ARES project
CONSOLIDER-INGENIO 2010 CSD2007-00004
Workpackage 5 - Task 1 (WP5.T1)
Yearly Legal Report on Critical Infraestructure Surveillance

Ana Isabel Cerezo Domínguez
Universidad de Málaga

November 8, 2010

SUMMARY

1. Introduction 1

2. The Governance of the Internet of Things 2

3. Obstacles to the uptake of the Internet of Things 2

   3.1. Privacy and protection of personal data 2

   3.2. Trust, Acceptance and Security 3

   3.3. Standardisation 3

4. Action Plan for Europe 3

7. Bibliography 7

1. Introduction

One major next step in the growth and development of Internet is to progressively evolve from a network of interconnected computers to a network of interconnected objects, from books to cars, from electrical appliances to food, and thus create an 'Internet of things'(IoT) [1] [2]. These objects will sometimes have their own Internet Protocol addresses, be embedded in complex systems and use sensors to obtain information from their environment (e.g. food products that record the temperature along the supply chain) and/or use actuators to interact with it (e.g. air conditioning valves that react to the presence of people).

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

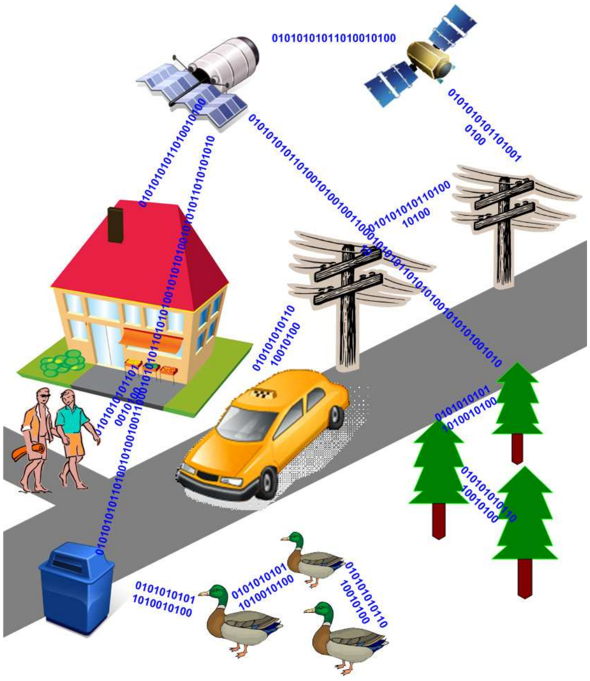

Figure 1. A particular vision of the Internet of Things [3]

2. The Governance of the Internet of Things

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

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

Leaving the development of IoT only to the private sector is not a sensible option in view of the deep societal changes that IoT will bring about. Many of these changes will have to be addressed by policy-makers and public authorities to ensure that the use of IoT technologies and applications will stimulate economic growth, improve individuals’ well-being and address some of today’s societal problems.

3. Obstacles to the uptake of the Internet of Things

3.1. Privacy and protection of personal data

Social acceptance of IoT will be strongly intertwined with respect to privacy and to protection of personal data. On the one hand, the protection of privacy and personal data will have an influence on how IoT is conceived. For example, a home equipped with a health monitoring system could process some of the inhabitants’ sensitive data. A prerequisite for trust and acceptance of these systems is that appropriate data protection measures are put in place against possible misuse and other personal data related risks. On the other hand, it is likely that the uptake of IoT will affect the way we understand privacy. Evidence for this is given by recent ICT evolutions, such as mobile phones and online social networks, particularly among younger generations.

3.2. Trust, Acceptance and Security

Information security is a must and is seen by most stakeholders as a major concern of IoT. In the private sphere, information security is closely linked to the questions of trust and privacy mentioned above. Past experience with the development of ICT shows that they are sometimes neglected during the design phase, and that integrating features to safeguard them at a later stage creates difficulties, is costly and can considerably reduce the quality of the systems. It is therefore crucial that IoT components are designed from their inception with a privacy and security-by-design mindset and comprehensively include user requirements [4] [5].

3.3. Standardisation

Standardisation will play an important role in the uptake of IoT, by lowering entry barriers to newcomers and operational costs for users, by being a prerequisite for interoperability and economies of scale and by allowing industry to better compete at international level. IoT Standardisation should aim at rationalising some existing standards or developing new ones where needed [6].

4. Action Plan for Europe

In 2006, the European Commission launched a public consultation (IP/06/289) on the development and use of smart chips (RFID technologies). Based on this it adopted a Communication in March 2007 (IP/07/332) underlining that RFID was only the tip of the iceberg of a broader ongoing evolution evoked under the name of the 'internet of things'.

The Action Plan for Europe (European Commission "COM (2009) 278) [7] expands on this statement and proposes fourteen-steps to exploit the full potential of this new evolution. The Commission, together with all parties concerned, will now implement this plan and report on the relevant activities in a further Communication in three years time.

5. Internet of Things: The 14-points of action

1. **Governance.** The Commission will work on the definition of a set of principles underlying the governance of the Internet of Things and the design of an architecture endowed with a sufficient level of decentralised management, so that public authorities throughout the world can exercise their responsibilities as regards transparency, competition and accountability.

2. **Privacy and data protection.** The Commission will observe carefully the application of data protection legislation to the Internet of Things:

- by consulting, when necessary, the Article 29 Data Protection Working Party [8];
- by providing guidance on the correct interpretation of EU legislation;
- by fostering dialogue among stakeholders;
- by proposing, if necessary, additional regulatory instruments.

4. **The right to the "silence of the chips".** The Commission will launch a debate about whether individuals should be able to disconnect from their networked environment at any moment. Citizens should be able to read basic RFID (Radio Frequency Identification Devices) tags – and destroy them too – to preserve their privacy. Such rights are likely to become more important as RFID and other wireless technologies become small enough to be invisible.

5. **Identification of Emerging risks.** The Commission will take effective action to enable the Internet of Things to meet challenges related to trust, acceptance and security.

6. **IoT as a vital resource to economy and society.** In connection with its activities on the protection of critical information infrastructures [9], the Commission will closely follow the development of the Internet of Things into a vital resource for Europe.

7. **Standardisation.** The Commission will, if necessary, launch additional standardisation mandates related to the Internet of Things [10]. Additionally, the Commission will keep monitoring developments in European Standards Organisations (ETSI, CEN, CENELEC), their international counterparts (ISO, ITU) and other standards bodies and consortia (IETF, EPCglobal, etc) with a view for IoT standards to be developed in an open, transparent and consensual manner with the participation of all interested parties. Particular attention will be given to the machine-to-machine workgroup of the European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF) in the area of discovery services.

8. **Research and Development.** The Commission will continue to finance collaborative research projects in the area of the Internet of Things through the 7th Framework Programme, putting an emphasis on important technological aspects such as microelectronics, non-silicon based components, energy harvesting technologies, ubiquitous positioning, networks of wirelessly communicating smart systems, semantics, privacy- and security-by-design, software emulating human reasoning and on novel applications.

9. **Public Private Partnership.** The Commission will integrate, as adequate, the Internet of Things in the four research and development public-private partnerships that are being prepared. Three of them, ‘green cars’, ‘energy-efficient buildings’ and ‘Factories of the Future’ were proposed by the Commission as part of the recovery package. The fourth one, ‘Future Internet’, aims at further integrating the existing ICT research efforts in relation to the future of the Internet.

10. **Openess to Innovation.** The Commission will launch pilot projects to promote the readiness of EU organisations to effectively deploy marketable, interoperable, secure and privacy-aware Internet of Things applications. These pilots should focus on IoT applications that deliver strong benefits to society, such as e-health, e-accessibility, climate change, or helping to bridge the digital divide. To be a catalyst for growth and innovation, these systems should:

– allow new applications to be built on top of existing systems and new systems to be deployed in parallel with existing systems without creating excessive burdens for market entry or other operational barriers, such as excessive licenses/fees or inappropriate intellectual property schemes [11];

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

11. **Institutional awareness.** The Commission will regularly inform the European Parliament and the Council about Internet of Things developments.

12. **International dialogue.** The Commission will intensify the dialogue on the Internet of Things with its international partners to share information and good practices and agree on relevant joint actions.

13. **Environment.** In many cases, the connection between objects will be made through a sensor or a tag embedded in the object. For the foreseeable future, tags will be made of metal (typically silicone, copper, silver and aluminium) whose presence can create difficulties on the recycling lines of glass, plastic, aluminium and tinplate. On the other hand, being able to precisely identify objects during the recycling process is an advantage and tagged objects could therefore be recycled more efficiently by being retrieved from normal bulk waste disposal.

The Commission will assess the difficulties of recycling RFID tags as well as the benefits that the presence of these tags can have on the recycling of objects.

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

6. **Assessment of Evolution.** The Commission will gather a representative set of European stakeholders to monitor the evolution of the Internet of Things. The Commission will use FP7 to conduct this work, by gathering a representative set of European stakeholders and ensuring a regular dialogue and sharing of best practices with other world regions.

7. Bibliography

[1] The Internet of Things Report:

http://www.itu.int/osg/spu/publications/internetofthings

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

[3] J. López, R. Román and P. Nájera: "Los desafíos de seguridad en la Internet de objetos", Revista SIC, 2010

[4] Christoph P. Mayer . "Security and Privacy Challenges in the Internet of Things". GSN09 Workshop

[5] Joris Claessens, Microsoft. "Trust, Security, Privacy, and Identity perspective". FIA Madrid 2008

[6] August Nilssen, Standards Norway. "Security and Privacy Standardisation in Internet of Things"

[7] IoT - An action plan for Europe:

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/952

[8] See ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

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

[10] See mandate EC/436 on RFID and mandate EC/441 on smart meters

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