# *From Internet of Data to Internet of Things*

**28 January 2009**

**Gérald Santucci**

**Head of Unit**

**European Commission, Directorate-General Information Society and Media**

> *"You could not step twice into the same river;*
> *for other waters are ever flowing on to you."*
>
> Heraclitus, On the Universe, Greek philosopher (540 BC – 480 BC)

## ABSTRACT

"Internet of Things" is not a stand-alone concept but one part of the Future Internet. The European Commission is currently making an effort to mobilise stakeholders, especially those involved in EU-funded R&D projects, around the idea of a Future Internet Assembly reaching out to whoever has talent when it comes to debating the Internet of the Future. Within this context, the Internet of Things must be seen as a vision where "things", especially everyday objects, such as nearly all home appliances but also furniture, clothes, vehicles, roads and smart materials, and more, are readable, recognisable, locatable, addressable and/or controllable via the Internet. This vision will surely change with time, especially as synergies between Identification Technologies, Wireless Sensor Networks, Intelligent Devices and Nanotechnology will enable a number of advanced applications. Nevertheless, the early implementations of the Internet of Things are already arriving on the market, thanks to the innovative use of technologies such as RFID, NFC, ZigBee and Bluetooth, and are contributing to create a value proposition for Internet of Things stakeholders. We discuss here the origin of the concept "Internet of Things", the technology challenge, the potential applications, and the current and planned actions of the European Commission to further explore the challenges and opportunities raised by the Internet of Things and to address the main policy issues that its development may entail.

## KEYWORDS

Acceptance, accountability, awareness, discovery services, Future Internet, governance, Internet of Things, interoperability, liability, naming, Nano-Bio-Info-Cogno, privacy, security, spectrum

The number of world Internet users has grown 20-fold in the past decade to about 1.5 billion people in 2008[1], with the number of computer servers rising from 22.5 million to 489 million. Eventually, the entire world will have access through a variety of smart devices to the services that are available on the Internet.

This phenomenon raises two main considerations. On one hand, the Internet architecture is going to face increasingly complex challenges, many of them being related to "scalability" issues linked to the ever growing number of users, devices, service attributes, applications, contexts, and environments. Europe is committed to take a leading role in exploring the emerging visions for the Future Internet that will drive the requirements for its underlying network and service infrastructure.

On the other hand, the Internet will continue to go through many transformations. Taking a very simplistic yet useful short-cut to the history and destiny of the Internet, it is possible to distinguish four main trends that partially overlap and have the potential to change the way the Internet works and affects how we live. The first stage has been about linking and sharing computers – the "Internet of Data". The second stage has been about linking and sharing documents and pages – the "Internet of Content". We are now at the beginning of the third stage which is about connecting with others and share – the "Internet of People". We have always had a social dimension, but the Internet is unleashing it in unforeseen new ways with considerable force. As barriers to entry to the Internet are getting lower and lower, the Internet looks more socio-centric. Consequently, social network sites such as Myspace.com, Facebook, Classmates Online or Linkedln are becoming the hub of the Internet while virtual world platforms such as Second Life or Twinity are looming on the horizon as the logical next step. But this third stage is not the end of the story. We can already catch a glimpse of a fourth stage beyond, which is the drift towards linking up the things themselves.

This paper will tell the beginning of the Internet of Things story. It is a fantastic journey if we consider that there are on Earth today 6.6 billion human beings (this is the potential of the "Internet of People"), around 50 billion machines (this is the potential of the "Internet of Machines"), and around 50 000 billion "things" (this is the potential of the "Internet of Things").

## <u>How It All Got Started?</u>

The term "Internet of Things" appears to have been coined by Kevin Ashton who first used it in a presentation at the Procter & Gamble Company in the spring of 1998: "*Adding radio-frequency identification and other sensors to everyday objects will create an Internet of Things, and lay the foundations of a new age of machine perception.*"

Since the beginning, Internet of Things has therefore been the vision of everyday items from TVs to toothbrushes, sports equipment and even buildings having in-built computing power and wireless that would allow them to communicate and share information.

Ironically, at about the same time Ashton was heralding the "Internet of Things", the European Union's Information Society Technologies Program Advisory Group (ISTAG) used the term "ambient intelligence" in a similar manner to describe a vision where people

[1] Source: Internet World Stats, figures for 30 June 2008.

will be surrounded by intelligent and intuitive interfaces embedded in everyday objects around us[2].

Incidentally, it is odd, and perhaps telling, that over the years Europe 'forgot' the term "Ambient Intelligence", which it had invented, and 'imported' and re-used the term "Internet of Things", which originally was invented by a British innovator and marketer and which made its way mainly in a U.S. private research university.

Anyway, at the EPC Executive Symposium in Chicago, Illinois, in September 2003, which marked the official launch of the first platform of the Electronic Product Code Network, the same Kevin Ashton, then executive director of the Auto-ID Center at the Massachusetts Institute of Technology (MIT), predicted that the EPC Network would enable machines to sense man-made objects anywhere in the world, thus effectively creating an "Internet of Things".

Two years after, in November 2005, the International Telecommunication Union (ITU) released its famous report on the Internet of Things, which was taking a look at the next step in "always on" communications – a vision in which new technologies like RFID, embedded systems, smart computing and nanotechnology promise a world of networked and interconnected devices that provide relevant content and information wherever the user is located.

Another 16 months were to pass before the European Commission, at the end of one year of extensive consultations, adopted a Communication on RFID[3], in which it was announced that it "*will continue to closely monitor the move towards the "Internet of Things", of which RFID is expected to be an important element, [and] will publish a Communication analysing the nature and the effects of these developments, with particular attention to the issues of privacy, trust and governance.*" This commitment triggered a thorough reflection process which culminated in the organisation by the German, Portuguese and French Presidencies of the European Union, of three major conferences and exhibitions, held respectively in June 2007, November 2007, and October 2008.

## The Internet of Things: Hip or Hype?

So, ten years after it has been coined by a member of the RFID community, the term "Internet of Things" is now recognised by Governments, Academia and the Global Industry as the right concept to refer to the general idea of "things", especially everyday objects, which are readable, recognisable, locatable, addressable and even controllable via the Internet. Hence, the Internet of Things can be defined as a world-wide network of networks, based on standard communication protocols, in which individual objects are interconnected and operate cooperatively.

In the context of the Internet of Things, everyday objects include not only the few electronic devices we use everyday, and not only the products of higher technological development such as vehicles and appliances, but actually all "things" that we do not ordinarily think of as electronic – such as clothes and food; materials, parts and

[2] ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-99-final.pdf

[3] Commission Communication on "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework", COM(2007) 96 final of 15 March 2007.

subassemblies; commodities and luxury items; buildings, monuments and sidewalks; and many other objects that belong to the population of around 50,000 billion things existing today on Earth!

At this level of abstraction, is the Internet of Things fact, fiction or exaggeration? Is it science fantasy or a technological probability? Is it hip or hype? Is it hype or hope?

Some early signs tend to show that the Internet of Things is to become a reality and that its realisation has actually begun to unfold in 2008, when most developers and visionary people recognised the soundness and relevance of the concept and the inevitability of its logic and widespread development.

Firstly, on 27 November 2008, the Council of the European Union, in its conclusions on Future Networks and the Internet acknowledges and endorses the work of the European Commission on the Internet of Things and invites the Member States and the Commission to further explore the key challenges and opportunities raised by the emergence of the Internet of Things. The Council especially raises the issues of privacy, security and governance as ones which the Member States and the European Commission should address in the near future.

Secondly, Cisco, Atmel, the Swedish Institute of Computer Science (SICS) and other leading technology vendors and users formed on 16 September 2008 the IP for Smart Objects (IPSO) Alliance and announced, a few weeks after, the availability of uIPv6, one of the world's smallest open-source, IPv6-ready protocol stack, which could enable every device, no matter how limited by power or memory to have an Internet Protocol address, thus promoting the "launch of the Internet of Things"[4].

Thirdly, Vinton Cerf, one of the fathers of the Internet, wrote on the Official Google Blog on 25 September 2008[5] that "*the Internet of the future will be suffused with software, information, data archives, and populated with devices, appliances, and people who are interacting with and through this rich fabric.*" A few months earlier, he had said in a newspaper interview[6] that billions of Internet-enabled devices with communication capabilities would emerge in the Internet of Things.

Fourthly, the Internet of Things is one of TIME magazine's 50 Best Inventions of 2008[7].

Fifthly, the Internet of Things is one of the Top Ten Inventions of 2008 which Ron Callari, a well-known American freelance journalist, has identified[8].

Sixthly, to support the U.S. National Intelligence Council in the elaboration of its 2008 Report on Global Trends 2025, SRI Consulting Business Intelligence has identified the Internet of Things as one of six Disruptive Technologies that may have an invaluable impact on U.S. national power, i.e. economic development and military capability.

So, infused with such a burst and palpable sense of excitement, the Internet of Things seems to be really hip.

[4] See http://www.ipso-alliance.org/Pages/Main.php

[5] http://googleblog.blogspot.com/2008/09/next-internet.html

[6] "Vers l'Internet à tout faire", interview with Le Monde, 5 April 2008.

[7] http://www.time.com/time/specials/packages/0,28757,1852747,00.html

[8] http://inventorspot.com/articles/top_ten_inventions_2008_21971

## Early Implementations of the Internet of Things

The Internet of Things cannot be reduced to one specific technology or application. In particular, the vision of the Internet of Things is not about the next generation RFID. The Internet of Things encompasses various technological solutions – RFID, sensor networks, actuators, TCP/IP, mobile technologies, software, etc. – which enable to identify objects and collect, store, process and transfer information not only in physical environments but also between the physical and virtual worlds.

Radio Frequency Identification (RFID), Near Field Communication (NFC), ZigBee and Bluetooth are among the key technologies currently at the front of the Internet of things. Let's look at a few examples of how these technologies are used today in a way that illustrates the many facets of Internet of Things applications.

### RFID

RFID marks the dawn of the Internet of Things – this is one of the key messages which the European Commission has passed in its RFID Communication of March 2007. The case of the Nabaztag Internet rabbit, created by Violet, is an interesting example. The company launched in 2008 its Mir:ror – a simple white disk which connects to a computer via USB[9]. The device is an RFID reader, which takes instructions from Violet's "Ztamps", which are essentially RFID tags and similar to those in use in the Oyster card[10] and electronic keys. The Ztamps already feature in mini-versions of the Nabaztag rabbits, as well as pre-programmed objects such as books. Now, the tags can be added to any object a user wants. Swipe the tag over the Mir:ror reader, and various applications are triggered, including Facebook, video and email. Violet co-founder Rafi Haladjian said: "*We are still living in a world where information is trapped in a few of our objects. We stare into our screens, which are like goldfish bowls full of information swimming around, but unable to escape. At Violet, we dream of a world where information would be a butterfly, flitting freely all over the place, and occasionally landing on any of the objects we touch to give them life and enrich them. We want to breathe magic into the world around us. This is our idea of the Internet of Things, and the Mir:ror is the first step in this direction.*"

### NFC

NFC, a technology that enables connections between notably mobile phones and physical things, has been designed to increase the usability of mobile devices and integrate networked services into physical space. This technology introduces a sense of touch, where interactions between devices are initiated by physical proximity. Touch-interactions are significant culturally and socially; touch carries meaning and this changes according to context, situation and culture. There is a rich history of industrial design, ergonomic and human factors research that can be used in the design of NFC-enabled systems. By using simple actions, NFC puts a sense of human control back into otherwise complex ubiquitous systems. For example, an NFC application pointing at the Internet of Things is tikitag, a new product launched by Alcatel-Lucent on 1 October 2008[11]. Tikitag, leveraging innovations within Bell Labs, enables consumers and third-party application developers to increase the value of everyday items by connecting them to online content or applications.

[9] http://www.violet.net/

[10] http://www.tfl.gov.uk/tickets/oysteronline/2732.aspx

[11] http://www.tikitag.com/

The tikitag service enables the launching of online applications by simply touching an NFC device, such as a mobile phone, to an item tagged with an RFID chip. Tikitag can be used in a variety of environments, for example in an in-home application (a father can use tikitag to link his child's teddy bear to an online story about that same bear), in an outdoor environment (tikitag makes it possible for a visitor to an art gallery to wave his NFC enabled mobile phone at a painting and then see the painter's Wikipedia profile appear on the phone's screen) or in a business environment (a cleaning company can use tikitag to record that a room has been successfully cleaned through a simple touch of an NFC-enabled mobile phone to a tikitag-linked tag that has been placed in the room).

### ZigBee

ZigBee, a standard for mesh networking, in which tiny low-powered radios form networks by passing data among themselves, is another promising solution for certain applications of the Internet of Things[12]. In February 2008, the ZigBee Alliance, a global ecosystem of companies creating wireless solutions for use in energy management, commercial and consumer applications, confirmed its commitment to further enhance ZigBee connectivity to the Internet and other networks. As a global open standard, ZigBee offers wireless networking to a wide range of devices ranging from light switches to thermostats, and electric meters to medical devices. To take just a recent example, Tendril[13] is making software that allows companies in the industrial and building automation, physical security and home automation industries to build, deploy and manage ZigBee applications, thus addressing the macro trends of energy efficiency, security, life expectance and connectedness.

### Bluetooth

Bluetooth can put the Internet of Things in the hands of the consumer. At the Consumer Electronics Show in Las Vegas in January 2009, Cambridge Consultants launched CatchNet, a new custom Internet-enabled device platform which features the first single chip Bluetooth modem running all of the protocols needed for Internet connectivity. For the consumer, devices developed on the CatchNet platform have the potential to provide seamless, ubiquitous access to their favourite online services, for example to indicate the level of congestion on the user's usual route between home and workplace, thus allowing them to delay their normal departure or to take an alternative route, or to allow a user to browse for a nearby bar, restaurant, club or cinema while out shopping or with friends, review independent peer rankings, and then be guided to their selected venue.

Looking ahead, a recent patent application filed by Apple, titled "Personal area network systems and devices and methods for use thereof" outlines its vision of a new Personal Area Network (PAN) that would make use of RF modules in everything, from clothes to accessories, to communicate with each other and connect to the Internet. It offers us a speculative indication of how the future of gadget interconnectivity might be. The

[12] The case of ZigBee is an interesting one. Some years ago ZigBee appeared to be a technological dead-end, crushed between cheaper RFID and more powerful Wi-Fi. But when the U.S. electricity industry decided to replace old electricity meters with new, network-enabled devices that would not just monitor energy consumption but potentially control it as well, Wi-Fi appeared to be too expensive and too power-hungry, while ZigBee was the obvious solution for meters, air conditioners and light switches that were conveniently located right alongside one another.

[13] http://www.tendrilinc.com/

embeddable modules would be smart enough to identify themselves and enable both short-range (WiFi and Bluetooth) and long-range (GSM, 3G, WiMax) connections between portable gadgets, in an automated manner. In other words, portable gadgets (e.g., an iPod, a handbag) would be able to communicate with and identify themselves to any other modules around and, potentially, piggyback their way onto the Internet.

This may look speculative at the moment, but it shows at least that the future starts now in the dreams of human beings and the inventive talents and innovative strengths of companies.

## The Technological Challenge

Obviously, the concept of an Internet of Things connecting everyday objects by means of the Internet Protocol and allowing both thing-to-person communications and thing-to-thing communications goes far beyond the applications that are visible today. The combination of embedded microcontrollers, sensors, actuators, network interfaces, and the enhanced Internet makes it likely for the Internet, whether by *evolution* (i.e. making the Internet a little better through incremental changes) or by *revolution* (i.e. rethinking the fundamental assumptions and design decisions underlying the Internet current architecture), to evolve from a network of interconnected computers to a network of interconnected objects. The Internet of Things is deemed to supplement the original Internet of Data.

Capacity will be the challenge that will need to be addressed in priority. As more devices become part of the Internet – there are some 50,000 billion "things" on Earth[14] – it will be essential to move to a new Internet address space. With its 128 bits of address space, that is about 340 trillion trillion trillion addresses, IPv6 should provide ample address space for the foreseeable future. Major efforts, especially in Japan, China and Europe[15], are being made to bring IPv6 online in parallel with the current IPv4 system. Quantity is not the only issue – quality is as much important! Information on the web varies in quality from useless (or even damaging) to valuable. As the emergence of the Internet of Things will make available online more data, the importance of search engines will dramatically increase.

A recent report published in the United States[16] has shown that the development of the Internet of Things would critically depend on progress in machine-to-machine interfaces and protocols of electronic communication, microcontrollers, wireless communication, RFID, sensors, actuators, location technology, energy harvesting techniques, and software. In addition, some other technologies that are not essential to the development of the Internet of Things may yet play a synergistic role in the nature and speed of the

[14] Figure given by Philippe Lemoine, Chairman of LaSer, at Summer University of GS1 France. See www.gs1.fr/gs1_fr/securedownload/dl/42955/400872/file/universite2006.pdf, page 10.

[15] In the case of Europe, in May 2008 Viviane Reding, Commissioner for the Information Society and Media, called upon governments and industry to accelerate the transition from IPv4 to IPv6, thus avoiding the risk of falling short of Internet addresses within 3 years, a situation which the "Internet of Things" will further deteriorate. The European Commission, which has set the target that 25% of European Internet users should be able to connect to the IPv6 Internet by 2010, will be pushing for it, notably by encouraging public services and leading websites to move faster to IPv6 (see COM(2008) 313 final of 27 May 2008.

[16] Disruptive Technologies: Global Trends 2025, SRI Consulting Business Intelligence, Appendix F: The Internet of Things, 2008.

deployment of its applications: geo-tagging/geo-caching, biometrics, machine vision, robotics, augmented reality, mirror worlds, telepresence and adjustable autonomy, life recorders and personal black boxes, tangible user interfaces, "clean technologies".

In Europe, the Information Society Technologies Advisory Group (ISTAG)[17] and the European Commission consider that the emergence of the Internet of Things, especially how quickly it will develop and what capabilities it will have, depends on the ability of the stakeholders to address the following research challenges[18]:

- Edge technologies, such as sensors and actuators, passive/active RFID tags, embedded systems, making devices that are attached to real-world objects smart enough to participate in Internet of Things application scenarios;

- Networking technologies, such as fixed, mobile, wired and wireless networks, allowing the highly available bi-directional communication on different levels;

- Middleware systems and service-oriented architectures putting real-world data into the context of various Internet of Things applications;

- Platform services ensuring scalability, high availability, and the safe and secure execution of the requested functionalities;

- Web service technologies making information and services available while reducing interoperability issues and enhancing extensibility, platform independence and standardised exchange of messages.

It is essential to note that the topography of the Internet of Things is one of private networks, public (open) networks and mixed-use networks. In supply chain settings, the need for secure and selective visibility for data sharing is significant for commercial entities. It must be stressed that the Internet of Things will not be, in all respects, globally and publicly accessible like the Internet. Therefore, interoperability will be a key issue in the future deployment of the Internet of Things.

## <u>The Applications of the Internet of Things</u>

A majority of experts today would probably argue that the Internet of Things is logically consistent, technologically feasible and cost-effective, geopolitically challenging, economically justified, socially desirable, and environmentally responsible. Even if targeted socio-economic research and market studies are needed to substantiate the case for the Internet of Things, existing evidence suggests that the implementation of the Internet of Things has indeed begun and its potential benefits for the economy and society are real, perhaps enormous.

[17] See ftp://ftp.cordis.europa.eu/pub/ist/docs/future-internet-istag_en.pdf

[18] For more details, see also: Santucci G., *Policy and Technological Drivers in the Internet of Things*, paper for the Internet of Things 2008 International Conference for Academia and Industry, Zurich, Switzerland, 27 March 2008, http://ec.europa.eu/information_society/policy/rfid/documents/gsiotspeech.pdf

However, if the Internet of Things should boost the technology prowess of those countries and organisations investing in it, the issue remains unclear as to which applications of the Internet of Things are likely to drive further market growth, be profitable, and meet the needs of stakeholders.

A workshop jointly organised in February 2008 by the European Commission and the EPoSS European Technology Platform[19] was the first initiative in Europe to suggest key uses and instantiations of the Internet of Things.

The first type of applications will concern "things on the move", especially in the retail, logistics, pharmaceutical, and food sectors. Today, RFID technology is already used for item identification in retail, from the producer to the storage, the shop floor, cashier and check-out, and to ensure theft protection, to increase transport, storage and handling efficiency as well as traceability achieving intelligent logistic management, including reduction in natural resource consumption, to prevent counterfeiting of drugs in the pharmaceutical sector, and to assure consumers that the food they buy is of controlled origin. But the Internet of Things should amplify the opportunities in these areas. For example, progress in nanotechnology will enable to embed smart biodegradable dust inside pills, which then may interact with the tag on the box or bottle, thus allowing the latter to monitor the use and abuse of medicine and inform the pharmacist when new supply is needed.

The second type of applications will concern "ubiquitous intelligent devices". The Internet of Things will make it possible for virtually any object around us to exchange information. This corresponds to the vision of "Ambient Intelligence" as promoted by the European Commission from 1999 onwards. Most devices will be able to execute behaviours according to a predetermined set of actions and even to make decisions following dynamically changing user preferences. Ultimately, advanced software will boost the capabilities of connected objects and enable them to interpret the environment, detect human intentions, make "human-like" inferences and decisions, and eventually act on behalf of people.

The third type of applications will concern "ambient and assisted living". For example, a pressure sensor in a bed detects heart rate, breathing, and movement; sensors in the floor nearby can detect when a person, in particular an elderly person, falls. This is perhaps the area where the applications of the Internet of Things will most be seen as being in the public interest. European, American and Japanese researchers are already carrying out dedicated work on such applications. In some areas of Tokyo, for instance, Ubiquitous Computing today supports human life through the collaborative operation of functions embedded in many objects in the living space – electric household appliances, walls, furniture, floors, sidewalks in cities (to guide blind people) or special computers (for physically challenged people); these objects are autonomous and can exchange information among them[20]. In a longer perspective, technological advances, especially the convergence of Nano-Bio-Info-Cogno[21], will create tremendous opportunities for improving citizens'

[19] See page 12.

[20] The TRONSHOW2009 organised by Professor Ken SAKAMURA in December 2008 in Tokyo was very informative about the current achievements and future potential of Ubiquitous Computing. See http://www.tronshow.org/index-e.html

[21] Nanotechnology, Biotechnology, Information Technology, Cognitive Science.

quality of life. This is particularly true for Assisted Living ("lab-on-a-chip" technologies, biodegradable materials, advanced telemedicine, in-vivo drug delivery, etc.), Intelligent Home (intelligent power control, energy conservation, use of robots for performing routine tasks, etc.), and Transportation (intelligent navigation systems, self diagnosis of vehicles, optimal route planning, energy harvesting, etc.). At the same time, ethical questions will be raised and seriously challenge any Internet of Things scenarios. The NBIC convergence will influence the development of the Internet of Things and will actually blur the boundary between therapy and improvement[22]. Where does therapy end, and where does human manipulation begin? Under what conditions is the intentional influencing of the human consciousness desirable or not? What are the human consequences of living in an Internet of Things where every item in our environment is intelligent and networked?

Therefore, the debate on the Internet of Things must focus on the opportunities as well as the threats deriving from its deployment in the form of applications supported by information and communication technologies but also eventually NBIC Converging Technologies embedded into everyday objects.

## The Role of the European Commission

The European Commission organised a workshop entitled "From RFID to the Internet of Things" on 6 and 7 March 2006[23]. This was the first in a series of five workshops that were held in 2006 to support the international debate on Radio Frequency Identification (RFID) launched by Commissioner Viviane Reding at CeBIT on 9 March 2006. The conclusions of this workshop regarding research perspectives (technology and applications) and non-research perspectives, especially the issue of naming and addressing, were taken into account in drafting the Commission Communication on RFID (March 2007) and in organising the two successive EU Presidency Conferences of Berlin (June 2007) and Lisbon (November 2007).

During 2008 two important developments occurred, which are likely to keep the Internet of Things on the list of top policy priorities in the years to come.

The first development was a public consultation on a Commission Staff Working Paper on the Internet of Things, which was made available to the public from 29 September to 28 November 2008 on the site "Your voice in Europe". Concerned stakeholders were invited to comment on issues raised in the document. During the consultation period, the web site was accessed 485 times and finally 36 responses were submitted from individuals, non governmental organisations, other associations and private companies. They addressed a wide range of policy issues: Internet of Things Architecture; Security; Privacy and Data Protection; Control of Critical Global Resources and Subsidiarity; Identity Management, Naming and Interoperability; Trials and Pilot Demonstrations; Spectrum; Standardisation;

[22] See *Converging Technologies for Improving Human Performance*, U.S. National Science Foundation, June 2002. The notion of "improving human performance" raises fundamental ethical and philosophical questions about what is called "transhumanism".

[23] See http://cordis.europa.eu/ist/audiovisual/neweve/e/conf6-70306/conf6-70306_a.htm (workshop program) and ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au_conf670306_buckley_en.pdf (workshop final report).

Ethics (the right to the *silence of the chips*); IPv6; Awareness Building; Accessibility, Digital Divide and Child Protection; Health (implications of Electro Magnetic Fields); E-waste (reuse, recycling and remediation of potential environmental harms). These issues will be considered in the drafting of the Communication on the Internet of Things, which was announced in the RFID Communication of March 2007 and is now scheduled for adoption by the European Commission in June 2009.

The second development has been the work started by the European Commission on the Internet of Things within the context of two broader policy initiatives: on one hand, a debate on the policy implications of developments concerning future networks and the Internet[24]; on the other hand, a special effort to explore and assess with all concerned stakeholders the perspectives emerging from R&D in Europe for the Future of the Internet[25].

The "Future Internet" theme has recently been gaining momentum all over the world. Europe is particularly active in this area. On 31 March 2008, the Future Internet Assembly was kicked off as the vehicle for discussion amongst concerned R&D projects and the European Technology Platforms at the Bled conference organised by the European Commission and the Slovenian EU Presidency[26]. Nine months later, on 9 and 10 December 2008, the Future Internet Assembly was held in Madrid as a networking meeting towards the Future Internet for Europe. The EU-funded projects selected through FP7-ICT Call 1 belonging to Challenge 1 "Pervasive and Trusted Network and Service Infrastructures" are collectively involved in addressing research issues like security, broadband, mobility, scalability, distributed services, media, dependability; which are all highly relevant for the Future Internet. The Future Internet Assembly is structured to allow open interactions and cross-fertilisation across technical domains and to promote a shared vision of what needs to be done for the Future Internet in Europe, common deliverables creating value for the projects concerned, joint strategic research agendas and the development of a consolidated calendar of events aiming at avoiding fragmentation of efforts.

Besides the public consultation on the Internet of Things and the broader debate on future networks and the Internet, further significant developments must be mentioned.

One concerns the clustering of research efforts at European level. On 15 January 2007, the European Commission called a meeting of relevant EU-funded research projects to recommend the creation of a Cluster of European RFID Projects (CERP). This cluster[27], which consists today of some 25 research projects, including a few national initiatives, was initially co-ordinated by Gerd Wolfram, Managing Director of MGI Metro Group Information Technology GmbH, and then from 13 February 2008 onwards by Patrick Guillemin, responsible within the ETSI Secretariat for development, co-ordination and management of new standardisation initiatives including the Internet of Things, RFID and related fields. At the cluster's 7th concertation meeting, held at ETSI Sophia-Antipolis on 8

[24] See COM(2008) 594 final of 29 September 2008 http://ec.europa.eu/information_society/eeurope/i2010/docs/future_internet/act_future_networks_internet_en.pdf

[25] See http://www.future-internet.eu/

[26] See the Bled Declaration at http://www.future-internet.eu/publications/bled-declaration.html

[27] See http://www.rfid-in-action.eu/cerp

October 2008, its name was changed from CERP to CERP-IoT to stress the commitment of the participating projects to address the challenges raised by the Internet of Things.

A second one concerns two Coordination and Support Actions funded by the European Commission within the context of the 7th Research Framework Programme[28]. On one hand, the CASAGRAS Coordination and Support Action for Global RFID-related Activities and Standardisation[29] provides a framework of foundation studies to assist the European Commission and the global community in defining and accommodating international issues and developments concerning RFID and the emerging Internet of Things. The initial partners from European Telecommunications Standards Institute (ETSI), Supply Chain innovation Centre (Hong Kong, China), YRP Ubiquitous Networking Laboratory (Japan), Electronics and Telecommunication Research Institute (ETRI, Korea), Q.E.D. Systems (USA) and FEIG Electronics GmbH (Germany) working with project leaders AIM UK and the European Centre for Automatic identification and Data Capture (AIDC) were joined at the end of 2008 by China Electronics Standardisation Institution (CESI), a state-run institution responsible for the standardisation and conformity assessment for the IT industry in China. On the other hand, the GRIFS Support Action concerning a Global Interoperability Forum for Standards[30] aims to improve collaboration and thereby maximise the global interoperability of RFID standards. Managed by GS1, ETSI and CEN, GRIFS has initiated a forum that will continue to work constructively after the end of the project through a Memorandum of Understanding between key global standard organisations active in RFID.

A third one concerns the dialogue which the European Commission has extended with industrial stakeholders with a view to assessing further the technological and market challenges and opportunities raised by the Internet of Things. Never before had the European ICT industry been so actively involved in debating the issue of the Internet of Things. To mention just one example, the European Commission and the EPoSS European Technology Platform organised on 11-12 February 2008 in Brussels a joint Expert Workshop entitled "Beyond RFID – the Internet of Things". The conclusions and recommendations of this workshop contributed to draft a report on *Internet of Things in 2020*, which was published in September 2008[31].

At the present stage of the consultations, discussions, and work on research and innovation, the European Commission develops its reflections on a wide range of policy issues, especially the following ones[32]: privacy; security; trust and acceptance; and management of critical resources. These are all very complex issues which need to be approached with a commensurate complexity in the policy measures to be worked out. The

[28] Besides the Coordination and Support Actions mentioned here, several FP7 R&D projects have been started in 2007 and 2008, like for instance the Network of Excellence CONET (http://www.cooperating-objects.eu/).

[29] http://www.rfidglobal.eu/

[30] http://www.grifs-project.eu/

[31] See http://www.smart-systems-integration.org/public/internet-of-things

[32] The list given here is of course not exclusive. For example, the various aspects relating to more flexible spectrum management, the environment (e.g., e-waste, energy harvesting, pollution and disaster avoidance), the potential effects on health from human exposure to Electro Magnetic Fields, and the broad ethical implications of science and new technologies are major concerns that are considered in the discussions about the Internet of Things and addressed effectively in the appropriate forums.

European Commission will adopt in 2009 a Communication on the Internet of Things, largely based on the work of the RFID Expert Group, the results of the public consultation launched during the second half of 2008, and the Telecom Council Conclusions of November 2008. The European Commission will also continue to foster the dialogue among all stakeholders in Europe and in other regions of the world.

Privacy

The very concept of *privacy* will change as the Internet of Things develops. Citizens may decide that the information they consider *private* now – about their health, relationships, and habits – is just too mundane to worry about. Some experts even argue that "*for most people, privacy will end in 2013, or a little beyond that*[33]." They believe that privacy as we know it will become impossible to attain[34]: hard disks will allow people to collect massive information about transactions – who did what; cheap cameras will allow people to collect massive amounts of information about locations – who was where; cheap computer power will allow the sorting and searching of massive amounts of information that is relevant to any one particular person; and cheap computers will allow almost anyone to access what will essentially become the stored life history of anyone. Other experts, interpreting the ideas of the internationally recognised information architect and user experience consultant Adam Greenfield[35], contend that "the silence of the chips" should be preserved as a fundamental right of citizens[36].

So, a "brave new world", a world of confusion, transparency at last, or just old problems recycled? Who can say?

The Internet of Things will inevitably enhance the possibility of information collection about persons and objects. The technologies supporting the Internet of Things will have the potential to facilitate and multiply the exchange and processing of the information in a context where geographical boundaries are blurred. Furthermore, the possibility of automated decisions will most likely create an impression of loss of control either by the *data subject* or the *data controller* (or controllers) who are responsible for the processing of the personal data. Therefore, new information management concepts need to be developed in such a way that they follow the principles which are enshrined in the European Data Protection Directive.

The exercise of data subject rights in the context of intelligent networked environments will require the creation of complex Identity Management systems, based on interoperability, identification, authentication, and authorisation. It is foreseeable that consumer organisations and civil society groups will insist on the provision of comprehensive information and transparency in order to thwart the dismal scenario of "no more privacy by 2013".

[33] Alex Fuss, lead researcher on CSC's Digital Disruptions report, in Financial Times, 3/12/2008.

[34] See, for example, David Brin (1998), *The Transparent Society*, New York: Addison-Wesley.

[35] Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing*, New Riders Publishing, 2006.

[36] For example, Bernard Benhamou, in 2008: "*The reality is that protecting privacy will be key to economic development of this sector. If this weren't the case, the European users would vote with their clicks or would abstain and refuse to enter into an overly intrusive system. The users want to have control, they want to be able to deactivate these devices, with a new generation of chips that give them control. The right to the "silence of the chips" will be key for developing an Internet of the future for all the citizens. We have to evolve to create a system in line with the values of the European continent. This is a prerequisite for this market to develop.*"

## Security

In the world of Information and Communications Technologies, two fundamental aspects of security are distinguished. On one hand, the *reliability* of ICT systems has to be ensured, i.e. neither the systems nor the processed data nor the data processing itself may be endangered in their existence, usage and availability. On the other hand, the ICT systems have to be *controllable*, i.e. the rights or legitimate interests of affected persons may not be endangered by the existence or usage of these systems.

To meet security requirements the following components are necessary:

- Confidentiality – no unauthorised access to data
- Integrity – no unauthorised/unrecognised manipulation of data
- Availability – processing of the system functions at the defined time, within the defined period of time
- Accountability – on every function (and its results) of a system, it must be possible to determine which instance (and/or person) handled its processing
- Liability – on every function (and its results) of a system, it must be legally provable which instance (and/or person) is responsible for it.

While the security issues raised by today's Internet and IT infrastructures are difficult to resolve (spam, Denial-of-Service attacks, identity theft, viruses, etc.), the Internet of Things is likely to generate even more complexity – and debate.

To preserve the confidentiality of data, mechanisms will be required to restrict access to the information stored on objects (e.g., on RFID tags). Further mechanisms will be needed to control whether an object is permitted to participate (i.e. to connect, transmit or receive information) in the Internet of Things, in general or at any given time.

Not all the information transmitted via the Internet of Things is meant to be public. Yet, available infrastructures might be used to transmit confidential information between objects and applications. Therefore, in order to ensure the confidentiality and integrity of that information, mechanisms providing protection against unauthorised access and manipulation of the transmitted data, such as end-to-end encryption and the use of digital signatures, are required for the various components of the Internet of Things. Supported by a comprehensive risk assessment, such mechanisms could be used by the applications according to their specific needs.

The interoperability of the different systems, based on a set of publicly accessible and open standards, will be a key prerequisite to ensure the availability of services on the Internet of Things. Mechanisms for addressing a variety of heterogeneous objects and discovering information on the Internet of Things need to be established and made available without restriction to the public by public authorities.

While the Internet of Things will be characterised by a more or less dynamic perception of the environment, the issues of accountability and legal liability are likely to gain importance. It is already difficult today to determine the responsible parties for certain activities on the Internet; this task will become even more daunting with an uncounted number of micro-systems participating in a highly dynamic, constantly evolving Internet of Things.

### Trust and acceptance

Providing trust for citizens is essential in the introduction of any new technology. However, the Internet of Things is expected to be more ubiquitous in nature and to change people's lives more radically than most existing information technologies. Citizens may rapidly become wary of the consequences the Internet of Things will have for their lives and therefore, they may reject the benefits it could bring to them. On one hand, there is the risk that the feeling of loss of control prevails over the feeling of empowerment by technology. On the other hand, there is still enough time for citizens to get accustomed to the development of the Internet of Things and to learn how to manage their privacy and trust the safety of new applications.

The Internet of Things, characterised by an unspecified and, to some extent, invisible network of objects communicating with each other, is likely to raise new challenges with respect to the transparency and user information that are needed to create trust. Furthermore, flexibility of privacy protection measures will be necessary to empower people to adapt to developing relationships and different environments in a way similar to what they experience in the offline world.

Finally, addressing the digital divide issue will be a prerequisite when the applications of the Internet of Things become more prevalent. All citizens, including elderly people and people with special needs, should in principle be enabled to understand, use and control the Internet of Things environments and to reap its social benefits.

### Awareness and education

Following on what was said before, it must be stressed that many technologies and applications will interact in the Internet of Things. Consequently, the level of complexity will be much higher than the one which citizens are used to today, and every transaction might produce a complex chain reaction – citizens, but also businesses, hardly trust what they cannot control or cannot understand.

Awareness and education are therefore critical to the eventual success of the Internet of Things. Without proper information, there will be no trust and no acceptance, and consequently the incentives to move towards the Internet of Things may vanish. In order to establish lasting confidence in the Internet of Things, awareness and education efforts should focus on its benefits but also on the policies and strategies followed to identify and mitigate its potential risks.

When time is ripe, i.e. at the dawn of the deployment of the Internet of Things, impartial and comprehensive information campaigns on what the Internet of Things is, what its main features are, what benefits it may bring, what the implications are, especially in terms of privacy and security, will be needed. It will also be essential that the education and awareness material be tailored to the segment of the population it is aimed at.

### Management of critical resources

In 2005, the European Commission initiated discussions with international experts to address the issues relating to the global naming and routing control architectures which are currently in place for RFID applications. For lack of anything better, the issue was defined as "the governance of the Internet of Things", a choice which proved not so judicious, although popular, since it caused confusion with the broader institutional debate over Internet Governance. Nevertheless, the debate initially restricted to a tiny guild of international experts, especially from academia and EPCglobal[37], gradually attracted interest and gained visibility among the wider RFID and Future Internet communities.

Following these initial discussions, concerns have been expressed in Europe that a fully centralised critical resource control may not be appropriate and that some form of resource control at national or regional level should rather be the rule. Another concern is that reliance on a single service provider, possibly placed under non-European jurisdiction, may not be compatible with business continuity needs, especially considering that resource centralisation is likely to generate single point failure. The following statement made in 2005 by Bernard Benhamou, now from the French Inter-ministerial Delegation on Internet Usage, reflects these concerns[38]:

*"The upcoming development of new Internet services based on the use Geographical Information Systems and their connections with mobile devices and RFID tags will make the Unique Identifiers even more crucial for the development of the Internet economy. The main difference between those new systems and the existing DNS is that they will not only control the information flow but also allow the monitoring of the merchandises and the persons' movements wearing these RFID tags. The public policy implications of these new Unique Identifiers will then become even more sensitive. The architecture of the new Unique Identifiers that will be deployed on the Internet will have to be analysed in terms of usability and value creation on the Internet but also in terms of security, stability and sovereignty regarding the management of key Internet resources. In order to ensure the development of the Internet, the collaboration between the States will soon become a necessity in all the technical segments (or all the layers) of the networks."*

A consultation involving Member States, national data protection authorities and the private sector might need to be planned in order to define the minimum level of visibility and control of critical resources that should be provided to national authorities for safeguarding public policy interests. These include security needs (i.e. how far the retained architectures are compatible with the objective of oversight by public authorities over the tracking and tracing of potentially dangerous goods such as foods and pharmaceuticals), economic interests (i.e. how far the retained architectures are compatible with business transaction confidentiality), competition rules (i.e. how far the retained architectures prevent other architectures to emerge), and protection of personal data and privacy (i.e. how far the retained architectures are compatible with user data confidentiality and access restricted to the right party only).

The debate on the governance of the Internet of Things gets rather technical. It derives essentially from the deep and widely-shared concern within world countries that, letting aside a few specific initiatives such as UCCnet, which aim at sharing and synchronising global trade information across retailer, distributor, and supplier organisations, the control

[37] EPCglobal is leading the development of industry-driven standards for the Electronic Product Code (EPC) to support the use of Radio Frequency Identification (RFID) in today's trading networks (http://www.epcglobalinc.org/home/).

[38] Source: *Radio Frequency Identification (RFID) Applications and Public Policy Considerations*, OECD Foresight Forum, Paris, 5 Oct 2005.

of look up and discovery services today is global and centralised, without delegation to national or regional levels[39].

To understand what's at stake in the debate on the governance of the Internet of Things, it is necessary to become familiar with the following key acronyms and concepts. These are used today in the RFID world but the approaches they describe have the potential to be used in the Internet of Things world as well.

- Object Naming Service (ONS) is a network service that leverages Domain Name System (DNS) to discover information about a product and related services from the Electronic Product Code (EPC). The most common example is where ONS is used to discover an EPCIS service that contains product data from a manufacturer for a given EPC. ONS may also be used to discover an EPCIS service that has master data pertaining to a particular EPCIS location identifier.

- EPC Information Services (EPCIS) aims to enable disparate applications to leverage Electronic Product Code (EPC) data via EPC-related data sharing, both within and across enterprises.

- Discovery Services offer to authenticated and authorised users the means to discover sources of information for a particular object. Discovery Services can be implemented as a decentralised directory of resources indexed by a shared identifier. Discovery Services need to be deployable in both closed networks as well as open and global networks such as Internet.

- EPCIS Discovery Service (EPCIS DS) refers to a mechanism for locating all EPCIS-enabled repositories that might have data about a particular EPC. This is useful when the relevant EPCIS services might not otherwise be known to the party who wishes to query them, such as when the handling history of an object is desired but not known (e.g. in support of track-and-trace across a multi-party supply chain). The volumes of serial-level records generated by the supply chains would place an unreasonable burden on the DNS roots if ONS were used as EPCIS DS for holding ONS records for each serial number.

- Extensible Supply Chain Discovery Service (ESDS) is an application layer protocol for the distributed sharing and discovery of notification events between associated partners within a supply chain. In other words, it has been chartered to architect

[39] This refers to the point that in 2004 U.S. Internet and telecommunications infrastructure services provider VeriSign was awarded by EPCglobal a contract to manage the directory for looking up EPC numbers on the Internet. Under the EPC Network system, each company has a server running its own Object Name Service (ONS). Like DNS, which points Web browsers to the server where they can download the Web site for any particular Web address, ONS points computers looking up EPC numbers to information stored on something called EPC Information Services (EPCIS), i.e. servers that store information about products. Companies may maintain their own EPCIS or subcontract it out, but it uses a distributed architecture, with information about products in more than one secure database on the Web. Under the deal with EPCglobal, VeriSign manages the EPC Network's root directory – the system that points computers to each company's ONS. Computers access the registry via the Internet, and if one registry goes down temporarily, a computer requesting information about an EPC number is automatically directed to another registry site, guaranteeing 100 percent up time.

and define a protocol for Discovery Services. To avoid traffic flat and walking up the Internet root hierarchy, ESDS might use peer-to-peer look up protocols as an alternative to hierarchical look up protocols such as DNS and ONS. Unlike DNS or ONS, where there is a known set of root servers, ESDS will have numerous roots for various supply chains operating globally.

The year 2008 injected a new momentum into the debate, thanks in particular to the special session on *Architectures and governance of the Internet of Things*, organised by the French Presidency of the European Union at the Nice conference[40], the public consultation launched by the European Commission on the basis of a Commission Staff Working Paper[41], and the involvement of key organisations such as the Internet Engineering Task Force (IETF)[42] and Afilias[43].

Afilias, for instance, released at the Nice conference a white paper that details a decentralised and interoperable model for implementation of Object Naming Services (ONS) and supporting Discovery Services. Brian Cute, Vice President of Discovery Services at Afilias, set the issue very clearly by saying: "*Questions are currently being asked as to whether an Internet of Things architecture can be implemented without a unique, single point of control, or ONS, at the root level. Afilias believes that a decentralised, interoperable ONS architecture, combined with Discovery Services, is the ultimate model that will provide success for the evolution of the Internet of Things.*"[44]

In April 2008, GS1 moved forward in that direction by offering an ONS operational platform: the use of the ONS Root is proposed to all the companies which have subscribed to EPCglobal, particularly in Europe. In France, Orange Business Services was selected for the nationwide implementation of the ONS Root of the EPCglobal network architecture.

The debate on the governance of the Internet of Things currently turns towards the following main points of discussion:

1. Many stakeholders believe that items should be labelled with globally unique identifiers. However, maintaining any particular identifier as globally unique, when there are multiple identifier authorities, would imply a significant and sustained effort of global cooperation.
2. Identifier Authorities want to continue to manage their unique identifier schemes and yet leverage the next generation of information exchange. These authorities need a path to participate in the Internet of Things while continuing to support existing identifier sets without a next generation third-party identity authority being required to enable them.

[40] See http://www.internet2008.fr/spip.php?article9

[41] See http://ec.europa.eu/information_society/eeurope/i2010/docs/future_internet/swp_internet_things.pdf

[42] The Internet Engineering Task Force (EITF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. See http://www.ietf.org/

[43] Afilias is the largest provider of outsourced global domain name registry services supporting over 14 million domains across 15 top level domains. See http://www.afilias.info/

[44] See http://www.afilias.info/news/2008/10/06/afilias-releases-proposal-internet-things-architecture-advance-eu-meeting

3. National and Regional authorities want to ensure that entire control of the Internet of Things will not lie exclusively within the power of a specific – public or private - authority. They want to ensure accountability with respect to local law and policy in any solution for information exchange.
4. All stakeholders want to be assured that any approach to the governance of the Internet of Things is practical, scalable and allows for open competition in providing the information services.
5. The future Internet of Things architecture should be developed in such a way that it provides for security, protects privacy, and has a trust model at its centre[45].

## Conclusions

Our initial goal was to "unpack" the idea of Internet of Things and propose a rationale for its integration into a policy framework. Our central arguments have been that the development of the Internet of Things, based on the synergistic combination of several scientific disciplines and technologies, creates tremendous opportunities for improving economic competitiveness and citizens' quality of life, but also raises complex non-technical issues, especially with respect to ethics, privacy, security, governance, spectrum, interoperability, and more, which deserve to catch the highest attention from public authorities, preferably within the context of a sustained and well focused international dialogue.

In offering both a framework and a vocabulary for talking about the Internet of Things, our goal is to foster discussion between all stakeholders and to encourage a nuanced understanding of the impacts of technology on society and policy-making. The Internet of Things will continue to be a significant issue in the global public debate; our understanding of what Internet of Things is and what its implications are for the economy and society will need be as sophisticated as the many technologies involved. We hope this is a useful initial step.

### Acknowledgements

This work owes a lot to the work of the RFID Expert Group which the European Commission set up in June 2007 and to the discussions I had in 2008 with several of the people who played a role in the organisation and implementation of the "Internet of Things – Internet of the Future" Conference in Nice, France. I am particularly grateful to Bernard Benhamou, Brian Cute, Patrick Guillemin, Ryo Imura, Marisa Jimenez, and Sarah Spiekermann, for their inspiration and creativity, and to Manuel Mateo, Project Officer in my unit, for sharing his time and ideas.

***Disclaimer: The opinions reported in this paper are purely the author's and do not necessarily represent the views of the European Commission. Any mistakes are the sole responsibility of the author.***

[45] See, for example, Benjamin Fabian, Oliver Günther and Sarah Spiekermann, *Security Analysis of the Object Name Service*, http://lasecwww.epfl.ch/~gavoine/download/papers/FabianGS-2005-sptpuc.pdf