

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: [Nokia Corporation](#)
- The type of organisation:
 - private company
 - government/public body/international organisation
 - academic/research institution
 - non governmental organisation
 - other:
- Your organisation details
 - o location: [Global, headquarters in Espoo, Finland](#)
 - o size: [112 262 employees at the end of 2007](#)
 - o scope of activities (max 3 sentences): [Mobile communications, Internet services](#)
 - o website: <http://www.nokia.com>
- Contact person: [Petteri Leiviskä](#)
- Contact person' telephone: [+358 40 7284 108](#)
- Contact person's email: petteri.s.leiviska@nokia.com

Please start replying on the next page

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

Nokia is committed to responsible and open deployment of RFID. Nokia wishes that the European Union will steer the policy issues concerning RFID / "The Internet of Things" into the right direction, so that effective technological adoption and consumer privacy, data protection and information security principles are respected in full balance, whilst bringing up all positive aspects of the respective technologies concerned that they have to offer to global economy, consumers and citizens alike, enabling innovation of new services and enhancing global technological and economic competitiveness.

Nokia is looking at RFID technology from two perspectives, both as a user and as a service provider. As a user, we would prefer that also other consumer electronics companies understand that RFID can bring numerous benefits to Nokia, its partners, customers and also to consumers when implemented in the supply chain. This kind of benefits will also be available to other players in the field of consumer electronics.

However, full benefit potential will be realized, when RFID is taken to the item level enabling after-market service related use cases like product recalls, anti-counterfeiting and more efficient and reliable repair and recycling processes. For example, the new European Union battery directive puts manufacturers and importers under an obligation to take care of recycling of their products. At the moment, there is no sensible way of identifying the manufacturer or importer of an individual battery unit. With the help of RFID, individual batteries could be automatically identified and sorted, giving manufacturers and importers an efficient way of recycling.

Nokia stresses that the end-user has to have visibility and control for deactivation of the RFID application by 'Opt-out', the possibility to deactivate the RFID feature either temporarily or permanently. However, deactivation of the tag should not mean only permanent disabling of the tag, so that the tag could still be used for e.g. after market services use cases if so desired.

The retail sector is one of the key users for RFID and NFC technologies. In the context of retail and regarding monitoring, it should be understood that allowing free monitoring e.g. even inside shops and retail stores can in some cases be potentially considered a violation of consumer privacy.

Nokia intends to utilize and deploy RFID to boost global socio-economic and technological welfare, to enable RFID and NFC service innovation, and to make its supply chain more efficient and transparent throughout the entire lifecycle of the product and to bring value to our customers and consumers. This can be achieved by correct implementation and application of the technology enablers and by rational and proportionate regulation that fulfils and respects commercial, societal and ethical requirements.

Nokia is actively partaking to the European Commission's RFID Expert Group as workgroup moderator and contributor.

On chapter "1. Introduction"

"The Internet of Things" will change the way citizens will communicate, exchange information and interact with each other, service providers, objects and governments and the entire technological environment that surrounds them. It will also have a substantial impact on people's digital behaviour and identity management, on people's private sphere, interpersonal relations and consequentially, even on democratic societies and societal values.

The concept of "The Internet of Things" is scoped well, even though conceptualizing a future scheme of such a wide scale is challenging. I would consider expanding the term reference of "RFID" with "NFC" (Near-field communication) as it is what takes RFID into the consumer sector and as a part of hands-on services that benefit the consumer community globally (NFC is referred to on page 4 but it could also be mentioned already in the introductory part). Hence, we see that the communication should span not only for RFID, but also cover all NFC (near-field communication) technologies to make the recommendation's scope future-proof as concerns the technology area.

On chapter "2. The Internet of Things"

In general, the addressing of the concept "The Internet of Things" and its benefit potential is done well and extensively but clearly enough.

On page 4, "Some potential applications of these technologies are described below. Behind the simple, visible functionalities illustrated in these examples lies an invisible but complex web of networked connections and smart systems, which capture information, process it, transmit it and store it. It is these invisible elements, the way in which they are identified and are connected, the scope of their actuation capabilities, the databases where information is stored and securely consulted, the spectral properties of the communication devices etc. that raise a number of important policy challenges." I suggest to possibly rethink the use of the term "invisible" as it might raise some concerns e.g. related to trust. Maybe a term such as "underlying" would convey the meaning in more neutral terms. Also, maybe reconsider the phrase "the databases where information is stored and securely consulted" as "the securely located databases where information is securely stored and consulted".

On page 4, "A retail example" – "Using a mobile phone as a credit card, a travel pass or to automatically get information from the Internet about products in a store is becoming possible." You can actually say that these use cases are possible already today, on the basis of a number of trials and pilot projects globally.

On page 5, "An e-health example" – the benefits that an individual consumer can also personally gain on the RFID and other sensing technologies could be highlighted too, in the form of monitoring personal fitness.

On page 5, "An environment example" – here it could be mentioned of how citizens can monitor their own carbon footprint of making use e.g. innovative mobile phone applications utilizing RFID and other sensing technologies.

On chapter "3.2.1 Security" and chapter "3.2.2 Privacy and Data Protection"

Nokia considers that within the framework of "The Internet of Things", rules concerning information security, consumer privacy and data protection have to apply to all RFID stakeholders equally and all the stakeholders must pay respect to these rules.

Security or privacy is usually as weak as the weakest link concerned. For example, only one industry segment or player that is not following common rules and recommendations can compromise the entire technology domain and its adoption and hence all branches of industry partaking in "The Internet of Things" should act accordingly and to their best ability to respect and protect consumer privacy and information/data security. The stakeholders should be held responsible in case the application they maintain or provide will compromise the end-users' security or privacy. It is important that the technology operators sufficiently protect and are fully responsible for their own assets, and are not avoiding the consequences of possible misuse of their application.

Tackling the issue of individual governments' use of RFID or other IoT enabling technologies and possible violations against their privacy commitments is also vital. We are counting on that governments adhere to the recommendation and are responsible for their possible liabilities. Governments can potentially overrule all possible information security measures taken by corporations, for example in forced access to data. Governments are not necessarily always using the latest state-of-the-art technology to protect privacy and information security, which is however something that the industry usually has the tendency to look after.

On chapter "3.2.3 Control of Critical Global Resources and Subsidiarity"

"Another concern is that reliance on a single, out-of-country service provider, possibly under non-European jurisdiction, may not be compatible with business continuity needs, especially considering that overly resource centralization naturally creates single point failure. Therefore, over-centralisation of critical RFID application resources raises potential concerns both from sovereignty and subsidiarity aspects and from the operational business viewpoint."

A similar regulatory approach should apply for RFID (and The Internet of Things) across the European Union Member States. Additionally, there is a need to find a global regulatory approach as the European Union should not be thought of as an isolated or separate domain what comes to RFID. The question remains how the European Union will tackle privacy when RFID content is logistically transferred to countries outside the European Union having a more flexible or different regulation or legislation? For example, the United States has a tendency of following the European Union's policy definitions, even within the U.S. territory. We should see and leverage the underlying positive momentum for European Union policy formulation.

On chapter "3.2.4 Identity Management, Naming and Interoperability Requirements"

Audit trails could be elaborated in slightly more detail. Regarding the current proliferation of identity codes and the attention raised in the text to the identification technologies themselves, such as RFID "legacy tags" installed fleet on the market, there potentially is not any data security or privacy protection solutions implemented on these tags – this should however not mean that manufacturers of RFID reader devices are solely held responsible for the security of the said tags. All stakeholders should care for the data security and privacy protection with equal responsibility.

"This means that Standardisation Organisations (SDOs) should be issued a mandate to define, with the support of public entities, the functional requirements that identity and naming schemes should respect, in order to comply with principles of general interest. SDOs should also define the global interoperability requirements across identity/naming schemes." It is important that the global interoperability is brought into discussion here in the text as we are essentially talking about global schematics nevertheless when discussing the scope proposed by "The Internet of Things".

On chapter "3.2.5 Fostering Innovation"

Maybe it would be worthwhile to mention here that sufficient attention must be paid to ensuring the security of distributed software and service platforms (middleware) as they are basically "the control layer for transactions and events" and "at the core of the potential innovation". True openness promoting innovation cannot be sustained without appropriate attention and care for security.

"... whilst favouring adoption by older or people with disabilities." Maybe consider rephrasing as "... whilst favouring adoption by elderly or disabled people."

As a general note, the traditional division of service providers and service consumers will blur and actually vanish in the field of RFID and "The Internet of Things" as self-made content is being introduced and it allows individual citizens an opportunity to similar data collection which was earlier possible only for large corporations. This means that everybody can be a data collector, a service provider or an application operator.

On chapter “3.2.6 Spectrum”

“The necessity for and possibility of globally harmonised spectrum for 'IoT-devices' shall also be considered in bilateral contacts with the EU’s trading partners and through the International Telecommunications Union.” This is an important thing to follow-up and should also be discussed in the EC RFID Expert Group forum.

On chapter “3.2.7 Standardisation”

Interoperability cannot be emphasized too much as it truly is key for mass adoption of RFID and other IoT technologies, enabling cost-effective implementations and feasible application and system integration.

On chapter “4. The Policy Challenges of the Internet of Things”

The list of policy issues do seem to span the issues brought up and discussed in the workgroups of the EC RFID / “The Internet of Things” Expert Group quite well.

On “Annex I – Likely Evolution of RFID Architectures” and “Annex II – Research and Innovation for the Internet of Things”

“Another scenario predicted in some reports⁷ is two separate tracks of development: one into the direction of the very cheap item-level tag and the other in the direction of sophisticated multi-purpose tags putting constraints on the functionality that can be requested, e.g. to enhance security, for these low end devices.” This paraphrases well the fact that the most low-cost solution cannot possibly or necessarily be the most secure one.

“A multiplicity of services will be composed from global sources: as an example, an event pertaining to an object could be linked to the location (GPS or Galileo coupling), and generate a command to a local device. So usage scenarios will use multiple sources of aggregated services which might in turn result in a need for increased levels of openness and stronger interoperability requirements.” Noteworthy also is that such usage scenarios also propose for care and attention in protecting consumer privacy and security.