. It does not prejudge the form or content of any future proposal by the European Commission.

1. INTRODUCTION

This report provides an overview of the results of the public consultation on the governance of the Internet of Things (IoT).

IoT is a long term technology and market development based on the connection of everyday objects to the Internet. Connected objects exchange, aggregate and process information on their physical environment to provide value added services to end-users, from individuals to companies to society as a whole.

IoT has the potential to considerably improve the life of EU citizen by addressing many of today's societal challenges in health, transport, environment, energy, etc. It will create tremendous opportunities for innovation-based growth and jobs creation in Europe. At the same time it holds risks for individuals in areas like privacy and security.

Through the public consultation, the Commission sought views on an appropriate policy approach to foster a dynamic development of IoT in the digital single market while ensuring appropriate protection of EU citizen. The consultation was held between 12 April and 12 July 2012 on "Your Voice in Europe" and attracted wide attention both from industry and civil society.

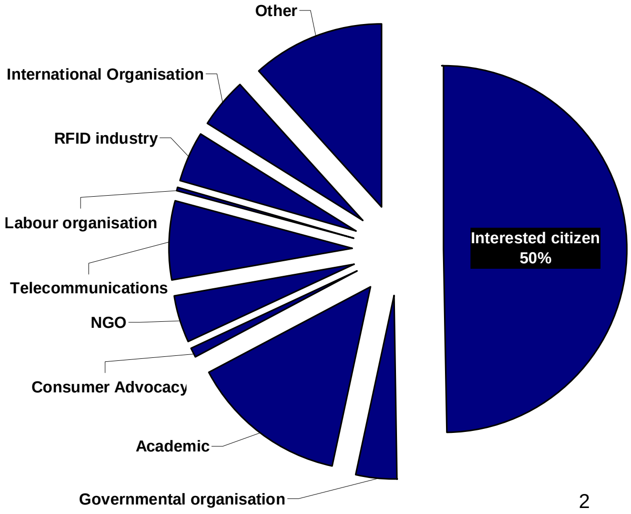
2. PARTICIPATION

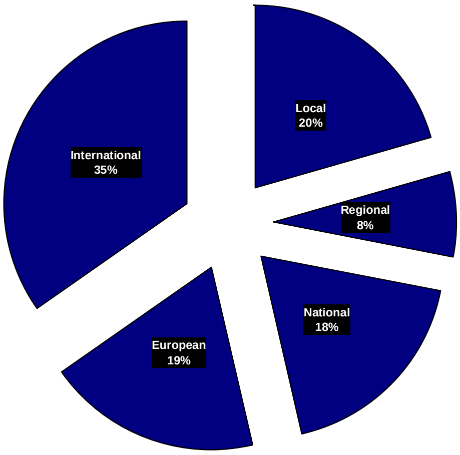
More than 600 answers to the online questionnaire on IoT Governance were received.

Respondents represent a wide range of stakeholders, from interested citizens, academics and civil society associations to various industry players (both ICT and non-ICT) and their associations. They range from local / regional stakeholders to European and international organisations. Respondents are mainly established in the European Union, but several answers were also received from third countries, in particular the United States.

More details on the respondents can be found in Annex 1, which gathers the statistical results of the public consultation.

The pie charts below show the spread of the participation.





3. Overview of the answers

The public consultation showed unambiguous consensus on the fact that IoT will bring significant economic and social benefits, in particular in the fields of healthcare, independent living, support for the disabled and social interactions. The questionnaire sought to identify those areas where public intervention would be required to allow such benefits to materialise while maintaining sufficient control and protection of consumers and society at large.

Most respondents acknowledge that IoT development raises a number of public policy issues, but their views diverge on the appropriate response and the scope for public intervention.

This section reports on both the quantitative and qualitative answers received during the public consultation.

3.1. Privacy and data protection

The questionnaire explored the need for specific data protection measures for IoT applications.

In general, the industry argued that the current Data Protection Framework is sufficient, and that no additional rules are needed. A few respondents even called for no public intervention at all to avoid stifling innovation. As far as Data Protection Impact Assessments (DPIA) are concerned, most industry players stressed the need for generic guidelines and flexibility to adapt to different industries. Some industry players pointed out that requesting users' explicit consent for each and every application would hinder the development of IoT. In their view, it should be possible to share anonymised IoT data with third parties.

In contrast, a large majority of interested citizens and consumer organisations claimed that the current Data Protection Framework is not sufficient and a greater focus on privacy and Data Protection in the context of IoT is needed. This could be done for instance by developing IoT-specific DPIA guidelines (77% of the respondents support it).

Harmonisation amongst EU countries and at international level, as well as stronger enforcement were emphasised.

These respondents consider that data subjects should remain in control of their data. In particular they support the following principles:

- User consent is primordial; the user should be able to choose whether or not to be part of an IoT system. The right to verify and to rectify personal data was also mentioned, as were the rights to delete data and to be forgotten.

- Personal data should not be used for means beyond those stated for the purpose of the application without the user's explicit consent. One privacy association warned for example that "*autonomous communication could very well lead to the building of extensive personal profiles without the consent of the data subject, a phenomenon we already see today in the conventional Internet environment*". Some respondents, however, would allow for a more general form of consent to benefit from the sharing nature of the IoT.

- Data anonymisation is seen as especially important to facilitate data sharing.

- Transparency should be ensured; users should be informed about the nature and the purpose of data collection and how they may access and amend personal data.

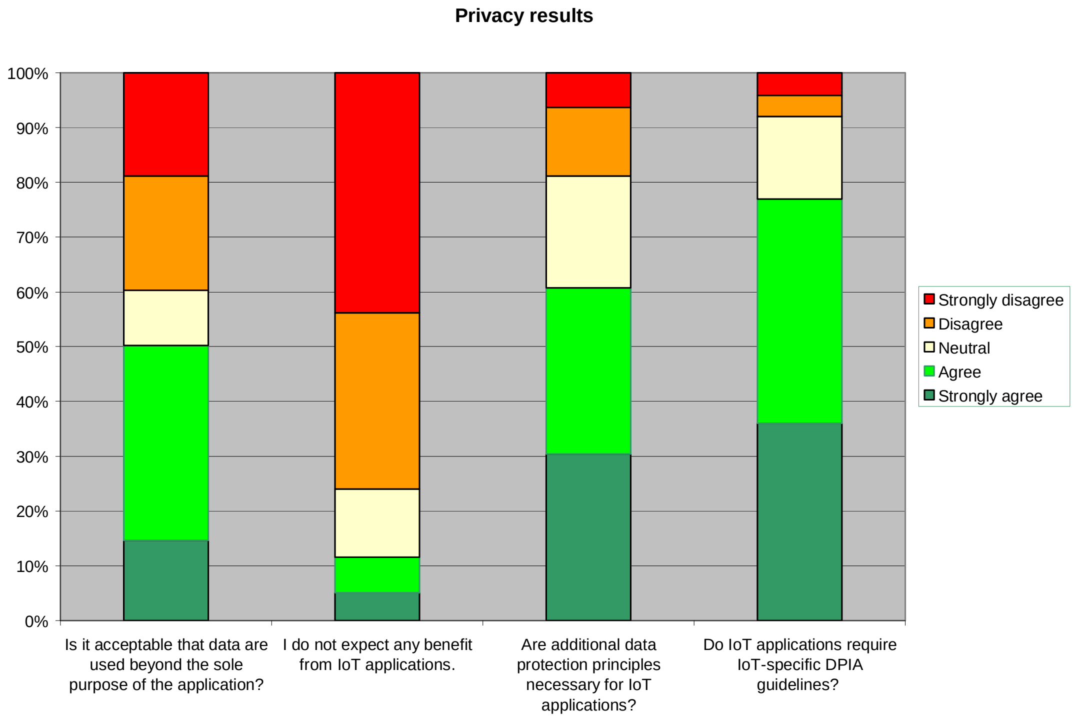
- Privacy by Default and by Design should be implemented.

- System security (including encryption) should be a priority to avoid illegal access.

- Data retention should be limited in time; however certain respondents claim it should not be permitted at all.

- Fair and lawful principles were also emphasised, such as accountability, fair use principles and ethics.

- Data Protection audits by an independent authority were mentioned by some respondents.



3.2. Security and safety

The questionnaire sought the views of the respondents on the need for specific guidelines and standards to ensure security and personal safety in the Internet of Things.

Several industry players, backed by a few interested citizens, claimed that additional guidelines may not be warranted and should in any case be specific to the problem at stake rather than generic. In their view:

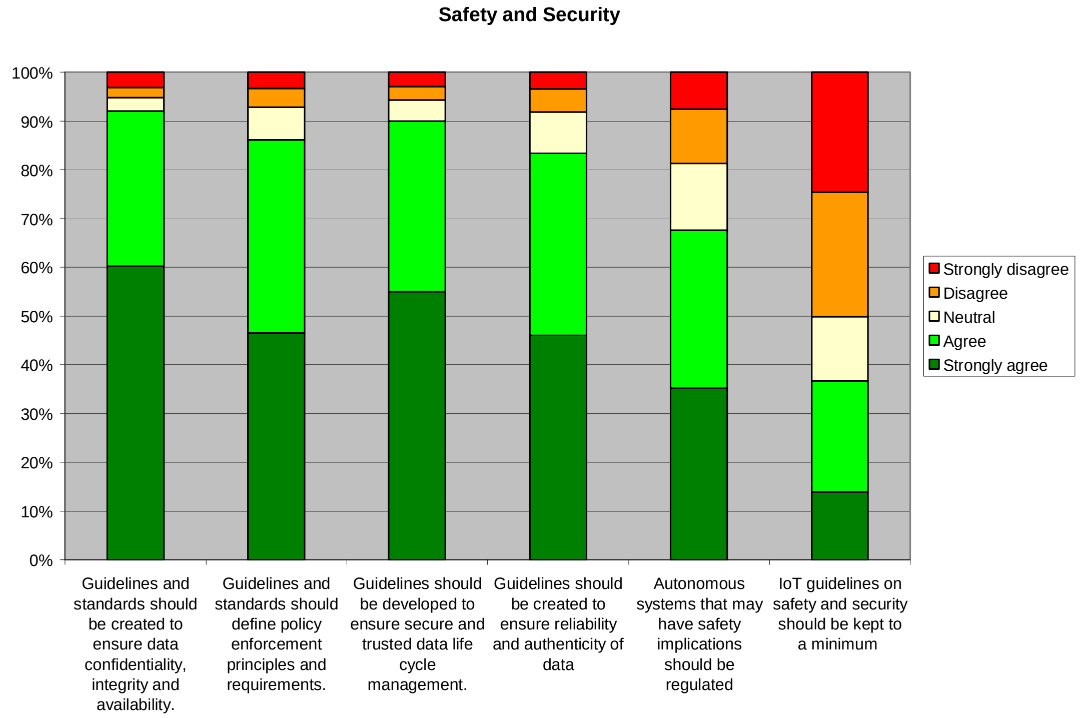
- The Commission should be careful not to over-regulate and create unnecessary regulatory burdens. For example a telecom operator argued that "*regulatory or "hard" policy enforcement will probably miss the target, introduce costs and delays, and in the end undermine the competitiveness of European industry*".

- Regulation should take stock of existing standards and guidelines, in particular in the field of safety. A large equipment manufacturer explained that "*a "one-size-fits-all" approach is not advisable and most likely counterproductive in this context. Any guideline or standard provided in this field should take this diversity into consideration and hence should be context based and flexible*".

At the same time, many respondents consider that safety and security are more important than economic viability. For example a consumer organisation stated that they "*would be opposed to any guidelines that would only establish minimum requirements in order not to compromise the economic validity of IoT applications*".

The need for guidelines and standards was put forward by a vast majority of respondents, with several of them underlining the need for international cooperation in a "*globally operating internet*". For example, 92% of the respondents agree that guidelines and standards should be created to ensure data confidentiality, integrity and availability in an IoT context. Many respondents are of the view that such guidelines and standards should be developed "*within a multi-stakeholder framework, with the participation of consumer organizations, civil society and regulatory authorities in addition to public authorities and private stakeholders*". For many respondents binding tools are required, whilst for others guidelines should spell out a general and technology agnostic approach to security problems.

Cooperation was put forward by certain respondents, as a way to ensure security on an end-to-end basis in an IoT context. An industry association advocated in particular a "*continued and sound breach notification policy*". For them, such a system should be "*reasonable and avoid being over-burdensome on organizations (i.e. it should not entail a "real-time" notification system or low reporting thresholds)*". It might encompass both security and privacy breaches.



3.3. Security of critical IoT supported infrastructures

The questionnaire explored whether more stringent and mandatory information security measures would be warranted when IoT services are related to critical infrastructures.

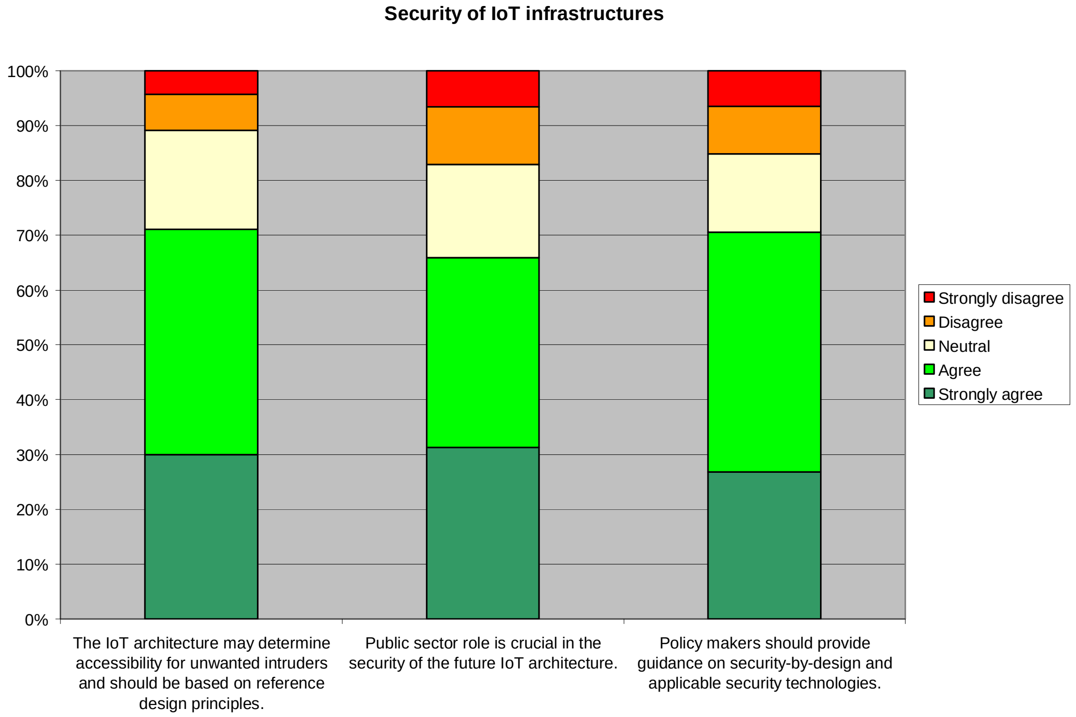
There was large support for public guidance. For example, 66% of respondents agree that public sector role is crucial in driving the definition of the security of future architecture for the IoT. However, the comments are more cautious on the need and the extent of public intervention.

Several respondents warned against prescriptive regulation. As an academic explained: "*IoT is stillin its early stages. Too much prescription via reference architectures - i.e. too early guidance towards standardization - could inhibit the emergence of better architectures via* *trial and error in the market*". A telecommunications manufacturing company argued that "*the definition of the security of future architecture for the IoT should primarily be an industry driven process*". Many respondents insisted on the need for a multi-stakeholder approach. For a telecommunications operator "*cooperation between industrial, public sectors and governmental institutions are essential to rightly address security issues and to improve safety and security of services*".

Several respondents singled out the possibility of evaluating the implementation of standards and guidelines by independent bodies. An interested citizen explained: "*A certification should exist for involved people for implementation of these standards, with a time limited certification (i.e. for 5 years -not whole life-)*". Some respondents stressed the need to increase information sharing and the key role of Computer Emergency Response Team (CERT) platforms. For a telecommunications manufacturer "*policy makers have an important role in securing the infrastructure by establishing an effective information sharing framework to counteract specific threats*".

Several respondents claimed that the diversity of technical solutions should be promoted. As one citizen explained: "*The most obvious lesson is that monolithic systems are very vulnerable for any critical disturbance. This means we should (force) diversity not just in behaviour, but also in implementation*".

Finally, several respondents argued that IoT services are not yet implemented as part of critical infrastructures and the issue should therefore be assessed later when such a "critical IoT" has developed.



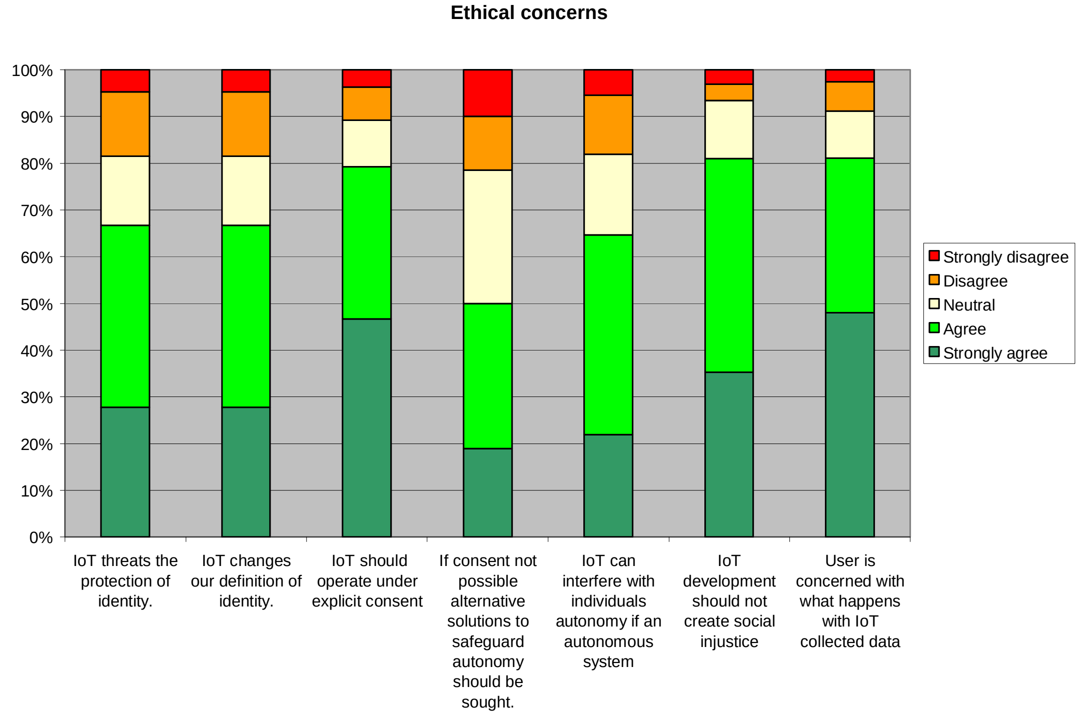
3.4. Ethics: ethical issues

The questionnaire also explored the possible impact of IoT applications in terms of ethics, including the sense of personal identity, individuals' autonomy, user consent, fairness and social justice.

The majority of respondents agree that IoT will have strong ethical implications and 65% of respondents believe that IoT applications could interfere with individuals' autonomy when decisions are taken by autonomous systems. However, certain respondents challenged this view. A telecommunications operator argued for example that IoT does not imply "*a loss of control but rather a shift in the locus of control*". For this operator "*there is nothing new about this shift. When a car owner upgrades from a manual gear box to an automatic, although it involves replacing a previously manual process with an automatic one, the owner remains in control of the car. The use of tools to replace 'low level' actions with 'machine automated' actions, leaving humans to focus on higher value actions, is a fundamental human desire*".

The majority of respondents insisted on the need to safeguard user consent and user control in an IoT context. At the same time, some industry players argued that explicit consent will not always be possible and should not be mandated. A software security company noted in this regard that "*A traffic light coordination system presents very little identity relevance compared to an eID smartcard scheme. Therefore, questions such as whether consent is at all relevant, or what consent should look like if applicable, can only be answered in consideration of the particular application, its purpose and the context in which it is used*". An industry association insisted on the need to apply the principles of proportionality and transparency: "*"Proportionality" in this context requires a balanced analysis of assessing risk and mitigating risk based upon threat to privacy. If the implementation is "proportionate," then the implementing entity should provide "transparency" thereby establishing a legal framework that would restrict the IoT from being secretly used to collect data. In order to achieve transparency, individuals should receive reasonable and appropriate notification of the type of data collected and how the data will be shared and used*".

A consumer organisation stressed that "*consumers should always have the right to disconnect from their networked environment or disable it at any time and without any discrimination*". For an academic: "*People should be afforded the right to be 'invisible' to these systems*". In addition many respondents argued that individuals should be in control at all times of their data. In this context, a majority of respondents underlined the need for informed consent, and emphasised the need to inform and educate users – in particular the elderly, children, the disabled – as to the potential benefits, risks and implications of IoT.



3.5. Ethics: procedural issues

The questionnaire further explored the measures to be adopted to take account of ethical aspects in the design and the deployment of IoT. The questionnaire asked in particular whether an ethical charter would be relevant.

Industry players stressed the role of the market and the existing legal framework to deliver the appropriate outcome. A telecommuncations equipment provider formulated it as follows: "*an effective application of the legal framework, together with company specific processes for privacy and security, should be sufficient to meet the desired objectives*".

On the other side, the majority of individual respondents argued that a charter or other forms of self-regulation would be insufficient. They insisted it would not be respected by IoT providers and cannot be enforced. A consumer organisation said that "*a strong regulatory framework that is properly enforced is needed to ensure that consumers' rights and autonomy are respected*". A bottom up multistakeholder approach to define the ethical framework relevant to IoT was proposed with participation of international institutions and authorities, national authorities, citizen and consumer communities, industry and business stakeholders, standardisation bodies, politicians (as citizens' representatives), human rights groups, academia and legal and ethical experts.

Many respondents called for regulatory oversight and governance, including regular audits, to be carried out by independent public-sector organisations. EU-wide ethical standards, regularly reviewed, were also proposed.

3.6. Object identifiers and interoperability

The questionnaire sought to identify the minimum set of interoperability requirements applicable to object naming and addressing to support competition and consumer choice.

The vast majority of respondents agreed that interoperability is an important policy objective and open IoT platforms will promote competition and service innovation. At the same time, many respondents explained that closed and open identifiers are currently used and will continue to co-exist. For example, a software security company explained that for certain applications *"(e.g. industrial control) non-interoperability could be a very appropriate security measure, while portability may be simply irrelevant*". For these respondents, the development of closed or vertically integrated systems should not be prevented. They insisted that in a free market companies should be entitled to develop closed platforms to increase their prospective profits. Such closed platforms will compete with open ones and according to a company active in industrial and automotive electronics "*it should be up to the market to decide which model (open/close) is more suitable and successful in an application area*". Several respondents argued that interoperability is the result of normal market functioning.

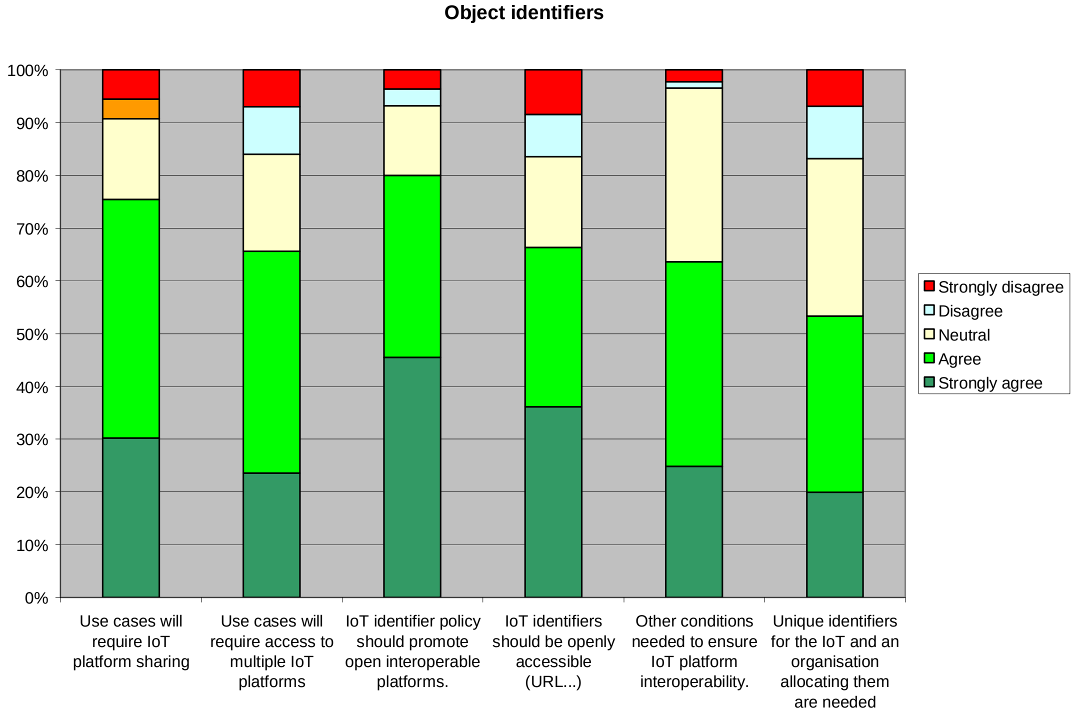
The development of a global identification scheme was supported by many respondents. An equipment manufacturer argued for example that "*the allocation of unique identifiers has to be managed in a consistent way at a global level*".

However, other respondents argued that "*a single global numbering scheme is unrealististic*" (a business applications provider) and mandating it could be a barrier to the development of IoT. For an internet stakeholder "*there exists already a number of organisations which are having their own object identification schema to identify objects. It will be nearly impossible to force these organisations to move to a single unique object identification schema. Hence, it would be acceptable to have different name spaces, managed by different organisations, provided that those organisations work in an open, transparent and non discriminatory manner, with a special effort on finding mapping/conversion mechanisms for a broader interoperability*". For many respondents there is no need for a new organisation to allocate identities. A decentralised system using a hierarchical assignment of identities removes the need of issuing agencies.

Several respondents insisted on the need to re-use existing protocols, in particular internet protocols and IPv6. A business application developer argued that "*the Internet of Things is part of a Future Internet and hence uses the same addressing mechanisms*".

In addition to open identifiers, certain respondents singled out the need to implement open Application Programming Interfaces (API) to develop compatible IoT applications.

Finally several respondents insisted that IoT identification schemes also raise privacy issues and should allow end-users to preserve their anonymity. . For example, one respondent argued that "*in order to protect privacy and to apply privacy-by-design technology, object identifiers should be valid for the shortest period of time possible and be changed as often as possible*".



3.7. Governance: scope for IoT governance

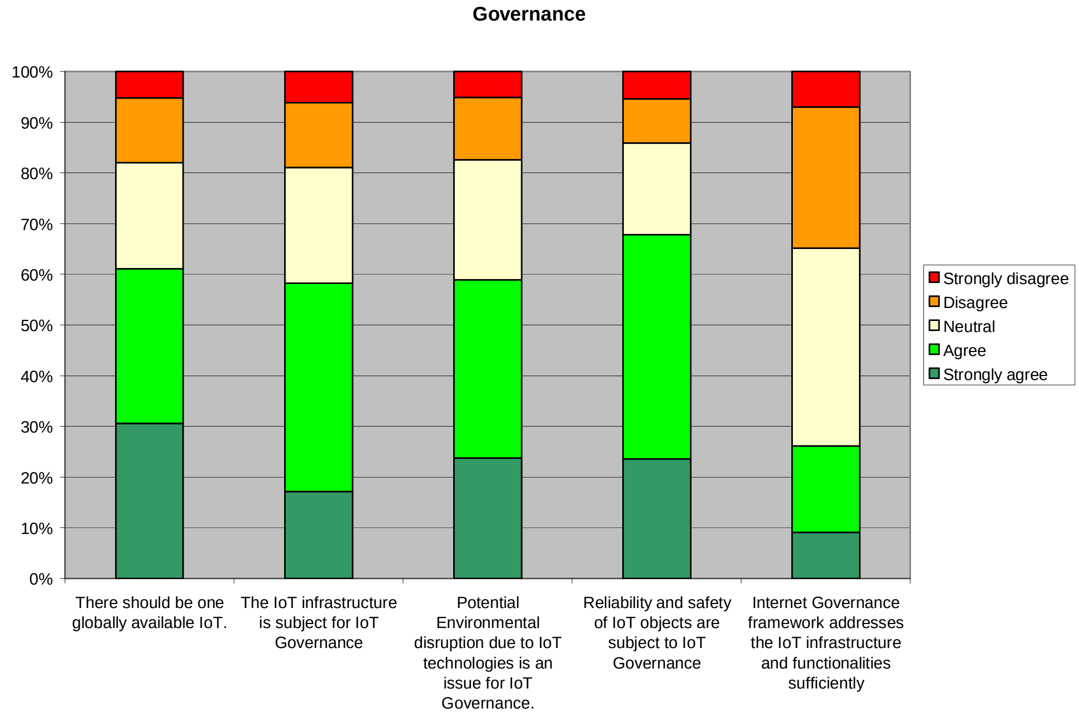
The questionnaire sought to identify IoT topics which may be relevant for governance – in addition to the above outlined topics of privacy, security, ethics and interoperability – and under which framework these topics should be addressed.

A majority of respondents agreed that the topics suggested in the questionnaire (implementation of the IoT physical world infrastructure, environmental impact of IoT deployment and functionalities provided by the IoT) should be addressed by specific IoT governance. They also agreed that there should be one unified IoT as opposed to a multiplicity of IoT "silos" without interoperability. Many respondents insisted that IoT governance should be defined before IoT is widely deployed.

However many respondents, industry players and also interested citizens, have a very different opinion in their comments. For them, there is no need for IoT specific regulation or governance and IoT deployment should be governed by current horizontal regulation (privacy rules, safety and environmental legislation, etc.), coupled with industry-led standards and general principles. A business software developer argued for example that "*No special IoT governance is needed. The existing Internet governance schemes should be used - but possibly improved. Secondly, we need to be wary about additional governance frameworks that may only deter functional/technological development. Environmental concerns are important, but should rather be dealt with in Environmental Law*". In the same vein, a software security company stated that "*real world impacts, e.g. infrastructural, environmental, social, will be governed by the same principles and rules that apply to any activity. It is for IoT technologies to integrate compliance with all applicable rules, and not for IoT governance to develop separate legislation or to replicate what already exists*".

Some respondents disagreed on the fact that the topics suggested in the questionnaire are relevant for specific governance. A large international equipment manufacturer argued that "*there is no need for an authority that shall decide or approve the different applications or decide on the infrastructure of devices*".

Several comments contend that there cannot be a unified IoT. For a telecommunications equipment provider "*the IoT, like the Internet, is a network of networks. While you may have a smart meter at home as well as a bio sensor, they have no need to communicate, are managed (and belong) to different entities and while one can be attached to a private infrastructure the other may go over the public Internet. As such, the IoT is a useful overarching term, but does not reflect the multiplicity of different architectures*".

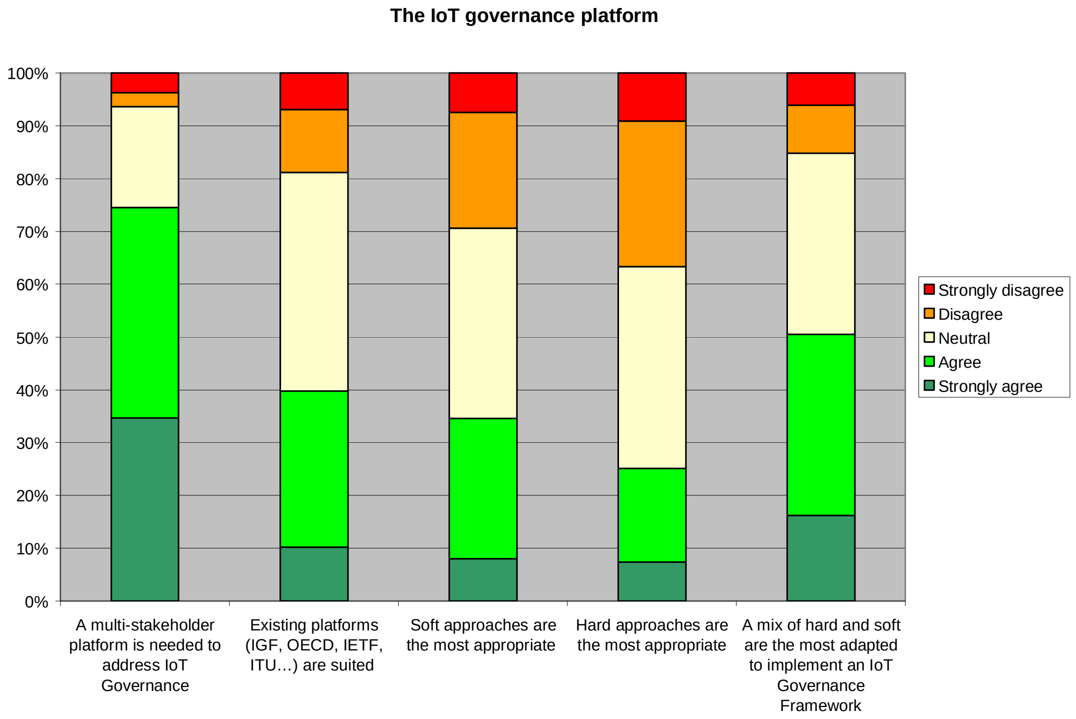


3.8. Governance: a framework for IoT Governance

The questionnaire also explored the organisation and the enforcement approaches of a possible IoT governance body / framework.

The views of the respondents were divided on the organisation of the such a governance body. Most respondents favoured a multi-stakeholder approach. For some respondents existing multi-stakeholder platforms are suitable to address IoT governance issues but they need increased coordination and allow a better representation of civil society. A consumer organisation noted that "*in addition to organisations like IGF, OECD, IETF, ITU…, the platform should also involve representatives of the Civil Society (e.g, ISOC) and Public Authorities, notably for legal aspects (e.g, EC). It is also very important that existing platforms liaise more effectively with each other to implement the governance framework*". Other respondents criticised existing bodies for being too slow and weak in enforcement: *"Their power is not enough to enforce new technologies, and so devices which use outdated technologies are commonplace, and needed improvements to internet* *technologies take decades to become the norm (HTTPS, IPv6, new cerificates structure...)*". For these respondents a new multi-stakeholder platform is needed to address IoT Governance issues.

Views were divided on the level of prescriptiveness of IoT governance (hard vs. soft approaches). Most industry players were in favour of no governance or a soft approach combined with self-regulation. Many respondent were in favour of a mix of hard approaches for crucial issues including privacy, safety and health and soft approaches on other issues.



3.9. Standards for meeting policy objectives

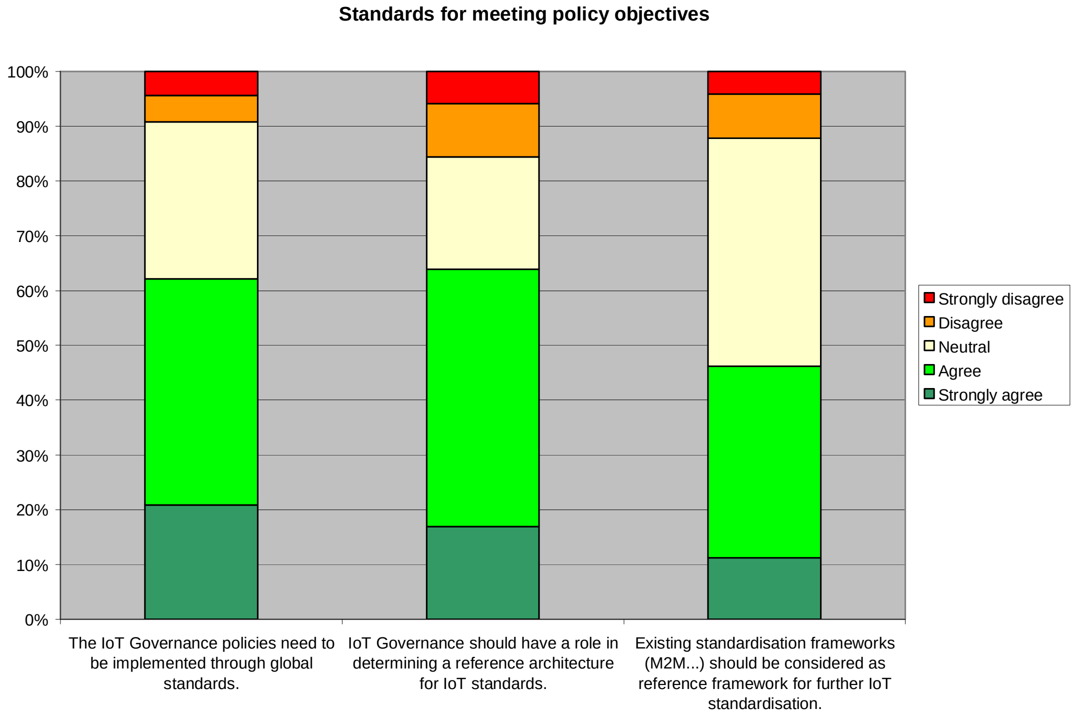
The questionnaire sought the views of the respondents on the need to develop standards that would support IoT policy objectives and on the best way to develop them.

Most respondents (62%) agreed that IoT Governance should be supported by global standards and that IoT governance should have a role in determining a reference architecture for IoT standards (64%). An organisation representing consumers for example supported "*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*". For many respondents IoT standardisation should be based on existing standards and market solutions, but for other respondents dedicated standards are needed to address the specificity of IoT.

Different areas for standardisation were put forward, generally they include broad policy issues such as "*privacy (mandatory and/or prohibited functionality), interoperability* *(addressing, protocols, formats), security (authentication, encryption, integrity), compatibility (frequency, power)*".

On the other hand, a lot of industry players argue that there is no need for new standards to achieve specific policy objectives. One respondent argued for example that "*standardisation is a private undertaking. Public policy should be used e.g. to mandate standards where the private sector fail to initiate standards needed to build a market. Standards for IoT are today being developed by existing fora, and should continue to do so*". Certain respondents warn against the idea of defining a common reference architecture for IoT standards. A security software company explained that "*it is very difficult to foresee the specific needs that particular IoT standards will have to meet in applications we may not even suspect today. Constraining future efforts into any preconceived architecture could be counterproductive*" A telecommunications equipment provider agreed that "*Fighting against that evolutionary momentum can only cause confusion, disparity, and risk throughout the IoT ecosystem.*". Some respondents claimed that the market should be left to develop further before standardisation starts.

For a consumer association, alternative ways for public authorities to steer the standardisation process in order to achieve policy objectives should be explored, in particular " *authorities can act as facilitator and moderator for the various companies and organisations interested to invest in the field of IoT, not the least by incorporating research tenders on the subject*".



4. Conclusion

There is no consensus on the need for and the scope of public intervention in the field of IoT.

A large part of industry – backed by several individual respondents and academics – questioned the legitimacy of public intervention in a sector which is still in its infancy. They claim that IoT technologies and applications should develop further before appropriate policy measures can be devised. The existing legal framework including data protection and competition rules, as well as safety and environmental legislation are already protecting the end-user. In their view, ongoing standardisation work on identification, IoT architecture or security will foster a competitive and safe development of IoT applications.

They also stressed that inappropriate governance will raise barriers to investment and innovation, or would be useless in case the market developed in a way different than foreseen. Policy intervention, if any, should be flexible, recognise the diversity inherent to IoT and build on the existing legal and technological acquis.

By contrast, many individual respondents backed by civil society and consumer associations claimed that economic considerations are secondary when fundamental rights like privacy, security, and other ethical issues are at stake. End-users' rights and autonomy should receive full protection in an IoT context. They underlined the risk that the IoT market would not develop in a competitive way and that consumers may get locked in certain technologies and / or by certain players. In their view, IoT specific rules should be developed and enforced to control the development of IoT technologies and markets. They conclude that a multi-stakeholder platform, securing appropriate representation of civil society, is needed to address IoT governance issues.

ANNEX 1: STATISTICAL RESULTS OF THE PUBLIC CONSULTATION

Respondents details

Categories of respondents	
Interested citizen	49,67%
Academic	13,79%
Governmental organisation	3,65%
NGO	4,32%
Consumer Advocacy Group	0,83%
Labour organisation	0,17%
International Organisation	4,49%
Telecommunications	6,98%
RFID (systems) industry	1,33%
RFID using industry	1,33%
RFID consulting industry	1,83%
Other	11,63%

It should be noted that several industry players registered themselves under "Other" or "International Organisations".

The following major stakeholders participated in the public consultation:

- ICT companies: Deutsche Telekom, Telecom Italia, Telefónica, Vodafone, Huawei, Cisco, Sierra Wireless, Ericsson, Nokia Siemens Networks, HP, ARM, SAP, Microsoft, Symantec, AVG, Ingenico

- Other companies: Bosch, ENI, Lloyds TSB, Volvo, Siemens

- Industry associations: European American Business Council (EABC) , European Semiconductor Industry Association (ESIA), DIGITALEUROPE, TechAmerica Europe, RFID in Europe, European Telecommunications Network Operators' association (ETNO), EUROSMART, Federation of European Direct and Interactive Marketing (FEDMA), European association for forwarding, transport, logistics and custom services (CLECAT)

- Other associations: Open Geospatial Consortium (OGC), GS1, RIPE, AFNIC

- Civil society: European Consumers' Bureau (BEUC), European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC), Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBud), ASPHI, AGE Platform Europe, Vrijbit, European Blind Union (EBU)

- Government: Generalitat de Catalunya, Gobierno de Aragon, Norwegian Post and Telecommunications Authority (NPT), Malta, Provincia di Firenze

Geographic area of activity	
Local	20,43%
Regional	7,64%
National	18,27%
European	18,94%
International	34,72%

Country of establishment	
Austria	1,16%
Australia	0,50%
Belgium	4,82%
Brazil	0,17%
Bulgaria	0,33%
Canada	0,33%
China	0,33%
Cyprus	0,66%
Czech Republic	0,50%
Denmark	0,33%
Finland	1,83%
France	16,28%
Germany	11,63%
Greece	0,83%
Hungary	0,17%
India	0,17%
Ireland	1,50%
Israël	0,33%
Italy	17,61%
Japan	0,17%
Latvia	0,17%
Lithuania	0,17%
Luxembourg	0,83%
Malta	0,17%
Mexico	0,33%
Netherlands	6,15%
Norway	0,17%
Other	0,17%
Poland	1,16%
Portugal	1,50%
Romania	0,33%
Slovak Republic	0,33%
Slovenia	0,50%
Spain	5,32%
Sweden	2,33%
Switzerland	1,16%
Turkey	0,17%
United Kingdom	15,61%
United States of America	3,82%

Age group	
Under 18	1,33%
18-24	8,31%
25-44	50,66%
45-64	36,54%
65+	2,99%

Gender	
Male	82,70%
Female	17,30%

Section 1: Privacy

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	14,65% 35,43%	50,09%
Neutral	10,05%	
Disagree Strongly disagree	20,95% 18,91%	39,86%

I do not expect any benefit from IoT applications.		
Strongly agree Agree	4,92% 6,45%	11,38%
Neutral	12,56%	
Disagree Strongly disagree	32,26% 43,80%	76,06%

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?		
Strongly agree Agree	30,53% 30,36%	60,89%
Neutral	20,58%	
Disagree Strongly disagree	12,18% 6,35%	18,52%

Data Protection Impact Assessments (DPIA) are contemplated for the deployment of applications involving personal data. IoT-based applications require to develop IoT-specific DPIA guidelines.		
Strongly agree	36,12%	77,05%
Agree	40,93%	
Neutral	15,12%	
Disagree	3,74%	7,83%
Strongly disagree	4,09%	

Section 2: Safety and Security

Guidelines and standards should be created to ensure data confidentiality, integrity and availability.		
Strongly agree	60,28%	92,06%
Agree	31,78%	
Neutral	2,76%	
Disagree	2,07%	5,18%
Strongly disagree	3,11%	

Guidelines and standards should define policy enforcement principles and requirements.		
Strongly agree	46,52%	86,06%
Agree	39,55%	
Neutral	6,79%	
Disagree	3,83%	7,14%
Strongly disagree	3,31%	

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	54,84%	89,97%
Agree	35,12%	
Neutral	4,33%	
Disagree	2,77%	5,71%
Strongly disagree	2,94%	

Guidelines should be created to determine reliability of data and to verify the authenticity/source of data (data provenance).		
Strongly agree	45,83%	83,33%
Agree	37,50%	
Neutral	8,51%	

Disagree	4,69%	8,16%
Strongly disagree	3,47%	

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	34,98%	67,49%
Agree	32,51%	
Neutral	13,78%	
Disagree	11,13%	18,73%
Strongly disagree	7,60%	

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	13,91%	36,80%
Agree	22,89%	
Neutral	13,03%	
Disagree	25,53%	50,18%
Strongly disagree	24,65%	

Section 3: Security of critical Internet of Things supported 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	30,05%	71,02%
Agree	40,97%	
Neutral	18,07%	
Disagree	6,62%	10,91%
Strongly disagree	4,29%	

Public sector role is crucial in driving the definition of the security of future architecture for the IoT.		
Strongly agree	31,42%	65,97%
Agree	34,55%	
Neutral	16,84%	
Disagree	10,59%	17,19%
Strongly disagree	6,60%	

Policy makers should provide guidance on security-by-design and applicable security technologies.		

Strongly agree	26,92%	70,45%
Agree	43,53%	
Neutral	14,34%	
Disagree	8,74%	15,21%
Strongly disagree	6,47%	

Section 4: Ethics – Group 1 – ethical issues

Identity: IoT applications pose threats to the protection of an individual's identity.		
Strongly agree	27,89%	66,84%
Agree	38,95%	
Neutral	14,56%	
Disagree	13,86%	18,60%
Strongly disagree	4,74%	

Identity: IoT applications could change our sense and definition of personal identity.		
Strongly agree	18,25%	58,95%
Agree	40,70%	
Neutral	17,72%	
Disagree	14,91%	23,33%
Strongly disagree	8,42%	

Autonomy: Insofar as possible, IoT applications should operate under "explicit consent" by its users as with other ICT applications.		
Strongly agree	46,82%	79,33%
Agree	32,51%	
Neutral	10,07%	
Disagree	6,89%	10,60%
Strongly disagree	3,71%	

Autonomy: It is not possible for IoT applications to operate under explicit consent; alternative solutions to safeguard autonomy should be sought.		
Strongly agree	18,97%	50,09%
Agree	31,12%	
Neutral	28,36%	
Disagree	11,60%	21,55%
Strongly disagree	9,94%	

Autonomy: IoT applications could interfere with individuals' autonomy when decisions are taken by autonomous systems.		
Strongly agree	22,00%	64,73%
Agree	42,73%	
Neutral	17,09%	

Disagree	12,73%	18,18%
Strongly disagree	5,45%	

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	35,37%	80,97%
Agree	45,60%	
Neutral	12,39%	
Disagree	3,59%	6,64%
Strongly disagree	3,05%	

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	48,19%	81,41%
Agree	33,21%	
Neutral	9,75%	
Disagree	6,32%	8,84%
Strongly disagree	2,53%	

Section 4: Ethics - Group 2 - procedural issues

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	9,35%	32,91%
Agree	23,56%	
Neutral	25,36%	
Disagree	25,18%	41,73%
Strongly disagree	16,55%	

Section 5: Open object Identifiers and interoperability

A number of use cases and business scenarios will require sharing a given IoT platform between multiple service providers.		
Strongly agree	30,19%	75,37%
Agree	45,19%	
Neutral	15,37%	
Disagree	3,70%	9,26%

Strongly disagree	5,56%	

A number of use cases and business scenarios will require access to multiple IoT platforms by a single service provider.		
Strongly agree	23,48%	65,43%
Agree	41,96%	
Neutral	18,48%	
Disagree	9,06%	16,08%
Strongly disagree	7,02%	

The Internet of Things identifier policy should promote business models for open interoperable platforms. (other option: vertically integrated business models.).		
Strongly agree	45,67%	79,93%
Agree	34,25%	
Neutral	13,26%	
Disagree	3,13%	6,81%
Strongly disagree	3,68%	

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	36,03%	66,18%
Agree	30,15%	
Neutral	17,28%	
Disagree	8,09%	16,54%
Strongly disagree	8,46%	

There are other conditions than open identifiers that need to be satisfied to ensure IoT platform interoperability.		
Strongly agree	24,90%	63,51%
Agree	38,61%	
Neutral	33,01%	
Disagree	1,16%	3,47%
Strongly disagree	2,32%	

There is a need of unique identifiers for the IoT and of an organisation allocating them.		
Strongly agree	20,04%	53,37%
Agree	33,33%	
Neutral	29,78%	
Disagree	9,93%	16,85%
Strongly disagree	6,93%	

Section 6: Governance - part 1

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	30,67% 30,48%	61,15%
Neutral	20,82%	
Disagree Strongly disagree	12,83% 5,20%	18,03%

In general, IoT physical world infrastructure is an issue for IoT Governance.		
Strongly agree Agree	17,20% 41,31%	58,50%
Neutral	22,43%	
Disagree Strongly disagree	12,90% 6,17%	19,07%

Potential environmental disruption due to IoT technologies is an issue for IoT Governance.		
Strongly agree Agree	23,92% 35,22%	59,13%
Neutral	23,35%	
Disagree Strongly disagree	12,43% 5,08%	17,51%

Collective issues of IoT device deployment (functionality, reliability, safety) are issues for IoT Governance.		
Strongly agree Agree	23,71% 44,17%	67,88%
Neutral	17,97%	
Disagree Strongly disagree	8,80% 5,35%	14,15%

Governance addressing infrastructure and functionalities of the IoT are already covered by the Internet Governance framework.		
Strongly agree Agree	9,14% 17,12%	26,26%
Neutral	39,11%	
Disagree Strongly disagree	27,63% 7,00%	34,63%

Section 6 - Governance - part 2

A multi-stakeholder platform is needed to address IoT Governance issues.

Strongly agree	34,65%	74,39%
Agree	39,74%	
Neutral	19,21%	
Disagree	2,64%	6,40%
Strongly disagree	3,77%	

Existing multi-stakeholder platforms (IGF, OECD, IETF, ITU…) are suited to address IoT Governance issues.		
Strongly agree	10,02%	39,50%
Agree	29,48%	
Neutral	41,62%	
Disagree	11,95%	18,88%
Strongly disagree	6,94%	

Soft approaches are the most appropriate to implement an IoT Governance Framework.		
Strongly agree	8,01%	34,77%
Agree	26,76%	
Neutral	36,13%	
Disagree	21,68%	29,10%
Strongly disagree	7,42%	

Hard approaches are the most appropriate to implement an IoT Governance Framework.		
Strongly agree	7,36%	25,19%
Agree	17,83%	
Neutral	38,37%	
Disagree	27,33%	36,43%
Strongly disagree	9,11%	

A mix of hard and soft approaches are the most adapted to implement an IoT Governance Framework.		
Strongly agree	16,24%	50,29%
Agree	34,05%	
Neutral	34,44%	
Disagree	9,20%	15,26%
Strongly disagree	6,07%	

Section 7: Standards for meeting policy objectives

The policies addressed under an IoT Governance framework need to be implemented with the development of global standards.		
Strongly agree	20,92%	62,00%
Agree	41,07%	
Neutral	28,79%	
Disagree	4,80%	9,21%
Strongly disagree	4,41%	

IoT Governance should have a role in determining a reference architecture for IoT standards.		
Strongly agree	16,96%	63,94%
Agree	46,98%	
Neutral	20,47%	
Disagree	9,75%	15,59%
Strongly disagree	5,85%	

Existing standardisation frameworks (e.g., M2M) should be considered as reference framework for further IoT standardisation.		
Strongly agree	11,00%	45,97%
Agree	34,97%	
Neutral	41,85%	
Disagree	8,06%	12,18%
Strongly disagree	4,13%	