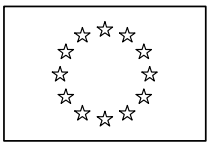

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 18.6.2009
COM(2009) 278 final

# COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

## Internet of Things — An action plan for Europe

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS**

# Internet of Things — An action plan for Europe

## 1. INTERNET OF THINGS: THE UMBRELLA FOR A NEW PARADIGM

The growth of the Internet is an ongoing process: only twenty-five years ago it was connecting about a thousand hosts and has grown ever since to link billions people through computers and mobile devices. One major next step in this development is to progressively evolve from a network of interconnected computers to a network of interconnected objects, from books to cars, from electrical appliances to food, and thus create an 'Internet of things'[1] (IoT). These objects will sometimes have their own Internet Protocol addresses, be embedded in complex systems and use sensors to obtain information from their environment (e.g. food products that record the temperature along the supply chain) and/or use actuators to interact with it (e.g. air conditioning valves that react to the presence of people).

The scope of IoT applications is expected to greatly contribute to addressing today's societal challenges: health monitoring systems will help meet the challenges of an ageing society[2]; connected trees will help fight deforestation[3]; connected cars will help reduce traffic congestion and improve their recyclability, thus reducing their carbon footprint. This interconnection of physical objects is expected to amplify the profound effects that large-scale networked communications are having on our society, gradually resulting in a genuine paradigm shift.

To complement this overview, it is worth noting three points that highlight the complex nature of IoT. First, it should not be seen as a mere extension of today's Internet but rather as a number of new independent systems that operate with their own infrastructures (and partly rely on existing Internet infrastructures). Second, as detailed in a recent ISTAG report[4], IoT will be implemented in symbiosis with new services. Third, IoT covers different modes of communication: things-to-person communication and thing-to-thing communications, including Machine-to-Machine (M2M) communication that potentially concerns 50-70 billion 'machines', of which only 1 % are connected today[5]. These connections can be established in restricted areas ('intranet of things') or made publicly accessible ('Internet of things').

The advent of IoT is taking place in an ICT environment affected by several major trends[6]. 'Scale' is one of them: the number of connected devices is increasing, while their size is reduced below the threshold of visibility to the human eye. 'Mobility' is another: objects are ever more wirelessly connected, carried permanently by individuals and geo-localisable. 'Heterogeneity and complexity' is a third trend: IoT will be deployed in an environment

---

1 See the ITU 2005 report www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf or the ISTAG report ftp://ftp.cordis.europa.eu/pub/ist/docs/istagscenarios2010.pdf

2 See for example www.aal-europe.eu/about-aal

3 See for example — www.planetaryskin.org/

4 See 'Revising Europe's ICT Strategy', — ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-revising-europes-ict-strategy-final-version_en.pdf

5 This figure is commonly used by different authors who assume that every human is on average surrounded by ~10 machines

6 See COM/2008/0594 final — Future networks and the Internet

already crowded with applications that generate a growing number of challenges in terms of interoperability.

The above examples show that the Internet of things can help to improve citizens' quality of life, delivering new and better jobs for workers, business opportunities and growth for the industry, and a boost to Europe's competitiveness. So this paper dovetails with the wider policy initiatives related to the Lisbon strategy and with the current thinking on post-i2010 initiatives[7]. The idea was first announced in the RFID communication[8] and has since received input from the RFID Expert Group[9], the EESC[10], and the EU Presidential Conferences of Berlin, Lisbon and Nice[11]. It comes in response to the invitation made by the Council[12] to *deepen the reflection on the development of decentralised architectures and promoting a shared and decentralised network governance* for the Internet of things. Finally, this paper takes account of the initial position outlined by the Commission[13] and the comments received[14].

## 2. SOME EXISTING INTERNET OF THINGS APPLICATIONS

IoT should not be considered as a utopian concept; in fact, several early-bird components of IoT are already being deployed as illustrated hereafter:

- Consumers are increasingly using web-enabled mobile phones equipped with cameras and/or employing Near-Field Communication[15]. These phones allow users to access additional information regarding products such as allergen information.
- Member States are increasingly using unique serial numbers on pharmaceutical products (supported by bar-codes), enabling the verification of each product before it reaches the patient. This reduces counterfeiting, reimbursement fraud and dispensing errors[16]. A similar approach taken on the traceability of consumer products in general would improve Europe's ability to tackle counterfeiting and to take measures against unsafe products[17].
- Several utility companies in the energy sector have started deploying smart electrical metering systems which provide consumption information to consumers in real time and allow electricity providers to monitor electrical appliances remotely[18].
- Within traditional industries, such as logistics (eFreight)[19], manufacturing[20] and retail, 'intelligent objects' facilitate the exchange of information and increase the effectiveness of the production cycle.

---

7 See ec.europa.eu/information_society/eeurope/i2010/index_en.htm
8 See COM/2007/0096 final — RFID in Europe: steps towards a policy framework
9 See 2007/467/EC — Decision setting up the Expert Group on RFID
10 See EESC Opinion n°1514 of 2008
11 See www.internet2008.eu
12 See Council Conclusion 16616/08
13 See SEC/2008/2516 — Early Challenges regarding the "Internet of Things"
14 See ec.europa.eu/information_society/policy/rfid/library/index_en.htm
15 See www.nfc-forum.org/home
16 See the work of EFPIA — www.efpia.eu/Content/Default.asp?PageID=566
17 See RAPEX annual report ec.europa.eu/consumers/safety/rapex/docs/rapex_annualreport2009_en.pdf
18 See www.esma-home.eu/default.asp
19 See COM/2007/0607 final – Freight Transport Logistics Action Plan
20 See The Fraunhofer Institute for Material Flow and Logistics : www.iml.fraunhofer.de/1327.html

These examples rely on several building blocks such as RFID, Near Field Communication (NFC), 2D bar codes, wireless sensor/actuators, Internet Protocol Version 6 (IPv6)[21], ultra-wide-band or 3/4G, which are all expected to play an important role in future deployments.

The European Commission, through the Framework Programme for Research and Development (FP5-6-7) and the Competitiveness and Innovation Framework Programme (CIP), has already invested in these technologies. For example, in the transport area, it is actively promoting their deployment through the Freight Transport Logistics and the Intelligent Transport System Action Plans[22]. Europe's industry is as well a strong player in many of these technologies, such as telecommunications equipment, enterprise software and semiconductors. Promoting the development of IoT thus reinforces the European ICT sector and should contribute to the growth of other sectors, such as those that include proximity services (tourism, personal healthcare, etc).

## 3. THE GOVERNANCE OF THE INTERNET OF THINGS

### Why is there a role for public authorities?

The technical advances described in the previous section will occur regardless of public intervention, simply following the normal cycle of innovation whereby industry harnesses for its own needs the new technologies developed by the scientific community.

Although IoT will help to address certain problems, it will usher in its own set of challenges, some directly affecting individuals. For example, some applications may be closely interlinked with critical infrastructures such as the power supply while others will handle information related to an individual's whereabouts.

Simply leaving the development of IoT to the private sector, and possibly to other world regions[23,24] is not a sensible option in view of the deep societal changes that IoT will bring about. Many of these changes will have to be addressed by European policy-makers and public authorities to ensure that the use of IoT technologies and applications will stimulate economic growth, improve individuals' well-being and address some of today's societal problems.

Finally, it must be stressed that a number of principles that should also underlie the governance of the IoT have already been debated at the World Summit on the Information Society (WSIS)[25]. The EU was a key contributor to this international consensus, reflecting its earlier positions[26]. An important point here is that WSIS recognised the responsibility of governments for public policy issues[27]: public authorities cannot shirk their responsibilities towards their citizens. In particular, the governance of the IoT must be designed and exercised in a coherent manner with all public policy activities related to Internet Governance.

---

21 See the related work conducted at IETF: tools.ietf.org/wg/6lowpan/

22 See COM/2008/0886 final – Action plan for the deployment of ITS in Europe

23 The American National Intelligence Council considers ubiquitous computing as one of the nine technologies that will be a 'game-changer' by 2025. See www.dni.gov/nic/NIC_2025_project.html

24 Songdo (South Korea) is a 6km² city, now under construction, that will showcase the first large-scale deployment of IoT. See www.songdo.com/page1992.aspx

25 The Tunis Agenda for the Information Society, one of the main outcome documents of WSIS, outlines the main principles www.itu.int/wsis/documents/doc_multi.asp?lang=fr&id=2266|2267

26 See COM/2006/0181 final — Towards a Global Partnership in the Information Society: Follow-up to the Tunis Phase of the WSIS

27 Tunis Agenda paragraph 35a states that '*policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues*'

**The governance of what?**

Typically, things become connected by getting assigned an identifier and a means to be connected to other objects or to the network. The amount of information on the object is usually limited, the remainder residing elsewhere in the network. In other words: accessing information related to an object implies establishing a network communication. Immediate questions arise as to:

– How is this identification structured? (the object naming)

– Who assigns the identifier? (the assigning authority)

– How and where can additional information about that thing be retrieved, including its history? (the addressing mechanism and the information repository)

– How is information security ensured?

– Which stakeholders are accountable for each of the above questions, what is the accountability mechanism?

– Which ethical and legal framework applies to the different stakeholders?

IoT systems which have not properly addressed these questions could have serious negative implications, such as:

– Mishandled information could reveal an individual's personal data or compromise the confidentiality of business data.

– Unsuitable assignation of rights and duties of private actors could stifle innovation.

– Lack of accountability could jeopardise the functioning of the IoT system itself.

**Line of action 1 — Governance**

The Commission will initiate and promote, in all relevant fora, discussions and decisions on:

– defining a set of principles underlying the governance of IoT;

– setting up an 'architecture' with a sufficient level of decentralised management, so that public authorities throughout the world can exercise their responsibilities as regards transparency, competition and accountability.

## 4. LIFTING THE OBSTACLES TO THE UPTAKE OF THE INTERNET OF THINGS

Besides the governance issues addressed in section 3, as IoT becomes a reality there are many other issues still unresolved, each of them constituting a potential impediment to IoT uptake. This section will highlight the main ones and detail the actions the Commission intends to take to address them.

**Privacy and protection of personal data**

Social acceptance of IoT will be strongly intertwined with respect for privacy and the protection of personal data, two fundamental rights of the EU[28]. On one hand, the protection of privacy and personal data will have an influence on how IoT is conceived. For example, a home equipped with a health monitoring system could process some of the inhabitants'

[28] See Articles 7 and 8 of the Charter of Fundamental Rights of the European Union

sensitive data. A prerequisite for trust and acceptance of these systems is that appropriate data protection measures are put in place against possible misuse and other personal data related risks.

On the other hand, it is likely that the uptake of IoT will affect the way we understand privacy. Evidence for this is given by recent ICT evolutions, such as mobile phones and online social networks, particularly among younger generations.

**Line of action 2 — Continuous monitoring of the privacy and the protection of personal data questions**

The Commission recently adopted a Recommendation[29] that provides guidelines on how to operate RFID applications in compliance with privacy and data protection principles; in 2010 it intends to publish a broader Communication on privacy and trust in the ubiquitous information society.

These two examples illustrate how, in practice, the Commission will watch over the application of data protection legislation to IoT:

– by consulting, when necessary, the Article 29 Data Protection Working Party;

– by providing guidance on the correct interpretation of EU legislation;

– by fostering dialogue among stakeholders;

– by proposing, if necessary, additional regulatory instruments.

**Line of action 3 — The 'silence of the chips'**

The Commission will launch a debate on the technical and legal aspects of the 'right to silence of the chips', which has been referred to under different names by different authors[30] and expresses the idea that individuals should be able to disconnect from their networked environment at any time.

**Trust, Acceptance and Security**

Information security is a must and is seen by most stakeholders as a major concern of IoT.

In the private sphere, information security is closely linked to the questions of trust and privacy mentioned above. Past experience with the development of ICT shows that they are sometimes neglected during the design phase, and that integrating features to safeguard them at a later stage creates difficulties, is costly and can considerably reduce the quality of the systems. It is therefore crucial that IoT components are designed from their inception with a privacy- and security-by-design mindset and comprehensively include user requirements.

As part of its 2009 Work Programme, in support of EU policy, the European Network and Information Security Agency (ENISA) has undertaken to identify emerging risks affecting trust and confidence, in particular regarding RFID. This constitutes a first step in the understanding of the privacy and security risks that will impinge on IoT.

---

29 See C(2009)3200 — Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification

30 See Adam Greenfield, *'Everyware'*, ISBN 0321384016

Another key aspect to building trust is the capability to adjust the functioning and properties of technological systems to individual preferences (within safe boundaries). Studies[31] have shown that giving users a sufficient level of control improves their level of trust and plays an important role in the uptake of the technology.

In the business sphere, information security translates into the availability, reliability and confidentiality of business data. For a company, questions arise as to who has access to their data or how they can grant partial access to their data to a third party. These questions, while in appearance simple, are profoundly affected by the complexity of today's business processes[32].

**Line of action 4 — Identification of emerging risks**

The Commission will follow the ENISA work mentioned above and will take further action as appropriate, including regulatory and non-regulatory measures, to provide a policy framework that enables IoT to meet the challenges related to trust, acceptance and security.

**Line of action 5 — IoT as a vital resource to economy and society**

Should IoT grow to the importance it is expected to attain, any disruption might have a significant impact on economy and society. The Commission will therefore closely follow the development of IoT infrastructures into a vital resource for Europe, especially in connection with its activities on the protection of critical information infrastructure[33].

**Standardisation**

Standardisation will play an important role in the uptake of IoT, by lowering entry barriers to newcomers and operational costs for users, by being a prerequisite for interoperability and economies of scale and by allowing industry to better compete at international level. IoT Standardisation should aim at rationalising some existing standards or developing new ones where needed.

IoT would also greatly benefit from a rapid deployment of IPv6, as proposed by the Commission[34] and endorsed by the Council, as this would make it possible to directly address any number of objects needed through the Internet.

**Line of action 6 — Standards Mandate**

The Commission will assess the extent to which existing standards mandates can include further issues related to IoT[35] or launch additional mandates if necessary. Additionally, the Commission will keep monitoring developments in European Standards Organisations (ETSI, CEN, CENELEC), their international counterparts (ISO, ITU) and other standards bodies and consortia (IETF, EPCglobal, etc) with a view for IoT standards to be developed in an open, transparent and consensual manner with the participation of all interested parties.

---

31 See the European research project SWAMI: www.isi.fraunhofer.de/t/projekte/e-fri-swami.htm

32 See the related work of IETF — https://www.ietf.org/mailman/listinfo/esds

33 See COM/2009/0149 final — Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience

34 See COM/2008/0313 final — Advancing the Internet: action plan for the deployment of IPv6 in Europe

35 See mandate EC/436 on RFID and mandate EC/441 on smart meters

Particular attention will be given to the machine-to-machine workgroup of the European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF) in the area of discovery services.

**Research and Development**

The Commission recently highlighted[36] its ambitions with regard to ICT research and proposed a number of measures to strengthen it in Europe. IoT is a promising candidate to contribute to this initiative, as it addresses wide societal problems and is an area where the EU and Member States have already achieved auspicious results, though significant research is still needed[37] to make IoT a reality.

**Line of action 7 — Research and Development**

The Commission will continue to finance FP7 research projects in the area of IoT, putting an emphasis on important technological aspects such as microelectronics, non-silicon based components, energy harvesting technologies, ubiquitous positioning, networks of wirelessly communicating smart systems, semantics, privacy- and security-by-design, software emulating human reasoning and on novel applications.

**Line of action 8 — Public-Private Partnership**

The Commission is currently preparing the setting-up of four public-private partnerships (PPP) where IoT can play an important role. Three of them, 'green cars', 'energy-efficient buildings' and 'Factories of the Future' were proposed by the Commission as part of the recovery package[38]. The fourth one, 'Future Internet', aims at further integrating the existing ICT research efforts in relation to the future of the Internet[39].

**Openness to innovation**

IoT systems will be designed, managed and used by multiple stakeholders driven by different business models and various interests. To be a catalyst for growth and innovation, these systems should:

– allow new applications to be built on top of existing systems and new systems to be deployed in parallel with existing systems without creating excessive burdens for market entry or other operational barriers, such as excessive licenses/fees or inappropriate intellectual property schemes[40];

---

36 See COM/2009/0116 final — A Strategy for ICT R&D and Innovation in Europe: Raising the Game

37 See the EU-EPoSS joint workshop report: www.iot-visitthefuture.eu/fileadmin/documents/researchforeurope/270808_IoT_in_2020_Workshop_Report_V1-1.pdf

38 See COM/2008/0800 final — A European Economic Recovery Plan

39 See www.future-Internet.eu

40 As an illustration, the efforts by essential RFID patent-holders to offer a one-stop shop for patent-users reveal the complexity and length of such a process. See www.rfidlicensing.com/ or the '*RFID Journal*' of 13 April 2009, *'RFID Consortium Readies to Launch First Licenses'* — www.rfidjournal.com/article/view/4785

– allow an adequate level of interoperability so that innovative and competitive cross-domain systems and applications can be developed.

Many of the technologies mentioned in section 2 are already mature. However, in some cases, real-case user-driven scenarios do not yet exist, leading to a situation where the uptake of the technology itself is slowed down. This is reinforced by the fact that the business models supporting IoT are not yet established and industry is sometimes hesitant to invest. Europe can be a catalyst in such situation by encouraging and, where appropriate, funding projects aimed at validating these applications.

**Line of action 9 — Innovation and pilot projects**

Complementing the research activities listed above, the Commission will consider promoting the deployment of IoT applications by launching pilot projects through CIP[41]. These pilots should focus on IoT applications that deliver strong benefits to society, such as e-health, e-accessibility, climate change, or helping to bridge the digital divide.

**Institutional awareness**

The preparatory work for the Communication has revealed that only a limited number of industrial and institutional stakeholders have a comprehensive understanding of the challenges and opportunities posed by IoT.

**Line of action 10 — Institutional Awareness**

The Commission will regularly inform the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions, the Article 29 Data Protection Working Party[42] and any other relevant stakeholders about IoT developments.

**International dialogue**

Many IoT systems and applications will be borderless by nature and therefore require a sustained international dialogue, notably on matters of architecture, standards and governance.

**Line of action 11: International dialogue**

The Commission intends to intensify the existing[43,44] dialogue on all aspects of IoT with its international partners, aiming to agree on relevant joint actions, share best practices and promote the lines of action laid down in this Communication.

---

41 See ec.europa.eu/cip/index_en.htm

42 See ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

43 As part of the 2007 Framework for Advancing Transatlantic Economic Integration between the European Union and the United States, cooperation on RFID has been singled out and EU and US are now exchanging best practices to optimise the economic and social impacts of RFID. See ec.europa.eu/enterprise/policies/international/cooperating-governments/usa/transatlantic-economic-council/index_en.htm

44 In summer 2009, the Directorate-General Information Society and Media of the Commission will sign a memorandum of cooperation with the Japanese Ministry of Economy, Trade and Industry on, among others, RFID, wireless sensor networks and the Internet of things

**Waste management**

In many cases, the connection between objects will be made through a sensor or a tag embedded in the object. For the foreseeable future, tags[45] will be made of metal (typically silicone, copper, silver and aluminium) whose presence can create difficulties on the recycling lines of glass, plastic, aluminium and tinplate.

On the other hand, being able to precisely identify objects during the recycling process is an advantage and tagged objects could therefore be recycled more efficiently by being retrieved from normal bulk waste disposal.

**Line of action 12 — RFID in recycling lines**

As part of its regular monitoring of the waste management industry, the Commission will launch a study to assess the difficulties of recycling tags and the benefits and nuisances that the presence of tags can have on the recycling of objects.

**Future developments**

As mentioned earlier, IoT is not a monolith but an umbrella that covers a diverse range of technologies, systems and applications being developed on a constant basis.

While engaging in constant monitoring of the evolution of IoT, the Commission will pursue its activities on:

– **the timely availability of appropriate spectrum resources.** The increased number of connected devices will require a new level of infrastructure deployment, both in terms of wired and wireless connectivity. For wireless communications, ensuring the timely availability of spectrum resources is important[46], and the Commission will continue to monitor and assess the need for additional harmonised spectrum for specific IoT purposes;

– **electromagnetic fields (EMF).** Most of today's foreseeable IoT devices are expected to be in the 'radiofrequency' group (i.e. >100 kHz) and operate with very low power, unlikely to produce significant levels of exposure to EMF. The existing regulatory framework on EMF[47] is under periodic review and will keep ensuring that all devices and systems will respect the safety and health needs of the population in the future.

**Line of action 13 — Measuring the uptake**

Eurostat will start publishing in December 2009 statistics on the use of RFID technologies.

Monitoring the introduction of IoT related technologies will provide information on their degree of penetration and allow the assessment of their impact on the economy and the society as well as the effectiveness of the related Community policies.

---

45 Long-term research is being conducted into making these tags out of organic and biodegradable material

46 Specifically, the intention is to regularly update the short-range devices (SRD) decision (See 2006/771/EC)

47 See Council Recommendation 1999/519/EC and Directives 1999/5/EC, 2004/40/EC and 2006/95/EC. See as well the opinion of 19 January 2009 from the Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR)

**Line of action 14 — Assessment of evolution**

Beyond the specific aspects mentioned above, it is important that a multi-stakeholder mechanism is put in place at European level to:

– monitor the evolution of IoT;

– support the Commission in carrying out the various actions listed in this Communication;

– assess which additional measures should be undertaken by European Public Authorities.

The Commission will use FP7 to conduct this work, by gathering a representative set of European stakeholders and ensuring a regular dialogue and sharing of best practices with other world regions.

## 5. CONCLUSIONS

As this document has described, IoT is not yet a tangible reality, but rather a prospective vision of a number of technologies that, combined together, could in the coming 5 to 15 years drastically modify the way our societies function.

By adopting a proactive approach, Europe could play a leading role in shaping how IoT works and reap the associated benefits in terms of economic growth and individual well-being, thus making the *Internet of things* an *Internet of things for people*. Failing to do so would mean missing an important opportunity and could place Europe into a position where it is forced to adopt technologies that have not been designed with its core values in mind, such as the protection of privacy and personal data.

By launching a number of actions and reflections, the Commission intends to be a driving force behind this effort and it invites the European Parliament, the Council and all concerned stakeholders to work jointly to achieve these ambitious yet achievable objectives.