Policy and Technological Drivers in the Internet of Things

Internet of Things 2008 Conference, Zurich, Switzerland

27 March 2008

Gérald Santucci

"Our world, and our lives, are being shaped by the conflicting trends of globalisation and identity. The information technology revolution, and the restructuring of capitalism, have induced a new form of society, the network society. It is characterised by the globalisation of strategically decisive economic activities. By the networking form of organisation... By a culture of real virtuality constructed by a pervasive, interconnected, and diversified media system. And by the transformation of material foundations of life, space and time, as expressions of dominant activities and controlling elites... It is indeed, brave or not, a new world."

Manuel Castells, The Power of Identity

Ladies and Gentlemen,

Some years ago, Kevin Ashton, co-founder of the Auto-ID Center at MIT and, as far as I know, the person who coined the phrase 'Internet of Things', said that "*RFID is kind of the amoeba of the wireless computing world.*" If we accept Karl Popper's view that the evolution of knowledge is continuous with biological evolution, that from the amoeba to Einstein, the growth of objective knowledge is always the same – trying to solve our problems and to obtain, by a process of elimination, something approaching adequacy in our tentative solution – then we just need to hope that the process which should lead from RFID to the Internet of Things won't take over 4 million years of evolution!

This International Conference for Industry and Academia "Internet of Things 2008" will certainly take care of this as it is an important milestone in the extensive international dialogue which is needed to provide guidance into how countries in the world should address the policy challenges and opportunities of the Internet of Things.

The European Commission started to pay attention to the Internet of Things in the context of its initiatives concerning Radio Frequency Identification (RFID). 2008 is the

year when the Commission will publish a Recommendation to the EU Member States on the implementation of privacy, data protection and information security principles in applications supported by RFID. A RFID Expert Group has been established in June 2007 to assist the Commission in this work. This group, which is expected to remain operational until March 2009, consists of some 30 representatives of the various categories of stakeholders who are involved in the debate on RFID in Europe. The draft Recommendation was completed a few weeks ago and is currently published online to probe and understand the reactions of the interested parties.

But 2008 is also the year when the Commission examines the issues, challenges and opportunities of the Internet of Things in a public policy perspective. This initiative was announced in the Communication on "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework", which the Commission adopted on 15 March 2007. In the wake of this Communication, the German and Portuguese Presidencies of the EU organised major conferences to debate the shift from RFID to the Internet of Things.

On the occasion of the Berlin Conference on 25-26 June 2007, the German Federal Ministry of Economics and Technology published a European Policy Outlook RFID document which acknowledged that the technical vision of the Internet of Things had begun to move into the realm of the possible. And the Lisbon Conference of 15-16 November 2007, building on the conclusions of the previous conference, heralded the importance for Europe and the re-launch of its Lisbon strategy of developing the technologies that are deemed to play a key role in the emergence of the Internet of Things.

Therefore, I am pleased that this International Conference in Zurich also takes place in Europe. For the European Commission, it is a confirmation that its ongoing action regarding the Internet of Things is both relevant and timely. It is also a moment when the existing visions of the Internet of Things can be confronted and enriched in the light of first hand accounts of the current developments, preliminary achievements, and stakeholders' expectations as delivered by distinguished experts from all over the world.

The Future Internet Challenges

The Internet architecture is facing today several challenges, many of them being related to scalability issues linked to the ever growing number of users, devices, service attributes, applications, contexts, and environments. Still, existing architectures are based on a number of features that have proved to be valuable from an economic and policy perspective:

- *The distributed architecture of the Internet*, opposed to earlier star topologies such as those of public telephony networks or data networks, has opened the possibility to a virtually unlimited number of actors to contribute as users and service developers, hence boosting innovation and economic growth.

- *The end to end characteristics of the architecture* has enabled to place intelligence at the periphery of the network, with the subsequent capability of making the Internet a neutral platform enabling any user to offer new content and new services, thereby opening the way towards collaborative usages.

- *The open architecture of the Internet*, based on standardised technologies, has facilitated large scale interoperability and early globalisation of services and applications. This is what made possible the Internet to become an “open innovation platform”.

- *The "neutral" access* characteristics have enabled various networking platforms and providers to offer competing access paths to the Internet, and contributed to the "infrastructure competition" objective that has been recognised by regulators as an important tool to catalyse the deployment of modern networks.

- *The clear layering* from a network, service and content perspective has enabled competition and innovation to flourish at different levels of the value chain whilst at the same time opening new opportunities for innovative business models.

- Even if security and resilience aspects have been questioned, today's Internet architecture has demonstrated a good level of *resilience to physical network disruption*.

The European Union has outlined its adherence to the openness, interoperability and end-to-end principles governing the Internet of today, notably on the occasion of the last World Summit on the Information Society. From an EU perspective, it is essential that any further redesign of the architecture of global networks will have to respect these basic principles and characteristics – the adherence to the latter is clearly an area for international co-operation at both technological (saying what is *possible*) and policy (saying the *requirements*) levels.

However, it can be observed that many forces and interests are at work to modify the Internet architecture in a way that may not be fully compatible with these principles:

- *Firstly, from an economic perspective*, the move towards Next Generation Networking can be interpreted as an attempt to reinstate some form of centralised control within an inherently distributed architecture. The risk is not negligible that gatekeeper or lock-in situations may develop, the net neutrality debate being one particular illustration of the problem at hand.

- *Secondly, from a technological perspective*, approaches such as those discussed within the "Autonomic Communication" context may bring in additional complexity within the network that could potentially damage the end to end characteristics of today's architectures.

- *Thirdly, from a political perspective*, as the Internet is increasingly becoming a "critical infrastructure", security and robustness of the Internet are naturally becoming issues of major concern. These concerns may find their solutions in closed forms of Internet connectivity through the emergence of secure islands or of restricted connectivity, hence breaking the openness characteristics of the Internet.

Meanwhile, from a user perspective, people in the Internet of Things era will be engaged in new roles, acquire an array of competencies enabling them to create social

networks, and interact with one another in virtual worlds with avatars enjoying their "second life".

The European Commission has systematically called for the Internet to remain a vector of freedom of expression, to contribute to economic development policies, and to support multilingualism. These issues, when applied to future Internet architectures, can only be addressed in a multi lateral perspective combining at the same time the technological and the policy/regulatory perspectives. The approach of systematically combining network technological development with policy issues has been and will continue to be systematically pursued by the RTD programmes sponsored by the European Union. In particular, we expect major contributions of Internet to development policies, to education, to culture, to health and to e-government. These issues are at the heart of Europe's contribution to the upcoming final declaration of the OECD member countries in the context of the Seoul Ministerial Meeting of next June on the Future of the Internet Economy. The European Union has much to offer on these issues, as they have been at the heart of concrete actions implemented under the i2010 policy initiative.

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.

The Emerging Visions for the Future Internet

There are at least four ways to look beyond the current Internet:

- The first way is to increase the performance of the infrastructure supporting the Internet.
- The second way is to improve the services offered through the Internet.
- The third way is to exploit the potential of Internet-enabled Virtual Economies for achieving something that humans have apparently been trying to do since the dawn of civilisation – I mean gaming or living a fantasy existence.

- The fourth way is to integrate more effectively the world of the Internet with the physical world outside the Internet.

The future starts today. You are all aware of the ambitious initiatives launched in different countries – let me mention simply the NSF's 'Global Environment for Network Innovations' research program and facility (GENI) and the 'Future Internet Design' long-term initiative (FIND) in the US, the AKARI Architecture Design Project in Japan, the 'Future Internet Forum' in Korea, and the EU's ICT projects carried out under the 7th Framework Programme.

In this context, I will purposefully discard the first way mentioned above – the evolutionary research approach – and focus my presentation on what researchers have called the "clean-slate paradigm", that is the paradigm which aims to address the fundamental problems and limitations of the Internet, without being constrained by the architecture or protocols currently used. Indeed, we should be aware that the current Internet architecture shows significant shortcomings, does not have the hooks to support the flexible business models that will be required to reward investment in the infrastructure, and cannot integrate horizontal services enabling virtualised connectivity. Therefore, adopting here a long term perspective, I would like to describe the Internet of Services, the Internet of 3D Worlds and, of course, the Internet of Things as three major use cases of the Future Internet that are emerging and that will drive the requirements for its network and service infrastructure. Some of the developments regarding these use cases can take place within existing architectures and business structures as exemplified by Service Delivery Platforms, gaming, and sensor networks, respectively. But their ultimate realisation will require architectural revolution and result in business disruptions. This is why I want to focus my presentation on them.

It is imperative to understand how clean-slate architectural research compares to diametrically opposite paradigm of evolutionary research. In my opinion, both approaches are probably needed and therefore we should for the time being encourage and support the diversity of ideas and innovations. We cannot predict the future, and even less summon philosopher Thomas Hobbes and his Leviathan or physicist James Clerk Maxwell and his "Sorting Demon" to impose any preferred scenario. We should

rather invest in the creation of multiple competing solutions and eventually select the fittest innovation given the constraints and requirements at a given time.

The three emerging use cases of the Future Internet, which I have chosen to highlight in my presentation, are equally important, very promising, rich of economic potential and of benefit for the society, very challenging also in many policy respect, and – above all – not mutually exclusive. I believe that they will eventually converge into the single global vision of an ever larger share of the economic and social activities moving on line, with a need to make the Internet capable of supporting an ever larger number of usages whilst remedying to its current deficiencies in terms of security, trust, scalability, mobility, etc. So, these emerging use cases should all be elaborated and tested while researchers, companies and government decision-makers contemplate the Future Internet.

More practically, considering the current EU research effort let me stress that over 200 million Euro have been invested in some 70 Future Internet related projects derived from the first two calls for proposals. Europe is eager to take an important, constructive and valuable part in the debate and activities around the Future Internet. In a few days, the conference on the Future of the Internet, taking place in Bled, Slovenia, will discuss the perspectives emerging from R&D in Europe. A European Future Internet Portal and a Bled Declaration will demonstrate the commitment of European stakeholders to co-ordinate their efforts and strategies in this field.

An Internet of Services

The first emerging use case can be called the "Internet of Services".

In an "Internet of Services," all people, machines, and goods will have access to the Internet by leveraging the network infrastructure of tomorrow. The Internet will offer services for all areas of life and business, such as virtual insurance, online banking and music, and so on. A complex services infrastructure, including Service Delivery Platforms bringing together demand and supply, will be required for those services.

The establishment of an open architecture that comprises possibilities for human beings to use and interact with Web-based resources has the potential to drive the development

of a global mesh of services. Arbitrary stakeholders can provide and host services, thereby leading to a global market with decentrally organised platforms that act as brokers. The actual users can access these platforms for discovery purposes via intuitive interfaces that facilitate tagging and mashing activities without requiring any coding effort. All of the different channels (such as mobiles, PDAs and IPTV) can then be leveraged to enter and use the platforms.

To realise this vision, an open platform for tradable, composable, value-added services on the internet is required. Such a platform will need to build upon and extend:

- Web 2.0 concepts to allow for community-driven service innovation and engineering on a large scale
- Global repositories for value-added services, and
- Semantic support to enable automatic composition of value-added services.

This will enhance reusability of services, and allow for reasoning to derive further knowledge. Legal, security, logistics, business, and technical aspects must be simultaneously addressed for an integrated approach to the Internet of Services, where the service consumer will get customised services within Business Webs.

So, a combination of principles from both Web 2.0 (user self-service and collective end-user intelligence) and SOA (a composition of reusable building blocks) can facilitate the wide dissemination of many resources. For instance, business users would be empowered to model and deploy business models in an extremely quick and efficient fashion. The interconnection of presentation-layer-focused Web applications to internal SOA implementations could be of significant value for enterprises, as this could extend their services' reach to the Web for further use and composition by their business partners and customers.

An Internet of 3D Worlds and Virtual Worlds

The second emerging use case can be called the "Internet of 3D Worlds".

Social communities of online gamers like *Second Life* or *There.com* can be seen as the forerunners of new business models on Internet. From the technology viewpoint, these communities also form a unique laboratory for the experimentation of new interfaces on Internet.

At first glance this topic may look of minor importance, but with more than ten million active players worldwide – and with Microsoft and Sony pouring hundreds of millions of dollars into video game development – online games have become too big to ignore. *Second Life* and so-called "massive multiplayer online role-playing games" (MMORG) such as *World of Warcraft* or *EverQuest* represent a new 3D environment for socialisation and creation of new service activities on Internet. Edward Castronova, Associate Professor of Telecommunications at Indiana University Bloomington, has shown that the technology supporting virtual worlds – or 'Synthetic Worlds' as he calls them – is advancing so quickly that it would be foolish to describe the next generation in any detail. But anyhow this technology places requirements on the Internet infrastructure. *Second Life* is a typical example, but more complex applications are expected to emerge, which will open new classes of issues. Increased technological capabilities are probably needed, whilst issues such as interaction between virtual and real world, interoperability across multiple virtual environments, multiple identities or standards are still open. In addition, such environments are expected to put additional requirements on search-and-find technologies which will have to cope not only with text based information, but also with unstructured and structured multimedia representation of objects, with or without semantics built in.

An Internet of Things

Now comes the third emerging use case – the one which looks to me the most important and the most challenging, and also the one that is the topic of this conference: the "Internet of Things".

The Internet of Things is a new paradigm in which real world objects have an individual digital presence. Objects are uniquely identified and described in a standardised way which facilitates access and interaction with them. It heralds the vision of a future world

where each item or thing is networked, and can communicate information about itself or from itself to other objects and to computer systems.

Assuming that IPv6 will be used as a global addressing scheme, then if any objects will have a unified address we will have an addressable continuum of computers, sensors, actuators, telephones and 'things'.

Combining information from an infinite amount of sources creates true *Ambient Intelligence* – to use the neologism coined by the IST Programme Advisory Group (ISTAG) for its vision statement of seamless delivery of services and applications, drawn up in 1999 for the 5th Framework Programme.

As Dr Mikhail Simonov, a Senior Researcher at ISMB in Turin, Italy, told me recently during a workshop in Brussels, we are now aware that a new dimension has been added to the ICT world: from anytime, anywhere connectivity for anyone, to anything, for instance between PCs, Human to Human, Human to Thing, and Thing to Thing. Indeed, multiple connections creates an Internet of Things which is based on solid technological advances and visions of network ubiquity, computing, communications, and dynamic technical innovation in a number of domains, ranging from wireless sensors to nanotechnology. No doubt we will continue to use the PC in order to interact with the Internet of Things, but many more options will exist, in particular those offered by the combined use of the knowledge and cognitive technologies, and those enabling the transition from RFID to networked RFIDs and the Internet of Things.

Imagine an Internet of things, where everyday objects, rooms, and machines are connected to one another and to the larger digital world. Sensors on expensive factory equipment would tell you when the machinery is about to fail. Cargo shipping containers could search their contents for nuclear material or other hazards. Every office could report its temperature and humidity and whether its lights are on or off, and each foot of a country's streets and highways could monitor traffic flow.

Is it fiction or a technological probability? I would like here to quote Aristotle: "*A likely impossibility is always preferable to an unconvincing possibility*." But rhetoric now set aside, let's consider a factual development. A project funded by the National Science

Foundation, Microsoft Research and the University of Washington has started this year to explore the use of RFID tags in a social environment. Volunteer students, engineers and staff wear electronic tags on their clothing and belongings that sense their location every five seconds. The information is transmitted to a database, published to Web pages and used in various custom tools. This is undoubtedly a precursor of the future Internet of Things.

Some months ago, Professor Michael ten Hompel, Director of the Fraunhofer Institute for Material Flow and Logistics in Dortmund (IML), said that he anticipated the initial rollout of the first phase of major applications of the Internet of Things in 2010. By 2015, he added, we should see completely new applications where things communicate autonomously amongst themselves. What will make this possible is the link of sensor networks – to measure pressure, light, humidity, etc. – with RFID systems.

But the Internet of Things is more than an era of RFID tags and networked sensors. As Julian Bleecker, Assistant Professor at University of Southern California, has shown, once 'things' are connected to the Internet, they become "first-class citizens" with which we will interact and communicate. He uses the neologism "Blogject" – 'objects that blog' – to point to the active role of 'things' in the blogosphere – the sphere of networked social discourse. The most peculiar feature of Blogjects, he says, is that they participate in the exchange of ideas – they circulate conversations as they track and trace where they are and where they have been, they have self-contained histories of their encounters and experiences, and they can foment action and experiences. Bleecker cleverly illustrates these characteristics of 'traces', 'history' and 'agency' by using the metaphor of the "pigeon that blogs" – actually a flock of pigeons that wear some wireless equipment to communicate on the Internet, a GPS device for tracing where it has been flying, and a sensor that records the levels of toxins and pollutants in the air through which they fly.

Perhaps the phrase 'Internet of Things' needs to be clarified – I trust this conference will be seen as a key milestone towards this clarification. We must now move beyond vague concepts that have many owners but little identity. The contrast between the broad rhetoric of those who speak of the Internet of Things and the narrow agenda that exists

to put Europe on track for the Future Internet is stark. Yet we are right to treat the Internet of Things as a serious idea rather than a shallow slogan.

This said, the European Commission will review this year the issues, challenges and opportunities in relation to the emerging Internet of Things. For this purpose, the RFID Expert Group that assists the Commission in this task has set up four working groups to address the following key aspects – Technologies, Applications, Standards, and Privacy and Security.

Other related activities supplement and support this initiative.

Firstly, work underway within the IST Advisory Group (ISTAG) on Future Internet Infrastructure suggests that to turn the Internet of Things into reality technical research challenges have to be addressed at multiple layers of the entire technological framework and infrastructure. More specifically, further research and development must concentrate on the following topics:

1. *Edge technologies*, such as sensors and actuators, passive and active identification tags, or embedded systems that are attached to real-world objects and make objects 'smart' enough to participate in novel Internet of Things application scenarios.

2. *Networking technologies*, such as fixed, mobile, wired and wireless networks allowing the highly available bi-directional communication on different levels – between real-world objects, applications and services that offer specific functionality.

3. *Middleware systems* that must be scalable, secure and semantically rich in order to put real-world data into the context of various Internet of Things applications. As the Internet of Things implies that enormous numbers of data sources need to be connected and related to each other, flexible and dynamic middleware support is a key requirement to cope with the sheer scale of this task and the heterogeneity of available devices, sensor networks and other technologies.

4. *Platform services* that run in the background have to support a superior management of all involved technical components – trillions of loosely coupled devices! – in an integrated way ensuring scalability, high availability, and the safe and secure execution of the requested functionalities.

5. *Web service technologies* must be used to provide a new way of making information and services available while reducing interoperability issues and enhancing extensibility, platform independence and standardised exchange of messages. The interaction between mobile devices and physical objects in the real world could provide a natural and intuitive way to request Semantic Web services associated with real-world objects.

Secondly, the Cluster of European RFID Projects (CERP - http://www.rfid-in-action.eu/cerp), which was launched in January 2007 and consists today of 17 research projects, has recently submitted, in the context of the Lisbon Conference of last November, a detailed Working Paper on future RFID Research Needs. The paper addresses the following RFID application fields: Logistical tracking & tracing; Production, monitoring & maintenance; Product safety, quality & information; and Payment applications/e-cash. Although it focuses on RFID technology, the applications covered are also likely powerful applications for the Internet of Things era. Gerd Wolfram from Metro kindly accepted to co-ordinate the Cluster during its first year of operation – a task which he fulfilled with outstanding abilities and success. During the fifth meeting of the Cluster on 13 February 2008, a new co-ordinator – Patrick Guillemin from ETSI – was appointed.

Thirdly, two projects derived from the first call of the ICT theme in the 7th Framework Programme have just started to analyse some of the major requirements and options in the development of the Internet of Things. On one hand, the CASAGRAS Co-ordination and Support Action (http://www.rfidglobal.eu/) consists of a group of international partners representing Europe, the United States, China, Japan and Korea who are looking at global standards, regulatory and other issues concerning RFID and its role in realising an "Internet of Things." On the other hand, the two-year GRIFS Support Action (http://www.grifs-project.eu/) aims to improve collaboration and

thereby maximise the global interoperability of RFID standards. This project will initiate 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. CASAGRAS and GRIFS will co-ordinate their activities as regards the establishment and maintenance of their respective forums.

Fourthly, following a joint European Commission / EPoSS Expert Workshop "Beyond RFID – the Internet of Things", held in Brussels on 11-12 February 2008, a "Framework Paper" describing future trends and roadmaps towards the Internet of Things will be soon published on the EUROPA and EPoSS websites to serve as a basis for the next ICT in FP7 calls for proposals and contribute to the EPoSS European Technology Platform's strategic research agenda.

Lastly, I would like to highlight the fact that the future French Presidency of the EU will organise in Nice on 6-7 October 2008 an international conference on "Internet of the Future – Internet of Things". This event will give an opportunity to debate the key policy issues surrounding the development of the Internet of Things in the context of the international work on the Internet of the Future. Technology, applications, governance of resources, standards and interoperability, radio spectrum, trust, security, privacy and data protection, and many other relevant topics will be discussed by and amongst international experts from Europe, America and Asia.

The Underlying Network and Service Infrastructure

The societal pulls for Internet changes, which I have outlined earlier, will be mirrored by technology push, as technologies become mature enough to open prospects for novel and cost efficient on line applications.

On the communication side, the ever growing demand for broadband and mobility is expected to place significant constraints on Internet architecture. Internet was originally not designed with the idea that more than 100 Mb/s would be one day available to end users and mobility was simply ignored in the original architectures. We are now rapidly moving towards 4 billion mobile users worldwide, with a significant part of them willing to access the Internet on the move. Attempts to further patch the Internet's

original architecture in order to support mobility or wider bandwidth have been disappointing – such an approach is probably not satisfactory in the long term.

The use cases which I have sketched out tend to define some of the features of the network and service infrastructure in the Future Internet. This infrastructure is expected to provide connectivity services, computing resources as services, information and knowledge services, business, government and societal services, and sense and action on the real world. These will need to be provided in an intelligent manner, personalised to the needs and context of the user and at the desired quality level. Furthermore, the infrastructure must support dynamic business relationships and value chains with a rich set of horizontal enabling services, such as identity, trust, location, or brokering, supporting the vertical services.

Security, Privacy and Trust in the Internet of Things

The actual realisation of the Future Internet will critically depend on its ability to cope with security and privacy challenges, in particular regarding how to deal with generalised mobility and scalability in the number of users, devices and services, and how to reliably deliver ever more time-critical and high-bandwidth applications.

In the Future Internet trust will be critical. The first question will be: "Can we trust the people we meet?" Trust must be understood in its multiple facets and manifestations – trust between people, between people and the cyber-infrastructure, amongst people using the cyber-infrastructure, in a society of human and software entities, and finally in more complex value networks and ecosystem settings. The second question will be: "Can we trust the data or the knowledge?" Trusting data or knowledge points to the engineering of trust management, access control and policy systems. These should be flexible enough to understand and accommodate the dynamic nature of trust. They should integrate seamlessly with existing and future security systems, for instance detection of fraud, intrusion attacks, other malicious behaviours, trust and risk assessments, and relationship and access control policies. Moreover, considering the huge number of data and knowledge circulating in the Future Internet, certifying the provenance of data or knowledge will definitely become a critical issue for security and source check reasons.

The term “Future Internet” encompasses, in fact, the emergence of future large heterogeneous and interconnected networked ICT infrastructures, as for example the evolution of the current Internet, the Internet of Things, and future wireless and mobile systems and sensor networks (post-IP, post-3G). It also encompasses the emergence of millions of different networked virtual constructs and entities such as virtual private or overlay networks, dynamic service software coalitions and interconnects, semantic P2P grids, and “virtual worlds” based on highly-distributed, virtualised communication, computing and storage resources.

From the viewpoint of security, privacy and trust in the Internet of Things, it is clear that we are today confronted with unprecedented research challenges.

New conceptual frameworks, technologies and tools are needed for:

- Managing and protecting the 'identity' of billions of networked persons, devices, 'things', services and virtual entities connected to the Future Internet;
- Securing the interactions and interfaces between heterogeneous ICT systems and engineering scalable security policies across the Future Internet;
- Securing critical infrastructures that are interdependent and controlled through vulnerable networks;
- Designing scalable, dependable and resilient open systems and composite services;
- Predicting, monitoring and managing dependable behaviour, evolution and adaptation to changing contexts, operating conditions, regulations or practices of use, while guaranteeing service level provision or best trade-off between conflicting factors based on business oriented risk analysis;
- Security of highly distributed virtual entities and trusted infrastructures based on virtualised communication, computing and storage resources;
- New crypto schemes both in the core networks and at network edges.

Security is a big concern in our 'hyper-connected' society, but who's responsible and accountable for a security breach? Is it the consumer who inadvertently downloaded a virus? Is it the device manufacturer who didn't design security software correctly from the start? Or, is it the fault of the service provider or carrier whose network the data moved across?

Unfortunately, when it comes to security, the industry has not outlined a proven best practices approach. Typically, security design decisions are made on an ad-hoc basis and different approaches are used for different products.

Device manufacturers have the most responsibility and control when it comes to device security and perhaps, the most at risk. The problem is that many device manufacturers have an incomplete security approach or refuse to acknowledge that it is their issue to address at all. Designing and budgeting for security while in the product design cycle is viewed as inconvenient by manufacturers. However, this stance is short-sighted when the cost of supporting a device over its useful life is taken into consideration. The irreparable damage to customer confidence and brand equity caused by devices that are compromised is unquantifiable. Additionally, even the most trivial security breach through incomplete device defences can impact shareholder value for device manufacturers.

A device manufacturers' approach to security affects service providers and enterprises as well. Service providers consistently strive to deliver a first-class consumer experience and the potential for compromised devices connecting to their networks poses great risk to their business. Service providers and carriers want to be able to offer enhanced, revenue generating services that enable people to transact, and consume valuable content and data online. If there's a loss of confidence or trust in the device's ability to leverage those services, people will simply stop transacting. For enterprises, improperly secured devices pose significant risk to network data security, with huge negative implications for customers, partners, and ultimately future sales.

To address the device security challenge and maximise the potential of the Internet of Things everyone – device manufacturers, service providers and enterprises – must therefore assume security responsibility and recognise the need to centralise and

standardise how device security is dealt with on all devices, wired and wireless. We must take a more holistic security approach and apply an extensible framework that secures all aspects of device data access and communications for any connected device. Securing devices is an industry imperative – doing it the right way will pay for itself in multiples in our increasingly connected world.

Governance of the Internet of Things

The Internet of Things is expected to generate significant policy issues in addition to those we are already confronted with for the current Internet. As the Internet of Things is still in its infancy, the opportunity exists to take pre-emptive steps to avoid, as far as possible, the problems raised presently by the Domain Name System (DNS).

To state the issue simply, let me stress the fact that for the uniqueness of the object identifier the creation of a centralised database, known as the 'root server', may seem to be a prerequisite. But over the past two years the Information Society and Media Directorate-General of the European Commission has relentlessly argued that alternative architectures could be envisioned where instead of a centralised and single root several interoperable roots could co-exist. This approach has gained visibility and momentum last year when, on 13 December, GS1 France chose Orange Business Services to lay the foundations of the first regional root of the Object Naming Service (ONS). Moreover, Bernard Benhamou, in charge of Internet usages at the French Ministry of Higher Education and Research, announced recently that during the second half of 2008 France will seek to share the governance of the ONS root with its EU partners – "*With the creation of the French ONS root, we open the way for an active cooperation with all our European partners in order to make that this ONS root eventually becomes the European base of the Internet of Things."* In other words, the French root would become the European root. But then, the main issue would be the interoperability of the various roots across the world with the possible objective of developing a system of joint distributed ONS roots.

From a broader perspective, a range of public policy concerns are likely to arise in the context of the developments leading to the Internet of Things. These concerns need to be considered when thinking about any technology that would enable the link between

physical objects and remote databases, and therefore when thinking about the governance of the future Internet of Things.

Firstly, with the anticipated widespread deployment of RFID the associated communications infrastructure is likely to become a new critical infrastructure. The need to ensure business continuity for critical infrastructure means that EU Member States will not accept to have to rely, for such systems to work, on a single out-of-country service provider which, in addition, might be placed under non-European jurisdiction.

Secondly, as we have seen previously, there is a need to evaluate the security implications such as denial-of-service or unauthorised item tracking and tracing. Such evaluation should take into account the technical and social infrastructure of the Internet. In this respect, the need for centralisation as an instrument to allow quicker and more focused reactions to security threats should be balanced against the advantages of a distributed architecture, both in terms of resilience to attacks and of more general social benefits such as low-cost accessibility and freedom to receive and transmit information.

Thirdly, facilitating transparent and non-discriminatory conditions is also essential to ensure that Europe's industry can offer competitive and innovative services on the global market. Furthermore, a market based on open standards and interoperable interfaces is necessary to provide small- and medium-sized enterprises with appropriate entry conditions in the market of Internet of Things services.

Fourthly, as the shift from RFID to the Internet of Things takes substance, the concerns regarding privacy and data protection will not focus primarily on the retail sector, as it has been the case during the debate which took place recently within the RFID Expert Group created by the Commission in June 2007. Such concerns will also be linked to a globally unique identifier of a known structure and to the information systems behind which the aggregation of different data could result in the creation and exploitation of individual's behaviour.

Fifthly, recent experience suggests that we need to avoid the emergence of a proprietary mono-culture and a *de facto* monopoly service provider situation where the consequent lack of diversity would generate a potential single-point of failure. Therefore, the question arises how to ensure that open standards, interoperable interfaces and compatible data exchange formats are provided, so as to allow providers to collaborate with one another and users to switch between systems.

Brave or not, a New World…

Besides and beyond these very important issues which will probably be translated into public policy principles in the next few years, I would like to draw your attention to another kind of challenge – a formidable societal and ethical challenge – with which we are confronted. To make it very clear, I have in mind the words of Trajan, a knowledgeful, aware, ironical and despairing poet in "The Twenty-Fifth Hour" by C. Virgil Gheorghiu: "*Every event taking place at this hour, on the entire surface of the earth, and every event yet to take place in the years ahead, is but a symptom and a phase of the same revolution, the revolution of 'technical slaves'. Men will be considered as equal, as identical, and treated according to the same laws which apply to technical slaves, without any possible concern for their human natures.*" In his book published in 1949, Gheorghiu was predicting a time when the earth would cease to belong to men, when man would be reduced to one single dimension, the social, the impersonal.

This is literature, of course, but we need to 'listen' to what novelists and other artists are telling us with this sixth sense which they often possess. The Internet of Things is not only a matter of technology; it's also a perspective which will transform our lives and our social interactions.

As Julian Bleecker said, "*the Internet of Things is a network in which socially meaningful exchanges take place, where culture is made, experiences circulate through media sharing (...) Whereas the Internet of Machines was limited to human agents, in the Internet of Things objects are also active participants in the creation, maintenance and knitting together of social formations through the dissemination of meaningful insights that, until now, were not easily circulated in human readable form.*"

What Bleecker is telling us is essential: the Internet of Things is not just about machine-to-machine communication or the location and status of objects. It is about the fact that 'things', once plugged into the Internet, will become agents that circulate data, obtained through a huge variety of sensors mounted in different environments, including towns and buildings – look at the Tokyo Ubiquitous Technology Project –, factories, energy generation plants, and so on, or embedded in systems, or worn by users. Outside the Internet, a world full of physical objects – the order of magnitude of things on earth is roughly 50,000 billions – are waiting to be connected. When this happens, we will not necessarily see *birds and dogs and chairs and shoes blogging and taking over the world*, as Bleecker jokingly suggests, but – if we remain aware and committed – we should have in our hands a formidable instrument to change the world to make it more habitable.

In a similar line, I would like to highlight a remark which was made some 30 months ago by an individual stakeholder who posted a message on the Internet. He was telling the following: "*The Internet of Things, for all rhetorical elegance, is an important and essential step to something more profound: not an Internet of Nouns, but an Internet of Verbs. If you believe that language tells us something about the future, this means that the critical, defining features of this new Web will revolve around interactions, events and experiences, not virtual places or even real things.*" This is a matter of language, of course, but there is behind the vocabulary – nouns versus verbs – the reflection of a truth – the Internet of Things is more than the promise of a technological prowess, it's also, and primarily, a fantastic human and societal challenge.

If the Internet of Things were built in the absence of social concertation, the risks would be very high, and probably unmanageable, for mankind. Let me point out here to the NSF-DOC-sponsored report of 2002 on Nanotechnology, Biotechnology, Information Technology and Cognitive Science (NBIC). This report is about "converging technologies for improving human performance". In the language of the U.S. National Science Foundation, this means contributing to human development not through the development of individual knowledge but through implants. This is quite different!

In fact, among the priorities for improving human health and physical performance are bio-nano machines for development of treatments, nanotechnology-based implants as replacements of human organs or for monitoring of physical well-being, and nanoscale robots for medical intervention. Such developments open up exciting new horizons, but also a new set of risks and challenges, for the human spirit.

Nanotechnology will be used in medicine in at least three ways. First, nanochips will detect proteins in the body that signal a disease is present. Second, doctors will use molecular radiology to find cancer in the body – certain kinds of DNA that recognise cancer will be attached to metallic molecules and injected into the body. Thirdly, nanochips will be used to develop a genetic profile of patients to help doctors determine which drugs will have the least side effects.

While nanotech seems like the wonder technology that will change many things in our lives, there are also plenty of unknowns and potential risks. That's because, among other things, we don't yet know all the side effects of breaking materials down into tiny pieces. Let me take one futuristic example. Let's imagine that inside a matter, each atom can be reprogrammable via nanoscale devices being controlled, identified and linked by nanochips. Wouldn't this look like 'the ultimate Internet of Things'? We are here confronted with possibilities that give rise to intense emotions.

The report on NBIC goes even further by pointing to a 'Transformation of Civilisation' – wholly new ethical principles will govern in areas of radical technological advance, such as the acceptance of brain implants, the role of robots in human society, and the ambiguity of death in an era where human cloning experimentations may prevail.

Pure fiction? Who knows? Let me give you a totally different hint of the future as it is shaped today. A few weeks ago a joint nanotechnology concept called *Morph*, developed by Nokia Research Centre (NRC) and the University of Cambridge, was launched alongside an exhibition on the "Design and the Elastic Mind". *Morph* foreshadows a combination of art and science with future mobile devices being stretchable and flexible, that is allowing the user to transform their mobile device into radically different shapes.

The Internet of Things deserves a social debate in which human authenticity, which is notably shown by our capability to rise up to the universal thanks to law, is defended.

Conclusion

To conclude, I would like to express my belief that the debate on the Internet of Things is a good test of our ability to cope with the complex challenges of our time and to use new technology to shape the society of tomorrow.

I have purposefully laid a stress in my presentation on the non-technical challenges of the Internet of Things, and more specifically on the societal and ethical challenges. I believe that it is indeed essential to give the highest consideration to these aspects – technology must be managed and used to serve human beings, and not the contrary.

This said, we don't want to walk away from our future. So, we'll have to come up with some balance. And first of all, as I've tried to explain, the emerging use cases of the Future Internet should drive the requirements for the network and service infrastructure. The technical characteristics of the future infrastructure should not be designed in a vacuum but instead derive from the actual technologies, constraints and requirements that are expected to prevail in the surrounding ecosystem.

I would like to thank our knowledgeable panellists and chairpersons for participating in this inspiring conference on the Internet of Things. I look forward to a passionate and constructive dialogue during this conference and also to future discussions on this unfailing subject.

Thank you for your attention.

Disclaimer: The opinions reported in this speech are purely the author's and do not necessarily represent the views of the European Commission.