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)?

Respondent details	
Your organisation's geographic area of activity (please indicate your geographic area of activity if answering as an individual person) -single choice reply-(compulsory)	European
Your organisation's country of establishment (indicate your country of residence if answering as an individual person) -single choice reply-(compulsory)	Belgium
Please indicate your age group -single choice reply-(compulsory)	45-64
e-mail address -open reply-(compulsory)	info@clecat.org
What type of stakeholder are you? -single choice reply-(compulsory)	International Organisation
First name -open reply-(compulsory)	Nicolette
Last name -open reply-(compulsory)	van der Jagt
Gender -single choice reply-(compulsory)	Female
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). -single choice reply-(optional)	Disagree
I do not expect any benefit from IoT applications. -single choice reply-(optional)	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	Disagree

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. -single choice reply-(optional)	
Data Protection Impact Assessments**[1]** (DPIA) are contemplated for the deployment of applications involving 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. -single choice reply-(optional)	Agree
Please insert comments here, if you wish – maximum 10 lines -open reply-(optional)	CLECAT sees clear value in the Internet of Things in connection with Intelligent Communication Technologies and intelligent transport infrastructure. We expect IoT applications to support the further optimisation of logistics services and delivery times. However, our members, European freight forwarders, are concerned with the securing of data, in particular commercial data. Cyber-crime is a new form of crime, in which commercial data can be used to target specific containers or deliveries of high value. The security of the data is therefore of utmost importance, in order to prevent persons with unauthorized access to data from using it in an unlawful way or to get access to sensitive commercial information.
## Section 2: Safety and Security	
Guidelines and standards should be created to ensure data confidentiality, integrity and availability. -single choice reply-(optional)	Strongly agree
Guidelines and standards should define policy enforcement principles and requirements. -single choice reply-(optional)	Agree
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. -single choice reply-(optional)	Strongly agree
Guidelines should be created to determine reliability of data and to verify the authenticity/source of data (data provenance). -single choice reply-(optional)	Strongly agree
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. -single choice reply-(optional)	Neutral
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. -single choice reply-(optional)	Neutral
Please insert a comment here, if you wish – maximum 20 lines -open reply-(optional)	In CLECAT's opinion data security is one of the crucial issues regarding the Internet of Things, and a potential cause for lack of commitment from the industry. While the advantages of IoT are clearly visible for most, the potential of IoT is often not yet fully understood, especially by SME's. It is therefore essential to address data security effectively. For that to happen CLECAT advocates clear and robust European, or even better international guidelines on how to store data and prevent the use of data for any other purpose than in the IoT remit. Who controls the data, who has access to it, what elements will be included in the data transmission? If the EU can develop guidelines or a standard, which can address these questions to authenticate and verify data coming from one source it would alleviate the breakthrough of the technology at least in the logistics sector. Important factors to consider regarding the data traffic are: ownership of data, access rights, ownership of processes, authorisation for intercommunication and interoperability. In that sense we support the International Standard ISO/IEC 17799, which covers data security under the topic of information security. One of its most important principles is that all stored information, i.e. data, should be owned so that it is clear whose responsibility it is to protect and control access to that data. CLECAT would welcome a similar approach towards an EU recommendation for a IoT governance.
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. -single choice reply-(optional)	Agree
Public sector role is crucial in driving the definition of the security of future architecture for the IoT. -single choice reply-(optional)	Agree
Policy makers should provide guidance on security-by-design and applicable security technologies. -single choice reply-(optional)	Agree
Please insert a comment here, if you wish – maximum 10 lines -open reply-(optional)	CLECAT is of the opinion that public authorities play a key role in providing and maintaining data security. While the infrastructure, innovation and methods of exchanging data will be business-driven, it is the task of the authorities to protect the IoT Community from criminal activities, be it cyber-crime or data theft, or an attack on the physical infrastructure (e.g. data storage centres). As electronic data can be exchanged across borders without problems the issue should be tackled at EU or international level (e.g. Europol, OLAF or Interpol).

Section 4: Ethics - Group 1 – ethical issues

Identity: IoT applications pose threats to the protection of an individual's identity. -single choice reply-(optional)	Neutral
Identity: IoT applications could change our sense and definition of personal identity. -single choice reply-(optional)	Neutral
Autonomy: Insofar as possible, IoT applications should operate under "explicit consent" by its users as with other ICT applications. -single choice reply-(optional)	Agree
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. -single choice reply-(optional)	Agree
Autonomy: IoT applications could interfere with individuals' autonomy when decisions are taken by autonomous systems. -single choice reply-(optional)	Neutral
Fairness and social justice: Current developments of IoT applications need to take into account the different capacities, constraints, needs and expectations of individuals. -single choice reply-(optional)	Neutral
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. -single choice reply-(optional)	Agree
Please insert comments here, if you wish – maximum 10 lines -open reply-(optional)	The user must have some method of controlling and influencing the data that is being sent and received by objects through the Internet of Things. While the idea is to let the objects communicate with each other, it is necessary and probably envisioned by the IoT providers that the user can set beforehand the kind of information that he wants to send and to whom he wants to send it. Once these preferences have been noted in the options of the network infrastructure the objects can then start communicating with each other on a more independent basis.

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	Neutral

technologies and applications. -single choice reply-(optional)	
(a) If you agree, please identify key ethical principles which you consider should be part of such charter: *Please state here- maximum 10 lines* -open reply-(optional)	As noted above ensuring data security and data integrity are the main points of interest. On top of that we refer to the comments made in the previous sections, especially about ownership of the data.
(b) Who should be involved in the definition of an "IoT ethical charter"? *Please state here – maximum 10 lines* -open reply-(optional)	If such a charter is to be developed, we would advocate that all relevant stakeholders are invited to participate. That includes at least users of the IoT services, appropriate authorities of each EU MS, the providers of the IoT infrastructure and services, data protection agencies and NGO's, industry associations, and academia. If the IoT ethical charter will be set up at EU level the European Commission should look at leading the discussion, with the inclusion of the EP and Council. We would advise to include members of the former Commission expert group on RFID, as well as members of the raceRFID network in the discussion.
Please insert comments here, if you wish – maximum 10 lines -open reply-(optional)	

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. -single choice reply-(optional)	Neutral
A number of use cases and business scenarios will require access to multiple IoT platforms by a single service provider. -single choice reply-(optional)	Neutral
The Internet of Things identifier policy should promote business models for open interoperable platforms. (other option: vertically integrated business models.). -single choice reply-(optional)	Agree
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"). -single choice reply-(optional)	Agree
There are other conditions than open identifiers that need to be satisfied to ensure IoT platform interoperability. -single choice reply-(optional)	Agree
There is a need of unique identifiers for the IoT	Strongly agree

and of an organisation allocating them. -single choice reply-(optional)	
Please insert a comment here, if you wish – maximum 10 lines -open reply-(optional)	CLECAT has no additional comments on this issue.

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). -single choice reply-(optional)	Agree
In general, IoT physical world infrastructure is an issue for IoT Governance. -single choice reply-(optional)	Agree
Potential environmental disruption due to IoT technologies is an issue for IoT Governance. -single choice reply-(optional)	Agree
Collective issues of IoT device deployment (functionality, reliability, safety) are issues for IoT Governance. -single choice reply-(optional)	Neutral
Governance addressing infrastructure and functionalities of the IoT are already covered by the Internet Governance framework. -single choice reply-(optional)	Neutral
Please insert a comment here, if you wish – maximum 10 lines -open reply-(optional)	CLECAT prefers one IoT, rather than several IoT's, to avoid regionalisation and different standards. However the global connection of communicating objects needs to adhere to strict security standards, considering the economic value of the operations and the role the technology will play in everyday life once it is more widely adopted. It is necessary to think about these issues before the implementation of an IoT and not react to the problems that arise once the technology is more widely used.

Section 6 - Governance - part 2

A multi-stakeholder platform is needed to address IoT Governance issues. -single choice reply-(optional)	Agree
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. -single choice reply-(optional)	Neutral
Soft approaches are the most appropriate to implement an IoT Governance Framework.	Agree

-single choice reply-(optional)	
Hard approaches are the most appropriate to implement an IoT Governance Framework. -single choice reply-(optional)	Disagree
A mix of hard and soft approaches are the most adapted to implement an IoT Governance Framework. -single choice reply-(optional)	Disagree
Please insert comments here, if you wish – maximum 10 lines -open reply-(optional)	CLECAT is of the opinion that soft measures are to be preferred over legislation, in particular because the Internet of Things is a global technology like the Internet. Standards will be helpful in order to facilitate its wider application. However global standards (like ISO/IEC 17799) are preferred over EU standards. In addition the EU needs to ensure that standardisation activities do not hamper innovation and existing IoT infrastructure and services are taken into account.
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. If the answer is ”strongly agree" or "agree”, please shortly indicate policy requirements needing global standards in free text box below. -single choice reply-(optional)	Agree
IoT Governance should have a role in determining a reference architecture for IoT standards. -single choice reply-(optional)	Neutral
Existing standardisation frameworks (e.g., M2M) should be considered as reference framework for further IoT standardisation. -single choice reply-(optional)	Agree
Please insert comments here, if you wish – maximum 10 lines -open reply-(optional)	CLECAT would support an international standard for the IoT infrastructure. We also encourage the European Commission to look at existing standards and solutions on the market and base EU standards on these approaches to avoid duplication of work and encourage utilisation of existing technology. International policy should especially work as an enabler for standards and should avoid picking winners at an early stage in the process. In addition 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.