

Answer to the European Commission public consultation on the early challenges regarding the "Internet of Things"

Please indicate your preference (use a X):

- I agree that this document is made public
 I want this document **not to** be made public

If you reply on your own behalf, please indicate:

- Name:
- Telephone:
- Email:
- Country of residence:

If you are replying on behalf of an organisation, please indicate:

- The organisation's name: American Chamber of Commerce to the European Union (AmCham EU)
- The type of organisation:
 - private company
 - government/public body/international organisation
 - academic/research institution
 - non governmental organisation
 - other: **business association**
- Your organisation details
 - o location: **Brussels, Belgium**
 - o size: **142 member companies**
 - o scope of activities (max 3 sentences):
The American Chamber of Commerce to the European Union (AmCham EU) is the voice of companies of American parentage committed to Europe towards the institutions and governments of the European Union.
 - o website: **<http://www.amchameu.be>**
- Contact person: **Christian Borggreen**
- Contact person' telephone: **(32 2) 289 10 36 (direct line)**
- Contact person's email: **christian.borggreen@amchameu.be**

Insert here your organisation name (or your own name if replying on your own behalf)

November 28th 2008

Response to “Internet of Things” Public Consultation

EXECUTIVE SUMMARY

ISSUE	AMCHAM EU POSITION
Definition & Scope	
The term “Internet of Things”	It is important to ensure a common understanding of what the term encompasses and how it is used.
“Internet of Things” and RFID	RFID is one of the IoT enabling identification technologies. The Commission should take a technology neutral framework approach and expand on the role that other technologies can also have in the IoT.
Clarifications on the term “Object Namespace”	It is important to understand what is an Object Namespace and how it works. A distinction needs to be made between the DNS and an Object Namespace.
Potential applications of the IoT technologies	
The emerging trend of analytics	The Commission should recognise the opportunities arising from the analysis of the increased amount of data generated and exchanged in the IoT and the “intelligent” information this data can produce.
Retail	The Document should also acknowledge the security aspects: the use of identification technologies can better “arm” companies against malicious attacks and can be an effective anti-counterfeiting tool.
E-health	The analysis and management of data generated with the use of RFID and sensing technologies in healthcare has the potential to transform our healthcare systems and the practice of medicine in terms of efficiency and quality.
Environment	The use of IoT technologies can allow not only the monitoring and statistics’ collection that the Working Document rightly mentions but has also the potential to provide powerful tools in the fight against climate change.
D. RFID applications	
Privacy and data protection	As there is no clear understanding yet of how the IoT will develop, a discussion on the aspects of privacy and security is highly speculative at this stage. On RFID and data protection, see AmCham

Insert here your organisation name (or your own name if replying on your own behalf)

	EU's submission of April 25 th 2008 to the relevant Commission's public consultation.
Security	We recognise the need to address the challenge of security in the IoT emerging architecture. As regards to RFID technology, some misconceptions relevant to ONS should be clarified.
Governance	The reference to broad governance rules without considering the nature of applications and their supporting architectures is problematic. At this point, the IoT is under defined and at a too early stage in its evolution to commit its future parameters to a concrete control model.
Standardisation	We urge the European Commission to avoid fragmentation and take a global approach to standards development so as not to hamper technological innovation and further deployment of IoT enabling technologies.
Transatlantic considerations	Need to intensify the dialogue between the EU and the US, as well as other countries in relation to the deployment of new technologies that will enable the IoT to ensure harmonised/compatible approaches.

Insert here your organisation name (or your own name if replying on your own behalf)

Introductory remarks

AmCham EU welcomes the publication of the European Commission's Staff Working Document on the Early Challenges of the "Internet of Things" as well as the opportunity to contribute to the public debate with comments on this Document and some initial thoughts on the issues discussed.

We believe that the "Internet of Things" (IoT) -as the term is used in this Document taking into account the concerns we point out in section B. "Definition & Scope"- and the technologies it may encompass have the potential to improve the quality of life and provide great economic and social benefits.

Although we welcome a public debate on how the "Internet of Things" may evolve, what technologies it may include, how an "Internet of Services" may benefit society, what policies need to be in place to allow technology development and innovation, we think it is very premature to discuss how to regulate the "Internet of Things"; because we do not and can not from a technology standpoint have a clear picture yet of what the "Internet of Things" will actually be.

A. Definition & Scope

a. The term "Internet of Things"

AmCham EU members believe that it is important to ensure a common understanding of what the term "Internet of Things" encompasses and how it is used. At the moment, it is not clear how the Commission understands the concept, moreover the current use of the term can be misleading:

As the use of data communication tools (primarily RFIDs) connected to a range of physical objects is expanding, these objects can be anything ranging from boxes of medicines (eg, to control these are genuine products), to motor vehicles (eg, tyre pressure systems) and to natural persons (eg, patients whose health requires continuous monitoring). While the information gathered by these new systems may be communicated via the Internet, this does not necessarily mean that the Internet as such will change or that there will be a new "form" of Internet only intended to be used for information exchange between these new communication tools. An analogy can be made here with the rapid increase of sharing of videos over the Internet which requires more bandwidth but has not led to a new "kind" of Internet.

From a technology standpoint it is important to note that there is no agreement, yet on whether the "Internet of Things" will be an evolution of the existing Internet or whether it will evolve in parallel.

Furthermore, the limited analysis of the concept of the "Internet of Things" in the Staff Working Document, does not clarify for the reader whether the Commission understands the concept as a new development in itself or as the next step in the RFID debate or as part of the RFID debate.

b. "Internet of Things" and RFID

RFID (Radio Frequency Identification) technology is one of the IoT enabling identification technologies, and not necessarily the main one. As the Commission acknowledges, there are several technologies that may be encompassed in an "Internet of Things" including identification technologies, Near Field Communications technologies, wireless sensor and smart technologies. We believe that a policy debate on the "Internet of Things" should include discussions on all technologies that enable this "eco-system".

Insert here your organisation name (or your own name if replying on your own behalf)

As the Staff Working Document strongly focuses on RFID the reader gets the impression that RFID is the dominating technology governing the “Internet of Things”. If the “Internet of Things” is the Internet of smart objects, RFID would only be a part of it: this “Internet of Things” will mainly consist of all the smart objects which will be connected using the Internet Protocol (IP), i.e. all forms of sensors, actuators, small devices connected together using radio technologies but also wired technologies like PLC and Ethernet. They will be used in a wide range of innovative areas like industrial automation, smart grids, smart cities, home and building automation etc. In this sense, the “Internet of Things” can be considered as an evolutionary process not as something completely new.

Though RFID has led to the deployment of these small computing devices it is not indicative of the “Internet of Things”, its capabilities and potential impact. This is due, in part, to RFID’s lack of internetworking capabilities. At present we feel that the RFID discussion is important to have at the EU level as the roll out of RFID especially in the retail sector has raised a number of regulatory concerns which need to be dealt with. However, it is important to highlight that the regulatory discussion about RFID should not be thought of as directly transferable to the evolving interconnected “Internet of Things”.

We urge the Commission to take a technology neutral framework approach and enrich the debate by expanding on the role that other technologies can also have in the “Internet of Things”. A technology-linked approach will always be behind developments and if the market perception is that the EU wants to regulate every emerging IoT enabling technology, companies may invest outside Europe, eg, in the US or Asia. Also such an approach can limit the development, deployment and potential contribution of IoT enabling technologies other than RFID.

c. Clarifications on the term “Object Namespace”

As noted already, an extremely diverse array of namespaces, objects and services may be implied by the “Internet of Things.” Given this diversity, as well as the public-private bifurcation, different technical and regulatory approaches and treatments will be needed. The Internet is ultimately a collection of private and public networks with an open architecture so as to accommodate lots of different needs and encourage innovation. Any future Object Namespace will build on this flexibility and create its own customised networks based on their respective applications and business models.

The term Object Namespace (also known as Object Identifier system) is a general term used to describe any registry service that enables parties to locate information about an object by directing a querying party to a source of information. One well known example of existing private namespaces with query capabilities is the EPCglobal Object Name System, a closed private network. Like many private namespaces it leverages the Internet DNS (an open network) to facilitate discovery among its users.

A distinction needs to be made between the DNS and an Object Namespace due to a number of functional and structural differences. Domain Names on the Internet are sold through ICANN-accredited registrars to the general public. At the same time ONS Company Prefixes are assigned by EPCglobal only to its member companies. Domain Names on the Internet resolve to servers that host associated websites and email services, while Company Prefixes on the ONS resolve to a network end point managed by an EPCglobal member company.

This difference is illustrated also by the fact that servers storing ONS data are ONS-specific servers with tailored geographical distribution for the respective namespaces (there are currently six ONS servers located in Europe, Asia, and the United States). The method of finding and

Insert here your organisation name (or your own name if replying on your own behalf)

sharing information on the ONS in particular follows a publicly available standard but the ability to find and share specific information on the EPCglobal network is restricted (private) and controlled by the member company, not the ONS. In this context, the ONS cannot currently equate to the concept of the “Internet of Things” that envisions connecting many different types of identifiers and sensors to a network.

The Internet is used for discovery, access and transport of private Object Namespace queries and data. It is utilised for transport of ONS data and queries, but any future generic Object Namespace is likely to be a network system with both private and public components that utilises the public DNS network to direct traffic. For example, individual companies or organisations can operate a public website that is accessible via the Internet, while also using a private Intranet that utilises DNS protocols and standards. The company Intranet site is protected by user name, passwords, and other security measures to ensure that only authorised users can access private information. Logically, the root of any future global Object Namespace linking pointers to various namespace registries would be operated on a separate platform from DNS.

B. Potential applications of the IoT technologies

AmCham EU member companies welcome the European Commission’s effort to list potential applications of IoT enabling technologies and encourage the Commission to expand on such applications (including and beyond RFID) in future policy initiatives as well as to support their deployment.

a. Opportunities in the new data capture architecture: the emerging trend of analytics

As the amount of data produced and exchanged in a network of physical objects will increase tremendously it will be a challenge to manage them and ensure that adequate privacy and security mechanisms are in place. We can therefore expect the emergence of a new trend in the “Internet of Things, i.e. the use of analytics as a tool to access and manage a wealth of information that will be produced by that data.

The European Commission should recognise this opportunity in the new architecture: Accessing and managing such information, can improve and fundamentally reshape business processes by supporting better decision-making and more effective strategy planning and implementation in the public and private sectors. For instance, the use of analytical software tools can help differentiate between useful and “noise” data which will become indispensable in the new data architecture.

Specifically for the retail sector as well as for the areas of e-health and the environment, we provide below some additional thoughts.

b. Retail

As the Commission recognises, fully automated warehouses will improve asset management and will make supply chain management more efficient. But furthermore, we believe that from a security aspect, the use of identification technology can be as a potential enabler to better “arm” the companies against attacks (fast response) as well as counterfeiting.

Notably, while most companies have or aim to have a secure supply chain, malicious attacks, such as product tampering, can still happen. IoT technologies can make the supply chain more secure, in

Insert here your organisation name (or your own name if replying on your own behalf)

detection, prevention and response. It is important that the European Commission takes such applications into account and does not only look at the “negative” privacy angle.

c. E-health

The use of RFID and sensing technologies in healthcare has the potential to transform our healthcare systems and the practice of medicine in terms of efficiency and quality. The analysis and management of the data that will be generated with the use of such technologies will provide valuable information and insight for practitioners, patients and researchers.

For instance, intelligent analytical software tools can process real-time data as they are collected with RFID and sensing technologies that are used to monitor the patient and provide real-time alerts to the medical staff signalling “deviations” from the normal treatment path, thus preventing medical errors. Furthermore, an emerging stage of data-powered healthcare, will enable the transition to personalised / “customised” and patient-centric healthcare that will acknowledge the uniqueness of individuals and will provide the right treatment in the right format to the right individual at the right time.

The policy challenges for the adequate protection of personal data and privacy are undoubtedly significant. However in its approach, the European Commission will need to find the right balance that will allow new technologies with the processing of medical data to transform the delivery of healthcare and improve citizens’ lives enormously.

d. Environment

As in the area of healthcare, the amount of data that will be generated by the use of the “Internet of Things” technologies, can allow not only the monitoring and statistics collection that the Working Document rightly mentions but furthermore has the potential to provide powerful tools in the fight against climate change.

The management and processing of real-time and historic data can improve the environmental performance of organizations and our society as a whole. Today, data collected on the environment is inconsistent, unstructured and not always reliable, thus the public and private sector can not take informed decisions to improve their performance and put together effective and sustainable strategies for a “greener” economy.

It will be indispensable, among others, to enable the deployment of new technologies in this area that will empower Europe to decisively tackle climate change.

C. RFID applications

a. Privacy and data protection

As there is no clear understanding yet of how the “Internet of Things” will develop and what would be its different functionalities, AmCham EU is of the opinion that a discussion on the aspects of privacy and security is highly speculative at this stage. We concur with the Commission’s assessment that there might be potential for identification and profiling of individuals but at this point it is difficult to assess how this might develop.

For example, the blood pressure of a named patient over a period of 24 hours that may be monitored by a sophisticated tool and that would be electronically (internet) sent to the database of a hospital, would be personal data and needs to be protected. However, in many instances information relating to eg, products purchased by an anonymous customer will not be personal data and would not have to be processed with the same restrictions.

Insert here your organisation name (or your own name if replying on your own behalf)

Overall, we believe that the current data protection framework can adequately cope with the possible privacy issues arising from the development of new technologies. Excessive and burdensome regulation may limit benefits coming from the management of data generated as described above and limit new technological developments.

On the other hand we believe that the Commission should encourage industry, non-profit and government stakeholders to establish self-regulatory guidelines and best practices regarding the “Internet of Things” to tackle the policy challenges described.

Furthermore, we welcome the Commission’s announcement of an upcoming Communication on Privacy and Trust and look forward to offering our views on this essential debate. As with all technologies and as rightly pointed out in the previous RFID consultation, trust is indeed an essential element in widespread adoption.

We also fully support the need to provide individuals with clear and sufficient information on the collection of personal data by communication tools. As pointed out in previous AmCham EU positions in relation to RFID technology, such applications do not identify individuals (eg, technical, logistics related) -it would be practically and financially impossible to comply with all data protection principles.

AmCham EU is looking forward with interest to the Recommendation that the Commission will soon adopt on RFIDs and data protection. For more details on AmCham EU’s views regarding RFID and data protection, please see our submission of April 25th 2008 to the Commission Consultation on the “Draft recommendation on the implementation of privacy, data protection and information security principles in applications supported by Radio Frequency Identification (RFID)”.

b. Security

AmCham EU believes that the “Internet of the Things “and the new architectures that may emerge within the “Internet of the Future” require a transition from “certainty” to “trust” for its users and a fundamental component of “trust” is indeed security.

Although as noted above it is too early to talk about how to regulate an “Internet of Things”, addressing security challenges will be fundamental for large deployment. As the Commission recognises, security concerns should not impede the need of interoperability within the new architecture.

In particular as regards RFID technology, we would like to clarify the misconception that data over the ONS is publicly available because it uses the Internet infrastructure. The technical possibilities for control of access to information depending on application and privacy and security concerns are many. Private discovery services, access, and applications are commonplace on Internet infrastructures. The need for security has resulted in countless closed user networks. These needs also apply in the object space and similar approaches have been employed among the users constituting the private infrastructure.

For example, companies that list their company prefixes on the ONS, the system issues a cert to validate their identity over a secure connection. For query parties, one could use EV SSL (Extended Validation SSL) to uniquely identify them. Individual citizens on the other hand, would need to connect through a company site, or be issued a credential such as an OpenID. Like

Insert here your organisation name (or your own name if replying on your own behalf)

"standard" SSL certificates, which rely on authentication of requesting organisation's identity and/or domain control, EV SSL certificates enable secure encrypted communication between a website and a site visitor's browser by facilitating the exchange of encryption keys. To ensure end-to-end protection to transactions, one secures a communication channel and assures that transaction originated from trusted source and can be delivered only to intended destination. For highly secure transactions, one can enable technologies like S/MIME to provide authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).

Just as some smartcards today employ the public key infrastructure (PKI) to ensure that only authorised parties can read the actual data on a smartcard, the same technologies can be employed on RFID tags to ensure that the information on the tag itself remains private. It should be noted that there are many degrees of sensitivity and privacy of data and a one-size-fits all approach cannot be applied. PKI technology provides an example of how the most private transactions and data can be employed.

c. Governance

AmCham EU members believe that it is problematic that there is reference to broad governance rules without considering the nature of applications and their supporting architectures. At the same time, we agree with the premise of the Commission Working Document that the already global nature of business and communication dictates global adoption of network components, as well as interoperable lookup services across geographical locations.

It will be important to make a distinction between (good) governance, necessarily general and future proof, the rules that should apply at operational level and the method by which these are put in practice. As mentioned previously, we believe that, at this point, the Internet of Things is undefined and at a too early stage in its evolution to commit its future parameters to a concrete control model. It would be premature to base such discussions on considerations of control that go beyond the concern for a technologically optimal governance structure.

d. Standardisation

AmCham EU believes that a Euro-centric approach to standards development may hamper technological innovation and deployment of "Internet of Things" enabling technologies.

We urge the European Commission to avoid fragmentation and look to a global approach on standards. This requires a pro-active policy by the Commission and reaching out to important regions, such as the US and Asia.

D. Final remarks: the Transatlantic dimension

AmCham EU looks forward to inputting further as the debate on the "Internet of Things" evolves. We would also like to take this opportunity to reiterate the importance of intensifying the dialogue between the EU and the US, as well as other countries in relation to the deployment of new technologies that will enable the "Internet of Things".

Insert here your organisation name (or your own name if replying on your own behalf)

An effective transatlantic dialogue, in particular regarding technology solutions and applications, R&D projects, global standards, awareness raising campaigns to address privacy and security risks and concerns will ensure harmonised/compatible approaches on both sides of the Atlantic to the benefit of citizens, business and both economies.

* * *

The American Chamber of Commerce to the European Union (AmCham EU) is the voice of companies of American parentage committed to Europe towards the institutions and governments of the European Union. It aims to ensure a growth-oriented business and investment climate in Europe. AmCham EU facilitates the resolution of EU – US issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Total US investment in Europe amounts to €702 billion, and currently supports over 4.1 million jobs.

* * *

Insert here your organisation name (or your own name if replying on your own behalf)