



## Answer to the European Commission's 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 are replying on behalf of an organisation, please indicate:

- The organisation's name: [Cisco Systems Inc.](#)
- The type of organisation:
  - private company
  - government/public body/international organisation
  - academic/research institution
  - non governmental organisation
  - other:
- Your organisation details
  - o location: [Headquarter: San Jose, California, USA](#)
  - o size: 66.129 employees and 39,5 billion US\$ annual revenue (FY 2008)
  - o scope of activities: [Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Today, networks are an essential part of business, education, government and home communications, and Cisco Internet Protocol-based \(IP\) networking solutions are the foundation of these networks.](#)

[Cisco hardware, software, and service offerings are used to create Internet solutions that allow individuals, companies, and countries to increase productivity, improve customer satisfaction and strengthen competitive advantage. The Cisco name has become synonymous with the Internet, as well as with the productivity improvements that Internet business solutions provide. At Cisco, our vision is to change the way people work, live, play and learn.](#)

- o website: [www.cisco.com](http://www.cisco.com)
- Contact person: [Patrick von Braunmühl, Government Affairs Europe](#)
- Contact person' telephone: [+49 30 97892435](#)
- Contact person's email: [pbraunmu@cisco.com](mailto:pbraunmu@cisco.com)

On September 29, 2008 the European Commission launched a public consultation on the early challenges regarding the Internet of Things. The Commission has published a Staff Working Document as a basis for the discussion and is seeking input for a Communication planned for the second quarter of 2009. The Communication on the Internet of Things will propose a policy approach addressing the whole range of political and technological issues related to the move from RFID and sensing technologies to the Internet of Things. It will focus especially on architectures, control of critical infrastructures, emerging applications, security, privacy and data protection, spectrum management, regulations and standards, broader socio-economic aspects. In addition the Commission is currently preparing a Recommendation on privacy and security aspects of RFID expected to be published later this year.

Cisco welcomes the consultation and the opportunity to provide input to the discussion about the early challenges of the Internet of Things.

As the Staff Working Paper strongly focuses on RFID the reader gets the impression that RFID is the dominating technology governing the Internet of Things. In our view the Internet of Things is the Internet of smart objects. This includes RFID of course, but only as a small part of it. The Internet of Things mainly consists 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. The Internet of Things should be considered as an evolutionary process not as something completely new.

Though RFID has led the deployment of these small computing devices it is not indicative of the Internet of Things and its capabilities and potential impact. This is due, in part, to its lack of internetworking capabilities. At present we feel that the RFID discussion is important at 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 we think 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'.

As the Internet of Things is still evolving it is much too early to consider new regulation in this area. Innovation and technology development and deployment should be market driven and barriers imposed by regulation should be avoided.

Cisco has a strong interest in the growth of the Internet of Things as this will extend current networks to include individual physical objects and make them manageable through intelligent network solutions. Apart from being the most relevant global player in building IP-enabled networks Cisco also produces WLANS that, in addition to communicating with client devices using WLAN frequencies, communicate with RFID "readers" & tags made by other companies. In addition Cisco is partnering with major retailers as Wal-Mart and METRO to promote RFID rollout in the logistics chain and to work towards item-level tagging at their supermarkets. Cisco works with RFID manufacturers to make sure their products are interoperable with Cisco built networks. Cisco delivers the intelligence to RFID that enables its customers to leverage the network for making decisions at local sites or wherever the tag is read. Cisco is a member of EPCglobal, the standards body that is defining RFID technical guidelines,

and has the opportunity to help shape this new technology. RFID is likely to be a major area of investment as Cisco's customers transform their business processes.

Some of the proposals contained in the EU Commission's draft Recommendation on privacy and security aspects of RFID ("the draft Recommendation") could potentially have a negative impact on the pace of RFID adoption in Europe and beyond, if they are adopted without changes. Therefore we encourage the Commission to reconsider some of the wording of the Recommendation to improve the balance between legitimate stakeholder interests such as privacy and security and the need to avoid obstacles to the development and deployment of RFID technology in Europe. This technology has the potential to drive innovation, improve efficiency and save substantial costs in different sectors of our economy. In the spirit of the Lisbon agenda the EU should strive to support the adoption of this technology and keep barriers to a minimum.

On the following pages Cisco comments on the policy challenges discussed in the Commission Staff Working Paper relating mostly to RFID:

#### 1) Security

Addressing security issues is very important, but care must be taken not to create a regulatory, instead of an innovation-based approach to security. Security has been characterised by intense innovation, in a game of leap frog between those protecting networks, information and consumers on the one hand, and the criminals and other actors who want to undertake theft, fraud, extortion or other illegal or politically motivated activity using the Internet, on the other hand. It is innovation, not regulation that will make networks and consumers more secure. Regulation will always be two versions behind the latest technical and process innovation, and hampers the ability of defenders to be able to act and react to protect networks and consumers. Setting specific defensive requirements tends to create a road-map for criminals to understand the defensive posture and create exploits that circumvent the set defences. This is why most network security regimes take the voluntary sharing of best practices approach (like the NRIC in the U.S.) and are careful not to take a top-down regulatory approach. A comprehensive market impact assessment is essential before proposing any regulatory measures in this area.

Any regulation in the field of security should be limited to defining certain principles and should be absolutely technology neutral. Only a market driven competition between the best solutions and constant improvement of such solutions can ensure that security is always a step ahead of potential intruders and criminals. Even specific examples of technologies should be avoided in the Communication as this could be interpreted in a way that some technologies are seen as favorable by the Commission. Therefore the mentioning of "end-to-end encryption technologies" as one example in the Staff Working Paper should not be repeated in the Communication.

Concerning RFID application operators and Member States should work closely together to ensure that information security risks are assessed and managed adequately whilst ensuring that existing security risk management approaches are maintained.

As regards the discussion on certification schemes, if certification is left to the Member States, companies working across the EU may have to deal with a patchwork of certification schemes hampering rollout of a pan-EU RFID application, such as a

payment card solution which has a RFID tag embedded within a credit card. This would make it inconvenient for citizens of one Member State to take advantage of the technology within another. A pan-EU certification scheme would be more desirable.

At the same time it should be assessed whether and how existing risk assessment schemes could be applied without necessarily creating new certification regimes. The Recommendation should also stress that any technology mandate should be avoided by all means as this could stifle innovation.

## 2) Privacy and Data Protection

Cisco believes that the current regulatory framework for data protection in the EU provides thorough protection for EU-citizens and consumers. The principles enshrined in this legislation also apply to RFID and any new applications in the context of the Internet of Things. There is no proof of any necessity to create new privacy legislation at the moment. A harmonized implementation and effective enforcement of the existing directives and regulations should be the focus. If any practical problems arise in the context of new technologies, self-regulatory approaches should be favored. We welcome that self-regulation is described as an “effective tool” in the Staff Working Paper and also proposed in the draft Recommendation.

It is important to recognize that international codes of conduct for the privacy-friendly operation of RFID already exist and are followed by RFID application operators. The introduction of national codes of conduct risks fragmenting the internal market. The recommendation should recognize and value the existing self regulatory codes of conducts, guidelines and principles that are already followed by RFID users, such as the EPCglobal Guidelines on EPC for Consumer products as well as other international instruments like the OECD policy principles on RFID.

The Recommendation should stress that European codes of conduct should be designed for the EU as a whole and not just for individual countries. Otherwise there is a risk that national codes of conduct could create an obstacle for pan-European RFID deployment.

Although consumer applications and item-level tagging are still very limited today, RFID use in retail applications potentially presents the greatest challenges and opportunities for full deployment of the technology in the near future. Policy developed for such applications must address privacy and security concerns that may arise from an extensive use of RFID tags on consumer products but should also ensure that deployment of the technology in consumer applications is not unnecessarily hampered by burdensome requirements that do not allow the use of RFID technology to deliver its full benefits -including after-sales services, facilitation of product recalls and other benefits.

The focus on default-deactivation of tags at the cash-point in the current discussion about RFID deployment in the retail sector as the only measure to protect privacy could be too rigid at this early stage in the discussion. As the process at the check-out and the technology to deactivate tags are not clear yet an obligation to deactivate tags by default could create a serious disincentive for retailers to roll out item-level tagging in their markets. While it is undisputed that consumers should be able to fully control any

collection of personal data it is far from clear whether default-deactivation is the only way to ensure this. An easy to use option for consumers to deactivate tags themselves at or after the check-out may fulfill the same purpose while being more cost efficient. Any such obligation should only be decided upon after a thorough impact assessment.

Concerning the impact assessments proposed by the draft Recommendation we believe that there is a need for adjusting them in order to make them proportionate and meaningful. Privacy impact assessments need to be based on existing data security standards which companies already have to follow, in order to make sure that the principles of better regulation are followed and additional bureaucratic burdens minimized as much as possible. The key element should be *the* 'reasonable likelihood of linkage' and not where it '*cannot be excluded*' that data will become potentially personal.

### 3) Control of Critical Global Resources and Subsidiarity

As mentioned earlier, existing principles governing the internet should be applied as much as possible instead of reinventing the wheel. Global naming and routing control architectures are currently in place for RFID applications. Concerns expressed about too much centralization of critical resources seem to be based on very hypothetical risks. The current governance structures of the internet have worked well and there is no need for a regionalization.

The centralized operation of the root object name service (ONS) by VeriSign in the US has not led to any real problems in the past. And it's not likely that any problems should arise in the future. Only France has demanded the setup of its own ONS platform which has been operational since March 2008.

As RFID applications and other Internet of Things technologies will operate globally an EU-centric approach to governance and standardization is not helpful and should be avoided. A consensus based multi-stakeholder approach to governance issues on a global scale should ensure adequate results.

### 4) Identity Management, Naming and Interoperability

Naming and look-up services should be harmonized globally in order to avoid regional islands. The internet has prospered because of a globally defined naming and identification schemes. Cisco welcomes the approach in the Staff Working Paper to encourage mandates for Standardization Organizations to define such schemes for the Internet of Things and develop interoperability requirements across different identity and naming schemes.

### 5) Fostering Innovation

Cisco fully supports the principles of open standards and interoperability of protocols, services and devices. These are fundamental principles which ensure the functioning of the internet and should be applied to the Internet of Things in the same way.

Proprietary standards can pose a potential barrier to market entry especially for SMEs. Naming and look-up services for the Internet of Things should be open to ensure broad access to such services at affordable costs.

The development of the architecture and service platforms should be monitored to avoid monopolistic structures. At the same time existing regulation and competition rules should be sufficient to react to any developments where competition is restricted or dominant positions abused.

A competitive environment and open architectures are vital for the development of innovative services around the Internet of Things.

## 6) Spectrum

It is well recognized that spectrum is a key resource for the development of broadband applications and ICT in Europe including the Internet of Things.

In Cisco's view, the full benefit of wireless technologies will not be obtained without the creation of a consistent, pan-European approach. Although the existing framework emphasizes the objectives of efficient management and harmonization, Cisco believes that a future revised spectrum framework should be adapted to a convergent environment, should aim at a greater harmonization of spectrum management, and should facilitate access to relevant spectrum for new technologies.

An increased harmonization of spectrum management will significantly improve today's situation where each national regulator tends to have its own spectrum management, with some level of co-ordination at the European level by CEPT, RSPG and RSC. The rules vary significantly from one Member State to another to the detriment of an EU single market.

The objective to increase the amount of EU-wide unlicensed spectrum and to define common licensing conditions will favour the creation of a European market for wireless services. Furthermore the approach will stimulate the development of new pan-European players, with greater weight in the global marketplace.

Regarding technological and service harmonisation, we believe this will be largely realized by the industry through international standardisation and through the choices of market players – in particular the pan-European ones. The industry and the market players are more legitimate and better positioned to make the service and technological choices than the governments.

The technological evolution – in particular multi-protocols / multi-bands devices – will enable Europe to take full advantage of an innovative and technologically neutral framework, fostering roaming across borders and across networks.

The allocation of appropriate and sufficient radio spectrum for RFID, sensor technologies and other applications in the context of the Internet of Things across Europe is key for a successful rollout of existing technologies.

## 7) Standardization

It is not clear what the benefits of a more EU-centric approach to the development of standards should be. The Internet of Things will only be successful if global standards are developed and applied. As far as standards exist for the internet they will be applied for IP-enabled smart objects as well. Only for RFID there are already more than 200 different standards today and there is a lack of cooperation between the different standards bodies active in this field. The development of global and industry-wide standards is a vital challenge to speed up the development of new applications and to reap the full benefits for industry, consumers and societies as a whole.

Berlin, 26th November 2008