Paper Prepared for the
1st Berlin Symposium on Internet and Society
October 25-27, 2011

The Internet of Things

Rob van Kranenburg
kranenbu@xs4ll.nl

Erin Anzelmo
erinanzelmo@hotmail.com

Alessandro Bassi
alessandro@bassiconsulting.eu

Dan Caprio
dcaprio@mckennalong.com

Sean Dodson
s.c.dodson@gmail.com

Matt Ratto
matt.ratto@utoronto.ca

Abstract

This paper traces the challenges and nature of the impact posed by the developments termed the ’Internet of Things (IoT)’. The Internet of Things is comprised of a number of technological protocols that aim to connect things to other things, to databases and to individuals. The speed with which the paradigm of connecting communicating objects has taken over the full range of connectivity protocol (IPv6), hardware (from cheap sensors to smart phones, iPads, tablets that are full blown computers), software (either proprietary in the cloud or collaborative open source), applications (ranging from location based services that link up to social networks to your car linked up to a particular brand network) and services (from car sharing with RFID (Radio Frequency Identification) cards (Buzzcar), to blinds texting you or your service layer that they are out of battery power (Designer) is determined by the collaborative power of the internet.

In this paper, we outline the Internet of Things’ recent history, technological challenges and policy ecology. We end by sketching a possible framework for grasping its impact in four domains: (1) the value chain where all objects can be tracked, logged and traced, (2) the service layer that can be built upon this, (3) the smart city layer and (4) its ultimate limit and scope of the Sensing Planet notion that aims to capture natural processes by globally distributed sensor grids to have counterparts in the cloud. We sketch the two basic policy and industry approaches: a reactive approach that argues IoT is manageable and non disruptive, and a proactive approach that assumes the inevitability of a full IoT situation of ’total’ connectivity and works back from this to identify the key moments of agency in policy tools and commercial products. Some assistance, we believe, can be gained by consulting a new and growing field of social research. Infrastructure Studies, a cross-disciplinary research area includes researchers from Information, Sociology, Political Science, and Computer Science. Its goal is to develop case studies on infrastructure as well as novel methods for delving into its importance in social life.

Contents

1 Introduction 2

2 Approaching the Internet of Things 4
2.1 Defining the Internet of Things . . . 4
2.2 Phases of the Internet of Things . . . 6
2.2.1 First Phase . . . 6
2.2.2 Early Research . . . 7
2.2.3 Second Phase . . . 8
2.2.4 Current Research . . . 12

3 Technological Changes and Foundations 16
3.1 Foundations . . . 16
3.2 The Internet in the Internet of Things . . . 18
3.3 Breaking the Unbreakable: The End-to-End Principle . . . 19
3.4 The Things in the Internet of Things . . . 22

4 Policy 24
4.1 The Role of RFID . . . 24
4.2 Protecting Privacy and Enabling Innovation . . . 25
4.3 Apply Existing Data Collection Privacy Requirements and Frameworks to the IoT . . . 27
4.4 Unintended Consequences . . . 27
4.5 Challenges in an IoT world . . . 28
4.6 Questions to Consider . . . 28

5 Scope and Impact 29
5.1 Development Approaches . . . 30
5.2 Moving Beyond a Reactive Approach to Governance . . . 32
5.3 Inclusive Designs for IoT Services . . . 34
5.4 How to Analyze IoT - Some Conceptual Guidance . . . 35

6 Use case: Privacy 38
6.1 A Reactive Approach: Issues to be Addressed . . . 39
6.2 Policy and Self Regulation: The RFID Privacy Impact Assessment Case . . . 41
6.3 A Proactive Approach: Issues to be Addressed . . . 42

1 Introduction

It is rare that one is in the presence of an ontological shift. It is even more rare that one is in a position to shape it. Yet this is exactly the position many engineers, policy makers, and citizens are in today. In 'The Computer for the 21th Century' (Weiser, 1991) was the first to voice the idea that miniaturization and ubiquity of sensors would eventually lead to the disappearing of computational elements 'into the fabric of everyday life' and the potential for computing as procedure, as visible hardware and as protocol, to move into an invisible background. Interestingly, Mark Weiser himself, who passed away in 1999, did not consider what he called 'ubiquitous computing' as something that would radically alter or change the relationship between humans and the new digitally hybrid environment. However, he did propose a series of ubiquitous computing scenarios that continue to involve both the rhetoric and the reality of computing today (Bell and Dourish, 2007).

From the 80's onwards, this domain has been identified with different names: ambient intelligence, calm computing, ubicomp, pervasive computing, most of them pushed by industrial players such as Philips and IBM. A dominant characteristic unites these different perspectives: a sense that internet connectivity is becoming increasingly ubiquitous and pervasive. In other words, the idea that eventually everything, including mundane physical artefacts, will be connected.

In a 2007 conference appearance, the founding executive editor of 'Wired Magazine', Kevin Kelly gave a lecture about the first 5,000 days of the world wide web. "In 5,000 days," he argued, "less time than it takes for a child to progress through the school system, the world had been transformed". Kelly noted how online social networking through applications like MySpace and Facebook was changing the nature of social interactions. He referenced the different engagements with travel and with space made possible by searchable maps and direction services. He emphasized the changing nature of expertise highlighted by free encyclopedias such as Wikipedia. Kelly then moved on to discuss the next 5,000 days of the web, arguing that the speed in which the web has caught on and the haste in which it has transformed the industrialised world, showed no signs of slowing. "Everything," Kelly stated, "will be part of the web. Every item, every artefact [. . .] will have some sliver of connectivity that will be part of the web." In other words, according to Kelly in 2007, before 2024, everything will be connected to the point where "the environment will become the web".

What Kelly was describing was no less than an "internet of things", namely, a world where a pair of shoes becomes seen as "as a chip with heels; a car as a chip with wheels". Like the promise of air travel or space flight, this vision has been an idea long before it has been made a reality. As other computing paradigms before it, this vision guides the direction of technical developments as much as it predicts them (Bell and Dourish, 2007).

At the heart of the Internet of Things is a metaphor. Put most simply: it is a network of connected objects. Vehicles, machine components, domestic consumable durables, the clothes on your back, all are being hooked up to a network with a speed most of us have yet to comprehend.

True, this Internet of Things (IoT) is difficult to conceive. But then again, 5,000 days ago, what journalist considered that the computer in the corner could shake the power of the printing press? What record company executive pondered the company's demise the first time they went online? What bibliophile imagined you could carry an entire library around in their briefcase?

It is now more than 10 years that individual RFID tags have dropped below a one cent cost, making their adoption within diverse business areas not just technically possible but economically feasible as well. Since that time, RFID and other technologies that are essential to IoT have been adopted in a variety of contexts. RFID tags are increasingly used in logistics, the pharmaceutical industry, agriculture's value chain, in addition to uses in a wide variety of contexts and business areas. Bit by bit, byte by byte, this Internet of Things is being assembled, much without a wider public's knowledge of the idea, much less their input or consent.

The discourses around these developments are in a variety of places and in different languages and styles. The people that shape the discussion come from very diverse backgrounds: Kevin Kelly started to work as a writer and photojournalist. Bruce Sterling writes science fiction novels. Usman Haque is an architect and designer, founder of Pachube. Rob van Kranenburg studied Language and Literature and is a writer. Rafi Haladjian is the founder of the first Internet Company in France in 1994, and Violet, including the Nabaztag Rabit, one of the first 'smart objects'. Adam Greenfield is a designer and writer who recently founded urbanscale.org Mike Kuniavsky is a user experience design, process and strategy consultant and the author of two books on user experience design and research. Actually, there is not one engineer or technologist among the first 10 of the Postcapes list 100 people "influencing the topic on a daily basis whether through evangelizing, standardizing or through their own companies.“ [1] The other three influencers listed are *Design Consultancy Berg* by Matt Webb, Jack Schulze Matt Jones, and Timo Arnall as Creative Director, the *Web of Things*, a "community of developers, researchers, and designers that explore the future of the physical Web" operated by Vlad Trifa and Dominique Guinard, and *Council, a think tank for the Internet of Things*.

Therefore, while many technical challenges remain to be overcome, the main themes and discourse around the Internet of Things are primarily social in scope and intent. This may be one reason why so many of the discourses and stories on this topic are deemed fuzzy: there is a clear gap between the writers and the engineers. This paper tries to bring these discussions and developments one step closer through analyses and commentary that link technical knowledge and expertise, as well as work on IoT policy and political importance. The research question of this paper offers directions to investigate IoT from two outer ends of the current governance and investment spectrum. On one side, a reactive position that sees IoT as a layer of connectivity on top of current institutions, business models, and governance structures. On the other, a proactive position that sees IoT as a new ontology that will alter the relationship between human beings, autonomous M2M (Machine to Machine) processes and decision making structures.

[1] [Internet] Available from: Postcapes, tracking the internet of Things, platforms; http://postscapes.com/internet-of-things-platforms [Accessed 02 December 2011].

2 Approaching the Internet of Things

2.1 Defining the Internet of Things

> *"When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly. What's revolutionary in all this is that these physical information systems are now beginning to be deployed, and some of them even work largely without human intervention."*
>
> *(McKinsey & Company, 2010)*

As noted by most commentators and articles on the subject the definition of the Internet of Things (IoT) is still rather fuzzy and subject to philosophical debate (Uckelmann, Harrison, Michahelles, 2011). Practically any book or report written on IoT starts with a discussion on previous definitions and each author seems to insist on adding their own special ingredient to the final recipe (Casagras, 2009). This process is somewhat strange, from a technologist perspective: it is doubtful that Vint Cerf and Bob Kahn spent long hours in forging a definition for the internet - first came the technology, then the definition. There are many linguistic versions of the concepts comprising the Internet of Things technologies. Often the variations are a result of the blurring of products and technologies involved. Such terms vary from ambient technology, ubiquitous technology, sensor web, sensor network, wireless sensor networks, smart dust, smart cities, smart data, smart grid, cloud data, Web 3.0, and Object Naming System (ONS), to name but a few (Uckelmann, Harrison, Michahelles, 2011).

Variations also result from geographic or the national boundaries; for example, in China and Europe the term internet of things is widely accepted. While in the US, it is more commonly referred to as smart object, smart grid, data grid, cloud computing. Brian Cute, CEO of the Public Interest Registry suggested that a common agreement on terminology and concepts is necessary and "a sound understanding of the internet itself by all stakeholders cannot be assumed" (Cute, 2011). In Opportunities, Challenges for Internet of Things Technologies, José Roberto de and Almeida Amazonas have searched the IEEE Xplore search engine (on December 2, 2010) for the term "Internet of Things" restricting the year of publication to 2010. The search resulted in "150 papers, including conference proceedings and periodicals". China leads with an overwhelming 51.3%, followed by Europe with 37.3%. The authors state that this does not mean "a leadership in any of the following criteria: quality, originality, technical and/or scientific contribution, worldly knowledge dissemination." The number of American papers is distorted "because IoT-related research and development has been conducted under different names such as pervasive and ubiquitous computing, wireless sensor networks and so forth." The authors also see a difference of approach: "Most American papers put the technology itself as the main objective while European papers focus on the use of the technology, i.e., they are more user-centric and care about the benefits IoT can provide to the society" (De and Almeida Amazonas 2010).

Whether we will get close to agree upon terminology largely depends on the applications that the technologies can enable. For the moment, we must agree to multiplicity.

The term "Internet of Things" was initially used by Kevin Ashton in 1999, and became of wide-spread use thanks to the work of the Auto-ID Centre, a research group working in the field of networked radio-frequency identification (RFID) and other emerging sensing technologies. However, the definition was not given at that time, and although there is a general agreement that IoT involves objects and connectivity, the precise wording is still to be found.

A commonly accepted understanding is the one articulated by the ITU (2005) tying together item identification; sensor technologies and their ability to interact with the environment (cf. also ENISA, 2010). Within the EU research domain, the Cluster of European Research Projects on internet of things (CERP-IoT, now IERC) defines IoT as a ”dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual ’things’ have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network“ [2] (Vermesan, 2009).

Trying to simplifying the matter, and including all possible devices that belong to the IoT domain, it is possible to consider the Internet of Things as the superset of all objects that are uniquely identifiable by electro-magnetic means and for which it is possible to specify a semantic and/or behaviour.

Not only is there disagreement on the nomenclature of the IoT, there is also disagreement on the scope of the IoT. Besides smart objects, there is an emerging question if human users included in the definition, as hypothesized by the European Research Cluster on the IoT (IERC). A pan-European consumer group wishes that the IoT be called ”the Internet of People“, so as to emphasize the human element (BEUC/ANEC, 2008) or the ”Internet of Everyone“ in a recent report published in 2011 funded by Accenture. IETF however states that the IoT as a concept ”refers to the usage of standard Internet protocols to allow for human-to-thing or thing-to-thing communication” (Garcia-Morchon, 2011), hence, including the human element in the very definition.

Finally, it is necessary to spend a few words on the meaning of the word "smart", used extensively in this field. A smart object is commonly called a device able to sense or interact with the environment, and uniquely identifiable. Smart is synonym of "intelligent", which comes from the Latin "*inter*" and "*legere*": literally, to read between [the lines]. As this practically means to be able to interpret, we can easily see that it has a very strong non-deterministic component. To show this fact in practical terms, let us imagine two people, both of whom are very intelligent. We might expect that they would share the same opinion quite seldom and both sides normally have their valid reasons. Many, if not all of us, experienced (or, better, suffered) from non-deterministic behaviour of computers; however, glorifying the capacity of objects to self-determine their actions is probably not the target of the work in this area. While we do not propose in this document an alternative expression, we strongly feel that the use of "smart" should be carefully thought through.

[2] For more definitions within the EU context see Casagras (2010) and EPoSS (2008).

2.2 Phases of the Internet of Things

2.2.1 First Phase

The first phase encompasses the period of 1990 to 2005 and can be traced to the moment Mark Weiser, chief scientist at Xerox Park, publishes “The Computer for the 21st Century“ (Weiser, 1991). From the 1950’s onwards the critical energy was spent on getting computers smaller, building a technological grid to host these and creating a psychological and social frame for bringing work to the home and private sphere.

Weiser realized that the dashboards for these models, the visualisations and experiential situations, were never meant for individuals, but instead for systems and large companies, institutions and think tanks. Weiser is the first the raise the problematic issue of the interface in everyday life and interactions. He begins to wonder how best to access this virtual world not only through the keyboard and mouse, but intuitively and using all of the computer’s potential.

The goal of ’making the computer disappear’ can happen in different ways and disappearance can take different forms (Weiser, 1991). Physical disappearance refers to the miniaturization of devices and their integration in other everyday artefacts, as for example, in clothes, so that you do not see them any more. Mental disappearance refers to the situation that the artefacts can still be large but they are not perceived as computers because people discern them as, e.g., interactive walls or interactive tables (Streitz, 2001). Thus, technology moves mentally into the background. Two core research questions emerge: “how can we design human-information interaction and support human-human communication [. . .] by exploiting the affordances of existing artefacts in our environment? And, in doing so, how can we exploit the potential of computer-based, support augmenting these activities?[3]”

A decade later, a Microsoft press notice echoed Mark Weiser: “As people find more ways to incorporate these inexpensive, flexible and infinitely customizable devices into their lives, the computers themselves will gradually ’disappear’ into the fabric of our lives.“ Unfortunately they are just not yet running on “inductively powered on heat and motion from their environment without batteries” (Microsoft, 2003).

One of the ways to exploit this potential, according to Liam Bannon, Director of the Interaction Design Centre, University of Limerick, is to look at the pioneering work of designers Anthony Dunne, Fiona Raby and Julian Bleecker. Dunne and Raby’s impressive body of work has managed to “raise awareness, expose assumptions, provoke action, spark debate, and even entertain” with their notion of critical design. Julian Bleecker creates “design fictions, artefacts that tell stories new forms of imagining and prototyping” by the blending of science fact, and science fiction.

This is the beginning of rethinking the computing paradigm and the discovery of an individual that claims a different kind of control over the machine; one of individual reciprocity. To paraphrase Mark Weiser, the idea was to take the connectivity out of the computer and put it in the very fabric of our clothes (so we get wearables), in homes (smart homes) and in cities (smart cities). In other words, let us make ourselves into a ’dashboard’; the environment will

[3] Streitz, N. A., Kameas, I. Mavrommati (Eds.) (2007), The Disappearing Computer: Interaction Design, System Infrastructures and Applications for Smart Environments. State-of-the-Art Survey, Springer LNCS 4500

become the interface.

The Internet of Things is an emerging field yet to reach the consciousness of the masses. Yet it has a surprisingly long, even illustrious industrial history. Radio Frequency Identification started in World War II. British ’spitfire’ fighter planes would have active tags in the cones of their noses. Huge radio towers blasted radio waves that searched for the Spitfire signals: friends flew, foes were downed. Access control appeared to be a logical peacetime uptake of the same principle: friends open doors, foes get locked out.

RFID is also an integral part of your life. Most of us carry RFID in our wallets without even acknowledging that we are engaging with network technology, but we hold the cards we use to get into the office to the RFID reader embedded in the wall near the door. This reader pushes a constant wave of energy. The antenna in the chip pucks up the energy then moves it on to the chip that says ’hello’. The number appears in a database and in the database one can attach any action to that number: ’accept as OK and allow to pass’. To all extents and purposes, the computer is in our pocket and yet it has disappeared from our consciousness, just in the way that Weiser and others predicted. As far back as 1999, MIT brought the cost of the tag down to below 0.01$ an important moment to start considering using RFID in a logistical ecology with barcodes and shotcodes (2 and 3D barcodes) (Albrecht, 2002).

2.2.2 Early Research

The Disappearing Computer [4] started in 2001, a cluster of 17 projects addressing a wide range of themes and issues, and therefore, being conducted by interdisciplinary research groups (Streitz, 2001; Streitz, N. and Nixon, P., 2005; Streitz, N. and Kameas, A. 2007).

Its mission was “to see how information technology can be diffused into everyday objects and settings, and to see how this can lead to new ways of supporting and enhancing people’s lives that go above and beyond what is possible with their computer today” It hosted a wide variety of projects, such as Workspace, aiming “to augment the work environment through spatial computing components, initially for members of the design professions, but with applicability to a wide range of work domains”[5]. The MiME[6] project that focuses on the relationship between computer technology and people’s experience of their intimate media collections around the home, and e-Gadgets (e stands for extrovert) seeking “to adapt to the world of tangible objects the notions of component-based software systems by transforming objects in people’s everyday environment into autonomous artefacts (the eGadgets). The eGadgets range from simple objects (like tags, lights, switches, cups) to complex ones (like PDAs, stereos) and from small ones (like sensors, pens, keys, books) to large ones (like desks, TVs)”[7]. The forerunner to the Disappearing Computer was i^3: Intelligent Information Interfaces[8]. The Call for $i^3$3 in 1996 read:

[4] [Internet] Available from: http://www.disappearing-computer.net/projects.html [Accessed 02 December 2011]

[5] [Internet] Available from: http://daimi.au.dk/workspace/index.htm [Accessed 02 December 2011]

[6] [Internet] Available from: http://www.mimeproject.org/ [Accessed 02 December 2011]

[7] [Internet] Available from: http://www.extrovert-gadgets.net/ [Accessed 02 December 2011]

[8] "Intelligent Information Interfaces, or i^3, is an Esprit Long-Term Research initiative. The aim of i^3(pronounced "eye-cubed") is to develop new human centred interfaces for interacting with information, aimed at the future broad population. i^3aims at a radical departure from present-day human-machine in-

> ”The Connected Community calls for investigative research leading to new interfaces and interaction paradigms aimed at the broad population. As its focus it takes interfaces for the creation and communication of information by people, and for people and groups in a local community.“[9]

2.2.3 Second Phase

Research in this area is very close to innovation, as the developments are ’real time’. Currently over 20 IoT platforms are starting up[10] and this number will grow exponentially as the connectivity between objects, platforms, services and infrastructure increases.

The second phase encompasses the period after 2005 until the present day. This section charts the construction of the competing technologies that constitute IoT. Competing terms and concepts are ’ubicomp’, ’ubiquitous computing’, ’ambient intelligence’, ’pervasive computing’, ’things that think’, ’calm technology’, ’intelligent information interfaces’. Why did the ’Internet of Things’ seem to be the winner? IoT is understandable for people as it works with the metaphor of the internet. Now we have the interconnection of everything as the web of things: a layer over things. The move to the term IoT by the International Telecommunications Union (ITU, 2005) is marking the second phase.

As the terms ’ubicomp’ and ’pervasive computing’ were pushed by IBM, and ambient intelligence by Philips, these terms seem to promote industrial agency of the environment over the individual, thus raising immediate privacy issues. When engaging with these early versions of the Internet of Things you cannot help but ask yourself who is in control? Fuelled by logistics, supply chain management and access control, their conceptual frameworks stem from the key function of what becomes to be seen as the glue to this world in which everything is connected to everything.

If asked in 2000, why are they building this nascent Internet of Things? The answer would have been because companies and governments amass huge amounts of data in order to run more agile data mining algorithms to bring them more likely scenarios of the immediate future. Because data storage became so cheap it soon became possible to store copies of the entire internet (Burleson Consulting, 2007). The early protests against RFID and its invisible tracking ability were directed not only against the patents of industry dug up by Katherine Albrecht in her book ’SPYCHIPS: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move’, but by the fact that this operation towards unique identifiers of all objects on earth was run as if it was a mere upgrade of the logistics and efficiency thinking of the barcode (Albrecht and McIntyre, 2003). There were too few stakeholders involved to create a critical debate.

terface concepts and does this under the assumption that this can only be done guided by a long-term vision intertwining human, societal and technological factors. The initiative aims to launch research on new forms of interaction that will place people as active participants rather than passive recipients of information.“ http://cordis.europa.eu/esprit/src/eyeintro.htm

[9] The Connected Community has been developed by Philips International (Irene McWilliam - email c887536@nlccmail.snads.philips.nl), Domus Academy and Meru Research. http://cordis.europa.eu/esprit/src/eyecall.htm

[10] [Internet] Available from: http://postscapes.com/internet-of-things-platforms [Accessed 02 December 2011]

If we are asked today, why are ”they“ building this, we notice immediately that is becomes increasingly unclear who ”they“ are. As ”they“ are now startup companies that have roots in artistic and design practice (such as Arduino and Pachube). In web 2.0, online social networks such as Facebook, as well as large technology corporations such as Apple, Google, IBM/Cisco, SAP, Siemens, Lufthansa, IoT Reference Architecture initiatives such as the FP7 IoT-A project (www.iot-a.eu), in the EU Expert Group on IoT bringing a wide variety of stakeholders together[11]. In the rapid prototyping ecology of fablabs, bricolabs and open soft- and hardware initiatives (Open NFC, 2011; Open Picus, 2011[12]; Arduino, 2011), and projects such as Sourcemap (Sourcemap, 2011) that makes maps of the parts and source of all kinds of objects from planes to French cheese. ”After a decade of hearing about 'the Internet of Things', where everything will have an IP address, I'm starting to finally believe it, says Chris Anderson editor of Wired Magazine, and author of The Long Tail and Free: “What's changed? The Open Hardware movement, which is doing for connected devices what the Web did for information. The old vision of the Internet of Things came to us from the likes of Cisco and Nokia, which were trying to promote end-to-end connected device standards (that used their gear). Think of that as the ”Information Superhighway“ era of the net, those days in the early 1990's when the wired future was going to be brought to us by AT&T and Cablevision.”[13]

In April of 2010, Arrayent launched its internet-connect-your-product-in-a-day DevKit “enabling product companies to connect their products (sold at retail or Cedia channel) to web applications, smartphone and PC browsers at unprecedented low cost”. Arrayent did not wait for global standards like EPC Global but decided to look at the real connectivity they wanted to offer and decided to take responsibility for every step: the tag, the reader, the database and the server.

Bob Dahlberg (VP sales of Arrayent) argued that, “There has to be business value in replacing [the] ”PC in the middle“ paradigm with a seamless wireless network. The obvious example is to examine what impact the Kindle has had on the e-book market, namely a 133% growth (Council, 2010). He foresees a coupling of functions, and selling ”consumables“, such as ”air cleaners that send text messages to remind you that the filter is clogged“. Brand loyalty can be build 'by giving a channel something more to sell, such as on going service. In the case of blinds, for example Designer gets notice that Mrs Jones batteries for her motorized blinds need to be changed.”[14]

This requires a different kind of trust for how can the aforementioned Mrs Jones know when her batteries are down?[15] If the company needs cash at one particular point might it

[11] In order to propose an Internet of Things Impact Assessment procedure and format similar to the process that led to the PIA, The ”Privacy Impact Assessment Framework for RFID applications“ has been endorsed by the Article 29 Working Party on 11 February 2011.

[12] Available from: http://www.theinternetofthings.eu/content/openpicus-open-source framework-embedded devices [Internet] Accessed 02 December 2011]

[13] Anderson, Chris. Why the Internet of Things finally makes sense. [Internet] Available from: http://www.wsnblog.com/2011/11/15/why-the-internet-of-things-finally-makes-sense/ [Accessed 02 December 2011]

[14] Dahlberg, Bob. [Internet] Available from: http://www.theinternetofthings.eu/content/arrayent-internet-connect-your-product day-devkit [Accessed 02 December 2011].

[15] “A security 'noob mistake' has left the batteries in Apple's laptops open to hacking, which could result in a bricked battery or, in a worst case scenario, fire or explosion [. . .] Laptop batteries include microcontrollers

not ping the batteries to send them notice? The ink cartridge industry, for example, has a very bad track record in this area, as customers realize that there is still ink in one particular colour reservoir yet the software indicates that you have to replace it. Here the physical world and the virtual world do not meet and this lack of transparency has created a huge grey market.

In this second phase of IoT, we see social media and objects beginning to merge in meaningful ways. This has a playful quality to it. Facebook bought Nextstop, a user-generated travel recommendation site, in July 2010 (Gannes, 2010). Before this deal Facebook had been trying to buy Foursquare, a web and mobile application that allows registered users to connect with friends and update their location. Bearing in mind the kind of merging of functions that Arrayent is encountering as business opportunities the following scenario was very conceivable. If you "check in" from a physical location by entering into the application on your mobile phone that you are here (sort of Tweeting your real life coordinates) this is converted into a direct update in your online Facebook status. You "check in" your local supermarket. A feed is alerting your Facebook status. You play Mafia Wars, a popular multiplayer social network game. The game "sees" your location and Coca-Cola has set up a good deal for you there. You buy one, you get two plus points in the game on-line.

The internet and the IoT, state Ratto and van Kranenburg, enable mass participation of growing groups of individuals in what used to be macroeconomic issues: energy (coupling smart meters, production of goods (reprap, fablabs), communication (open content, software, hardware and networks). Broader question for future research include how far these trends – that are global - could affect planning and large architectural projects: mobility, transport (mapping on different data, construction and community co-design). Ratto and van Kranenburg propose the creation of an infrastructure of generic information through the development of shared and open hardware and software test beds for experimentation and a supportive online space for the sharing of questions, ”how-to's“, problems, and results. They call this loosely organized set of already existing bottom-up techno-cultural labs, R&D institutes, academic labs and research, and open source hardware initiatives bricolabs (see www.bricolabs.net), in order to celebrate their ad-hoc, experimental nature, and their emphasis on practices of reworking, redoing, and ”making do“.

When we think of infrastructural projects, we think ”big“, ”scale“, ”expensive“, ”complex“ and ”central“. Is it possible to address things such as roads, sewage systems and other infrastructural requirements in a decentralized way while still keeping the balance in costs, productivity and energy efficiency? Can infrastructural projects be crowd sourced? This was the subject of a Council workshop in the Picnic 2011 festival. Festivals like Picnic, Isea, Transmediale, Lift, RIXC, DEAF, Future Everything, Pixelache, Scrapyard Challenges – and local dorkbots – have greatly accelerated the playful adoption of open source software (Processing) and hardware (Arduino – an open-source electronic prototyping platform) and have facilitated debate and discussion on smart objects and environments among hackers, designers, thinkers and tinkerers. The first Conference to address the Design Challenge of

which constantly monitor charging voltage, current, and thermal characteristics, among other properties. These microcontrollers are part of a system called the Smart Battery System, designed to improve the safety of Li-Ion and Li-Poly cells used in these batteries." (Foresman)

Pervasive Computing was Doors of Perception, Flow 2002. Neil Gershenfield,[16] Bruce Sterling, John Thackara,[17] Malcom McCullough,[18] Esther Polak[19] as well as Usman Haque were among the speakers. Pachube stems from sensor based projects that circulated and grew in this environment (Haque, 2011). A diverse array of projects including, FabLabs, maker communities, the pontos de cultura in Brazil, co-working Design studios and others (citizen science, DIYbio) have grown in numbers in recent years and enhance both citizenship and democracy but also the innovation potential through an active and direct involvement of citizens in the R&D process, not least in term of translational and participatory research. Supportive of both science and technology literacy as much as of citizen power, they aim to involve people directly in the design and R&D phase of technology but also in the political, legal, and ethical issues related to the adoption of emergent technologies."[20]

While there is a growing interest from Venture Capitals towards IoT Services and Technologies, some companies and start-ups still face troubles in finding sufficient funding to develop fully-fledged operations. We can take Pachube as an example; labelled the ”most promising IoT start up” for years, Pachube was bought in July 2011 by Logmein for $15m outright (MacManus, 2011). Pachube, a web-based service built to manage the world's real-time data ("patch-bay") was beta until 2010. In a very short space in time it became an instigator, as well as a hub and a driver for the Open Data movement, “as the Fukushima disaster has touched off concern worldwide by showing the need for governments to provide data in open, accessible formats.”[21] Usman Haque, founder and CEO, related at Forum Europe Brussels 2011 how he preferred to stay in Europe for its rich cultural climate, high

[16] Prof. Neil Gershenfeld Director, The Center for Bits and Atoms, MIT. Author of When things start to think, Neil A Gershenfeld, 2000. Holt Paperbacks.

[17] author of In the Bubble: Designing in a Complex World. Cambridge, Mass: MIT Press, 2005

[18] Digital Ground Architecture, Pervasive Computing, and Environmental Knowing, October 2005.ISBN-10: 0-262-63327-2 ISBN-13: 978-0-262-63327-7 Digital Ground is an architect's response to the design challenge posed by pervasive computing. One century into the electronic age, people have become accustomed to interacting indirectly, mediated through networks. But now as digital technology becomes invisibly embedded in everyday things, even more activities become mediated, and networks extend rather than replace architecture.

[19] Esther Polak showed one of the first location based art works: " In our everyday life, we usually follow fixed paths and trajectories throughout the day: from our home to work or school, to family, to familiar stores and to places where we spend our free time. We all have invisible maps in our head: of our immediate surroundings and of the roads we take every day. The way we move around in the city, and the choices we make in this process, are determined by this mental map. For the exhibition 'Maps of Amsterdam 1866-2000', Waag Society and Esther Polak together with Jeroen Kee were invited by the Amsterdam City Archive to produce a work about mental maps in that city: 'Amsterdam RealTime'. During two months, 75 volunteers were tracked by GPS in their everyday movements and routines around the city. These traces were then drawn as white lines over a black background. The resulting, animated map has a distinct look and feel of psycho-geographic experience: it is not precise or rational,but expresses the intuitive and personal aspects of geography. It shows a city that does not consist of buildings, roads and water, but of the movement of its inhabitants. Thicker and brighter lines indicate greater frequency of travel. The map also was influenced by the variety of means of transportation: a cyclist will produce completely different traces than someone who drives a car. Once the participants became aware of their mapping outcomes, some even attempted to create artful GPS drawings. Interestingly, the final, combined map of all individual traces resembles an objective city map again. " http://realtime.waag.org/

[20] This is the subject of the research of Denisa Kera who has received a small modest research grant from the Singapore government to investigate where innovation comes from in the current networked reality

[21] Steinbach, Marian. Pachube blog 25 July 2011, [Internet] Available from: http://blog.pachube.com/2011/07/no-more-secrets-open-data-pioneer.html). [Accessed 02 December 2011]

education culturally diverse young talent and politically stable climate. Yet, no venture capital money was found in Europe.

2.2.4 Current Research

The European Research Cluster on the Internet of Things (IERC) is sponsored by the European Commission's Seventh Framework Programme. It focuses on enhancing Europe's competitiveness in the information society, as well as exchanges in best practice sharing at an international level on IoT matters (IERC, 2011). In a separate development, the UK government has allocated a £5m ($8.3m) grant to develop the IoT in the UK. Hosted by the EU's Seventh Framework Programme (FP7) and the European Lighthouse Integrated Project is the "Internet of Things Architecture" (IoT-A) project. IoT-A addresses the Reference Model and possibly several Reference Architectures related to the IoT domain. IoT-A plans to generate different reference architectures according to abstract requirements for the technology, creating design guidelines for real systems. At the same time, real end-users and real applications will provide precise domain-specific requirements, which will drive theoretical work. Key EU research issues are discussed at the IERC's IoT-week[22]

Patrick Guillemin of Strategy & New Initiatives, ETSI, The European Telecommunications Standards Institute[23] sees IoT as ”a system of systems, a network of networks and although the challenges are huge as the terrain is so big: FP7 research, RFID Mandate, IoT/RFID, ISGF AFI M2M through initiatives like Casagras 1 and 2 there are timely standardisation debates going on. We tend to look from the rear view mirror so the challenge with all policy makers in this dynamic and exciting time is to be careful before we legislate and lock in. It is important to realise that in Europe, IoT did not simply 'pop up'. The work of EU research, from i^3(Intelligent Information Interfaces), Future and Emergent Technologies through more specific programs such as Casagras has been very deliberate“.

The past decade has also shown that there will not be one technical standard for IoT but several generic numbering schemes, which makes the role of middleware, interfaces and open standards of paramount importance. The key factor of openness was very present in the discussion that followed. uID in Japan was very much a result of the openness of the infrastructure and platform together with the very strong links between academic research and industry R&D successful cases, favouring, as Ken Sakamura, originator of uID stated, not a *de jus*, but a *de facto*, more informal environment (van Kranenburg, 2010).

The Annual Internet of Things Europe 2011 Conference[24] (going into its fourth year),

[22] The IoT-Week is an event organised together with four European Projects, IoT-A, IoT-i, CASAGRAS2, SMART SANTANDER and with the support of the European Research Cluster on Internet of Things (IERC). It is held once a year. For the calender see http://www.internet-of-things-research.eu/events.htm For more information, please contact us at info@internet-of-things-research.eu.

[23] The European Telecommunications Standards Institute (ETSI) “produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies“. [Internet] Available from: http://www.etsi.org/WebSite/AboutETSI/AboutEtsi.aspx [Accessed 02 December 2011]

[24] See also The 2nd Annual Conference Internet of Things Europe 2010 Report. Held on 1st and 2nd June 2011. The Crowne Plaza - Le Palace, Brussels. A Roadmap for Europe This report of the conference has been written by Rob van Kranenburg, Conference chair. [Internet] Available from: ec.europa.eu/information_society/policy/.../iotconferencereport2010.pdf [Accessed 02 December 2011]

is ”run with the support of the European Commission, joined together business leaders, consumer advocates, policy makers and entrepreneurs to explore what opportunities and risks the Internet of Things will offer businesses and consumers (van Kranenburg 2010). These kinds of meetings become more important as the stakeholders become more varied, unschooled in bureaucratic processes, less formal and less hidden from public view.

The story of the current RFID standard called ’EPC Global’ - is the story of two standard bodies EAN and UCC merging to become GS1 in 2005. In a bold movement that no regulator foresaw, they scaled their unit of data from being in a batch of 10,000 and thus uninteresting for individual consumers to that of the uniquely identifiable item. Holding your phone to a package of coffee not only gives you information on where it came from, how green it is, but also who, in your social network on LinkedIn or Facebook, is buying it. From a very mundane and ’dull’ logistics tracker of batches of goods they are now enablers of rich information that can potentially target individual people in their consuming, informational and social habits. GS1 is now potentially a media company. These kinds of direct interaction with consumers by former logistical and back end operators, is fuelling interest in Near Field Communication (NFC). Talbot points to the “inherent power, sensing and location-finding capacities, access to internet-based the cloud services and burgeoning popularity of NFC-equipped mobile phones, and their ability to target advertising, translate text, check into flights, buses or metros, make photo analysis, data bumping on phones, allow people to broadcast their location in order to meet, and make payments.“ These services are made available through technology, such as GPS chips, location identifiers based on Wi-Fi signal strength, and cameras (Talbot, 2011). It is forecasted that NFC will spearhead machine-to-machine (M2M), or IoT, development (China Communication Network, 2011).

The primary standards bodies or agencies who aim to manage standards in IoT are varied both locally and internationally. Internationally, it is the International Telecommunication Union (ITU), International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), GS1/EPC Global, the of Electrical Electronics Engineers (IEEE). In Europe, it is the European Telecommunications Standards Institute (ETSI) and European Committee for Electrotechnical Standardization (CEN/CENELEC). In China, it is the Ministry of Industry and Information Technology, the China Communications Standards Association and the China Electronics Standardization Institute (CESI). In the US, the standards body is the American National Standards Institute (ANSI). As an exception, it does not presently seek to implement standards on the IoT (Chinese Communication Network, 2010).

There is a delicate balance between producing standards at an early phase of development, or letting the developers and users determine organically which protocols are best serving the dynamic IoT and applications. On the one hand, standards can produce more quickly a format to promulgate the spread of IoT technology. Particularly, it is China who is calling for standards to be defined in the IoT, claiming that standardisation is urgent.[25].

Along these lines of advocating for standards, there is the view that competing standards may paralyze markets as users and consumers will wait for a dominant technology

[25] Cf. the article by Wen Ku, director of the Technology Division of the Ministry of Industry and Information technology, as well as Zhu Gaofeng, chairman of China Communications Standards Association, advocating the study of and advancement of standards in IoT (REFERENCE from c114.net, cite as Wen/Zhu 2010, and put the full reference in the bibl)

to emerge. Jakobs, Wagner, and Reimers in 2011 argue that delayed standards may negatively impact their competitiveness, as some producers may get locked into old technology. To avoid such a situation, the authors claim that co-ordination between standards bodies is necessary and that such co-ordination exists and should be implemented. They state that various formal contracts exist, including the World Standards Cooperation (WSC) that governs the relations between the international standards bodies International Organization for Standardization (ISO), Electrotechnical Commission (IEC), and International Telecommunication Union (ITU). Similarly, the Vienna Agreement (ISO, 2001) provided the basis for the co-ordination of the work done within European Committee for Electrotechnical Standardization (CEN/CENELEC) and ISO. Lastly, Jakobs, Wagner, and Reimers assert that EPC Global is an ”Approved Referenced Specifications Originator Organization“ of the Technical Committee 1 (JTC1), of Electrical and Electronics Engineers (IEEE) and ISO have signed an ‘ISO/IEEE Partnership Standards Development Organization“ (PSDO) agreement. Therefore, as one will note, there are many permutations of standards in IoT. The lack of homogeneity among standards bodies themselves is a noteworthy and ponderous point in and of itself.

Another claim to early adoption of standards is the issue of interoperability. ICANN, while it does not deal with matters of standardization, it does promote interoperability for the development of the IoT. A European standards body, ETSI states that, “incomplete, unclear standards with poorly specified options can contribute to the biggest single cause of non-interoperability, namely that the unfortunate implementer is forced to make potentially non-interoperable design“.

There is further the notion of differing interoperability, for example: technical interoperability, syntactical or syntax interoperability, semantic interoperability and organizational interoperability (van der Veer, 2008).

A panel group discussion at the June 2011 Forum Europe’s conference on the Internet of Things led to consensus, particularly by the ITU and Europe’s ETSI agreeing that the responsibility of standards should not be with a single organization, but rather be a community based standards movement. ITU and ETSI stated, among several others, that they are open to working with the industry and other standards bodies in order to develop standardization in IoT.

A contrary approach to rigid standards development and regulation is to let technology develop naturally, through trial and error and user uptake. Proponents of less early adoption of standards prefer to let the community decide the mechanisms that work best, allowing for a flexible evolution. Proponents of looser standards for the IoT suggest that without enough time to allow for the dominant standard to emerge, artificial standards can be adopted prematurely. Pasi Hurri, of Finnish company BaseN Corporation, and Usman Haque of Pachube, have stated that they preferred to let technology evolve before implementing overly stringent standards.[26] Patrick Wetterwald of Cisco has further stated that not only does IoT need to be built on open standards, but it needs to be open source, inter-operable and certifiable.[27]

[26] The 3rd Annual Internet of Things Europe 2011 Conference, run with the support of the European Commission, http://www.eu-ems.com/summary.asp?event_id=70&page_id=495

[27] Idem 35

Sceptics of premature adoption, such as those above, remind us to think about who is asking for the standards? There is the topic of accountability of standards bodies, additionally. Weber suggests that standards need to be introduced that hold governing bodies accountable, information should be made more readily available and beneficiaries of accountability must be able to impose some sort of sanction on the accountable in case of non-compliance. Improving accountability by creating such framework also supports the betterment of security in the Internet of Things (Weber, 2011).

3 Technological Changes and Foundations

The technological domain of the Internet of Things (IoT) embraces several developments, as disjointed as they are numerous. As the definition itself is still under heavy discussion, as we saw in the earlier section, it is quite difficult, even tricky, to set boundaries, in order to determine clearly which technologies are within its range. Considering, for the sake of brevity, that IoT is built by “interconnected smart objects”, we can orientate our interest more towards communication technologies, developing the way this connection is established, or else consider the "smart object" perspective, in which for instance, developments related to energy harvesting and conservation, as well as the miniaturisation of printed circuits, and inclusion of transistors into commonly used materials such as plastic, wood or metals are of central importance.

3.1 Foundations

In any case, starting from the architectural level until the devices, a wide range of current technologies is labelled “IoT”. Regarding architectures, several public funded projects, especially in the EU, have attempted to set common reference models and/or architectures. The EU project IoT-A produced a publicly available deliverable highlighting in details the IoT state of the art (IoT-A, 2011). In general, for IoT Architecture we mean an integration of heterogeneous wireless sensor and actuator networks (WS&AN) into a common framework of global scale and made available to services and applications via universal service interfaces. The EU project SENSEI aimed at creating an open, business driven architecture addressing the scalability problems for a large number of globally distributed WS&AN devices.

To enable RFID and EPCGlobal standard solutions in practice, technical, social and educational constraints - particularly in the area of security must be overcome. BRIDGE (Building Radio Frequency Identification solutions for the Global Environment) addresses these problems by extending the EPC network architecture (Bridge, 2011). This is done by researching, developing and implementing tools that will enable the deployment of EPCGlobal applications in Europe. The *enablement* is mostly in the development of security apparatus, both in hardware, software and business practises.

The Cross Ubiquitous Platform (CUBIQ) project aims to develop a common platform that facilitates the development of context-aware applications (CUBIQ, 2010). The idea is to provide an integrated platform that offers unified data access, processing and service federation on top of existing, heterogeneous ubiquitous services. The CUBIQ architecture consists of three layers: (1) a data resource layer, (2) an intra-context processing layer and (3) an inter-context processing layer. The data resource layer provides transparent data access and handles mobility, migration, replication, concurrency, faults and persistence. The intra-context layer provides data processing services. The inter-context processing layer is responsible for service composition. The CUBIQ architecture provides interfaces for each layer (Dempo, 2010).

Beside the results coming from those research efforts, there are several architectures currently used in several commercial products. Zigbee developed by the Zigbee Alliance is probably the most popular one, as it is a simpler, more scalable alternative to Bluetooth (Ashton, 2009).

WirelessHART, extension of the popular HART (Highway Addressable Remote Transducer) communication technology, provides several features such as security and robustness, but provides no interoperability with other communication technologies because of its single-purpose philosophy (Mindtech, 2009; Song, 2008).

Sun SPOTs are a platform from Sun Microsystems for the development of sensor networks and embedded systems. Sun SPOT is an acronym that stands for Sun Small Programmable Object Technology (Sunspot, 2010).

Representational state transfer (REST) is a coordinated set of architectural constraints that attempts to minimize latency and network communication, while at the same time maximizing the independence and scalability of component implementations. This is achieved by placing constraints on connector semantics, where other styles have focused on component semantics (Fielding, 2000). REST enables the caching and reuse of interactions, dynamic substitutability of components, and processing of actions by intermediaries, in order to meet the needs of an Internet-scale distributed hypermedia system. REST elaborates only those portions of the architecture that are considered essential for Internet-scale distributed hypermedia interaction.

Regarding communication protocols, several solutions have been developed to overcome the limitations of current network technologies. Stream Control Transmission Protocol (SCTP) is an IETF proposed standard protocol for the transport layer. It is designed to eventually replace TCP and perhaps also UDP (Stewart, 2000). Like TCP, SCTP is reliable but offers new features such as multi-streaming and multi-homing. In particular, the multi-homing feature of SCTP enables it to be used for mobility support, without any special router agents in the network. Other features included in SCTP are error-free and non-duplicated data transfer, network-level fault tolerance through supporting of multi-homing, and resistance to flooding or masquerade attacks.

The Host Identity Protocol (HIP) is a solution that locates the mobility between the network and transport layers (Moskowitz, 2006). HIP introduces a new Host Identity layer (layer 3.5) between the IP layer (layer 3) and the upper layers. The reason for this is to avoid the situation where binding sockets to IP addresses forces the address into a dual role of endpoint and forwarding identifier. In HIP, upper layer sockets are bound to Host Identities (HI, identifiers) instead of IP addresses. In addition, the binding of these host identities to IP addresses (the locators) is done dynamically. The purpose of HI is to support trust between systems, enhance mobility, and greatly reduce the Denial-of-Service (DoS) attacks.

The Mobile IP protocol is an IETF proposed standard that provides a network layer solution to node mobility across IPv4 (Mobile IPv4, Perkins, 2002) and IPv6 networks (Mobile IPv6, Johnson, 2004). Mobile IP allows a node to change its point of attachment to the Internet without needing to change its IP address. This is not simply a configuration simplification, but can facilitate continuous application-level connectivity as the node moves from point to point.

Using Mobile IP, it is possible to move a single IP device from point to point on the Internet without losing higher level connections. However, with the proliferation of IP and the desire to always remain connected to the Internet, we are seeing entire networks of IP devices moving together from one place to another. It is possible to enable mobility for all of these devices using standard Mobile IP; however, this would require all devices to be capable of Mobile IP and generate excess overhead as every device would have to perform Mobile IP functions.

Another solution to the problem is Network Mobility (NEMO) that works by moving the mobility functionality from Mobile IP mobile nodes to a moving network's router (Devarapalli, 2005). The router is able to change its attachment point to the Internet in a manner that is transparent to attached nodes. NEMO is an extension of Mobile IP that enables an entire network to change its attachment point to the Internet.

In the IoT domain, smart objects and services exploiting them are distributed globally. Thus, there must be a sort of identification and resolution infrastructure to discover and lookup the services that allow accessing information about smart objects as well as controlling them. Resource Identification can essentially encompass both the naming and addressing of a resource, or either of them. In the Web, the identification of a resource that represents some form of information has been achieved by the development of the 'Universal Resource Identifier' (URI) [W3, 2004], which is a global agreement on the identification of a particular resource based on specified schemes. In IoT, similar to the Internet and the Web, objects and resources need to have common naming and addressing schemes and also discovery services to enable global reference and access to them.

In SENSEI, the resource ID is formed through a concatenation of several parameters; the domain of resource's provider, the type of device, a name representative of the resource's function, and a unique identifier that differentiates the resource from others of the same device type (Much-Ellingsen, 2011). In the Ubiquitous ID (uID), framework identification is represented by the 'uCode', which is a unique identifier for either physical or logical entities. The uCode itself is a 128-bit number that has no relationship to what it represents, but rather the relationship is retrieved from dedicated database servers. The structure of the uCode is formed in a manner to support its management (uID, 2011).

In the field of RFIDs, EPCglobal have promoted the adoption and standardization of Electronic Product Code (EPC), which has been used as a means of uniquely identifying RFID tags (EPCglobal, 2005). It is based on the URI model. ID@URI developed by the DIALOG research project is also another identification model that takes the same properties of the EPC/ONS standard but can also be manifested in barcodes as well (Dialog, 2011).

3.2 The Internet in the Internet of Things

Whatever the perspective, however, there is a need for substantial progress in research achievements in several fields. Firstly, today there is no single way of identifying an object in the Internet of Things: there are several standards, such as 2-D bar codes, GS1, uID, IPv6 addresses, but they are non-compatible. Moreover, reference architectures which can lead the way to any kind of real-life system implementation must be identified and standardised. As well, security mechanisms should ensure reasonable safety and privacy properties. Communication protocols, from physical layer to interfaces with services and applications, need substantial advances in order to leverage the upcoming of any IoT vision. The above are just a few examples of areas of research that need substantial development in the coming five to 10 years.

Within the “internet” side of IoT, which is dealing with communication between objects, there is a need to develop a convergence between different communication means. Today, several communication mechanisms, as shown in the table 1, are deployed in current applications, and any novel technologies will need to guarantee interoperability between different protocols. We must also consider that the lifetime of network technologies might be much shorter than the one of the physical objects connected to it, where that same technology is applied. In the ’common’ internet, the interoperability between low-layers technology and services is assured by the use of the Internet Protocol (IP). Usually, the network technologies are represented in an hourglass shape, with the IP layer in the middle, and this is commonly referred as ’the narrow waist’ of internet. The questions of what shape the IoT ’narrow waist’ will have - and even if such a thing will exist considering the heterogeneity of IoT technologies - are of primary importance, and future research should clearly focus on them. Just to make an example of the complexity we face, if we describe the communication layers in the classic way, we could imagine a ’thin layer’, just below the service and application layers and above all the different technologies used to transfer information, as the glue of different solutions developed for a specific target using very specific technologies. However, such a solution is clearly simplistic, as we would then need high-level gateways between different technology silos, and this would not make any sense from not only from the technological point of view, but first and foremost from the economical point of view.

Regarding security issues of communicating objects, a significant research effort has been undertaken on cryptography tailored for low-cost, low-throughput, and resource-constraint devices. This domain has been referred to as ’light-weight cryptography’, and has produced a number of new protocols that have been proposed for small devices, such as RFID tags (Internet Security Group, 2011). In spite of the large number of available methods, there are very few which have been examined enough to be considered safe.

In the past years, a few light cryptography algorithms that have been widely deployed were proven vulnerable such as, for instance, the well known case of MiFare Crypto-1 (Garcia, de Konig Gans, Muijrers, van Rossum et al, 2005). The development of light cryptography standards is paramount for the wide-spread adoption of IoT technologies.

In addition, the combination of lightweight cryptography protocols for use of light duty devices and regular cryptography framework such as Public Key Infrastructure (PKI) for back-end infrastructures should be analyzed. A very important consideration in this is key management: such a holistic framework should identify the actors generating the encryption keys, in case of private/public keys schemes, how these will be distributed and who (which agencies/companies/authorities) will eventually be given access to such keys when necessary.

In the table 2, we will produce a synthesis of common threats per network communication layer, to give the reader an initial idea of the vulnerabilities that IoT systems face.

3.3 Breaking the Unbreakable: The End-to-End Principle

The internet as we know today is based on a few, very simple and very meaningful principles. One of those is the "end-to-end" principle: keeping the technologies in the network very

Physical Communication interface type	Communication type	Protocols	OSI Layers
802.15.X Series (ZigBee, Bluetooth, RFID, etc.)	Wireless	NWK/APS/API defined by each standardisation body (all non-IP)	Network/Transport/upper
WiFi	Wireless	IP/TCP-UDP	Network/Transport/upper
UWB	Wireless	Baseband/LinkManager/L2CAP (non-IP)	Network/Transport/upper
Sensor network busses (e.g., CAN, Profibus, etc.)	Fixed	Up to data link	Data Link
Serial	Fixed	Up to data Link	Data Link
USB	Fixed, Wireless	Up to Data Link	Data Link
DeviceNet	Fixed	DeviceNet network and transport	Network/Transport/upper
ControlNet	Fixed	ControlNet network and transport	Network/Transport/upper
Ethernet/IP	Fixed	IP/TCP-UDP	Network/Transport/upper
Power line (KNX, LonWorks)	Fixed	Network/transport layers according Network layer/Transport to KNX and LonWorks specifications	Network/Transport

Table 1: Protocols of popular physical communication interfaces exploited by communication-enabled objects

Layer	Threat	Requirements	Targets	Approaches
Transport	Ping/ICMP flood	attacker being part of the network, ICMP	All connected devices	
	Synflood	TCP, attacker being part of the network	All connected devices	
Network	Neighbor discovery attack	Neighbor Discovery protocol	Networks using unauthenticated ND protocol	Authentication support for ND protocols
	Wormhole	Mesh networking	Multihop wireless networks	Specific hardware, time constraints on packet delivery
	Black hole	Attacker being part of the network	Multihop wireless networks	Don't use plain distance-vector based protocols.
Link	Spoofing	-	All networks, especially wireless	Packet authentication
	Eavesdropping	-	Wireless networks	Encryption
	DoS - Collision	-	Wireless networks	Use UWB, increase datarate
	DoS - Exhaustion	-	Embedded wireless networks	Link-layer Intrusion detection
	Replay protection att.	Replay protection	Multihop wireless networks	RANBAR, Tesla

Table 2: Network Layers and Common Threats

simple and dealing with complexity at the end points only, allowed the internet architecture to be very scalable (Carpenter, 1996).

With regards to the IoT domain, there might be a different point of view. It has to be considered up to what extent IP technology will be used. While many technologists believe that IP will finally be on each and every smart device there are two particular cases which show the likeliness that different solutions are necessary. Firstly, real-time devices, such as braking systems in cars, which cannot be based on best-effort, connectionless, unreliable protocol (as the IP is, by definition) (Ipso, 2011). Secondly, tiny, extremely cheap devices, (such as passive RFID tags) which may be stateless, and therefore cannot use complex protocols such as IP.

Moreover, it is questionable if the end-to-end principle can (and will) be used in the IoT domain. As the end points of IoT can be extremely simple (as a temperature sensor), even if they will be able to use the IP protocol it is unlikely that they will be able to deal with complexity. Moreover, smart devices do not necessarily need to speak the same language: a medical device such as a Nano robot used to fight cancer cells in the human body has totally different needs than those of a smart fabric needing to communicate its characteristics to a washing machine. Therefore, it is likely that, at some layer, there will be bridges between systems; and these bridges (or gateways) might be considered the end-to-end points between communicating entities. In other words, between two different objects communicating, the communication path may be broken into different sections (object-to-gateway, gateway-to-gateway, and gateway-to-object). As this is considered a "curse" in today's internet, and is likely to be a highly controversial topic, there is a strong need to further investigate this matter, and to come up with a commonly accepted set of founding principles.

3.4 The Things in the Internet of Things

With regard to smart objects, there seem to be the two main research axes to be developed: energy harvesting and conservation, and integration of smart components into materials.

Regarding energy, in all its phases of harvesting, conservation and consumption, there is a need to develop solutions with the objective of developing a level of entropy as close as possible to zero. Common objects, such a mobile phone, should be able to harvest the energy they need, whether by photo-voltaic cells, or transforming the vibrations and motion into electric energy. Current technology development is inadequate in this respect and existing processing power and energy capacity is too low to cope with future needs. The development of new and more efficient and compact energy storage sources such as batteries, fuel cells, and printed/polymer batteries, as well as new energy generation devices coupling energy transmission methods or energy harvesting using energy conversion, will be the key factors for the roll out of autonomous wireless smart systems, which will be the backbone of IoT.

The second axe of technological development in the area of smart objects, however, is one step further. The integration of chips and antennas into non-standard substrates, such as textiles and paper, will become mainstream technologies in the coming years. Metal laminates and new substrates based on polymer with conducting paths and bonding materials, better adapted to harsh environments and environmentally friendly disposal will become as commonplace as silicon is today. RFID inlays will be used to connect the integrated circuit chip and antenna in order to produce a variety of shapes and sizes of labels, instead of direct mounting. Inductive or capacitive coupling of specifically designed strap-like antennas will avoid galvanic interconnection and thus increase reliability and allow even faster production processes. The target must be to physically integrate the RFID structure with the material of the object to be identified, in such a way as to enable the object to physically act as the antenna. Looking back few years ago, there was a huge hype in polymer RFID prototyping, with companies such as PolyIC[28] and Philips[29] demonstrating fully polymer RFID tags. In parallel, silicon ultra-thin structures, such as the Hitachi μ-chip[30], need to be developed, with regards not only to further miniaturisation, but especially to resistance to harsh environments and packaging, in order to be included in commonly used objects (Hitachi, 2007).

[28] (PolyIC, 2004): [Internet] Available from: http://www.printedelectronicsworld.com/articles/polyic-demonstrate-polymer-driven-rfid-tag-00000091.asp?sessionid=1 [Accessed 02 December 2011]

[29] (Philips, 2006): [Internet] Available from: http://www.rfidjournal.com/article/view/2139 [Accessed 02 December 2011]

[30] (Hitachi, 2007): [Internet] Available from: http://www.technovelgy.com/ct/Science-Fiction News.asp?NewsNum=939 [Accessed 02 December 2011]

4 Policy

The emergence of novel computing paradigms entailed in the Internet of Things stresses the necessity of having a sound policy agreements and strategies. Indeed, a policy debate on the IoT needs to include discussions on all technologies that enable this ’ecosystem.’ As applications and data run on hardware not under the direct control of the end user, a weak policy strategy is likely to jeopardise the added value of the distributed computing paradigm. Therefore, while on common desktops or ’island’ systems a strong security, often implemented by a firewall, was sufficient, the fact that the data is ’out there somewhere’ in the future IoT ecosystems, this necessitates all players define precise policies and regulations.

The foundations of privacy regulation were created 30 years ago when information technology was centralized and hierarchical. With a great deal of effort, one could ascertain who was collecting information, who controlled the information, and who one had to deal with to ensure that the information was being handled appropriately. That is no longer the case today. The tension between protecting privacy and enabling innovation in a distributed computing model must build upon important privacy principles that have emerged since the late 1970’s over the last thirty years. However, applying long standing privacy principles will be challenging in a world of distributed computing.

4.1 The Role of RFID

As we saw in the previous section, Radio Frequency Identification (RFID) technology is one of many IoT enabling identification technologies, and not necessarily the main one. In a sense, RFID represents a small aspect of the overall debate since the IoT will mainly consist of smart objects, including all forms of sensors, actuators, small devices connected together using radio technologies but also wired technologies. IoT applications will be used in a wide range of innovative areas like industrial automation, smart grids, smart cities, home and building automation to name a few. However, in order to be uniquely addressable, all smart objects will have some form of electro-magnetic identification, and RFID technologies will be likely used to ’tag’ every sort of manufactured item.

In the past years, the RFID domain was under the spotlight as it was often depicted as a mean to implement some sort of Orwellian *1984* scenario. Policy makers, through several different instruments such as the European RFID Expert Group, were urged to shape sustainable policies for protecting citizens’ privacy.

As IoT can be considered as an evolutionary process rather than something completely new, debates on RFID policies are of primary importance within the IoT domain. While RFID usage is still somehow limited, forecasts show that in the future billions of devices will be interconnected; latency in defining policies can have a terrific impact on privacy and security of end users and business. For instance, Cisco[31] foresees the IoT and the number of devices connected to the Internet will exceed the number of people populating the entire planet. That is not just smart phones and tablets; it is sensors enabling a smart grid,

[31] Evans, Dave 2010 Infographics [Internet] Available from: http://blogs.cisco.com/news/the-internet-of-things-infographic/ [Accessed 02 December 2011]

smarter transportation flows, and medical devices monitoring the health of cardiac patients, to name a few. Rather than always interacting with humans, sensors will be interacting with each other automatically, updating our daily schedules. Devices will, for the most part, be mitigated through local area networks.

While it is arguable that there is today a strong business case supporting independent communication of every tagged item, it is undeniable that missing or contradicting policy definitions can slow down the adoption of otherwise mature technologies.

4.2 Protecting Privacy and Enabling Innovation

A policy debate on the IoT needs to include discussions on all technologies that enable this ’ecosystem’. Such a broad multi-stakeholder discussion needs to include the importance of the transatlantic dialogue and be informed by the review of the EU Data Directive, and legislative and regulatory debate around privacy and mobile applications taking place in the United States and Europe. Global policy approaches need to avoid technology specific silos where specific technology is regulated separately. A broader technology policy approach that is horizontal in nature must be considered to include other important issues like cloud computing. Although there are self-evident societal benefits to individuals from this computing continuum, these ’smart connected’ devices present privacy and security challenges, as well as opportunities, which require an examination of the underpinning of the 1980 OECD[32] privacy guidelines known as the Fair Information Principles (FIPPS).

The core FIPPS address the following principles:

Notice/Awareness: The most fundamental principle is notice. Consumers should be given notice of an entity’s information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.

While the scope and content of notice will depend on the entity’s substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information of the following:

- the entity that is collecting the data;
- the uses to which the data will be put;
- any potential recipients of the data;
- the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);
- the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and

[32] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Background

- steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

Choice/Consent: The second widely-accepted core principle of fair information practice is consumer choice or consent. At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information, uses beyond those necessary to complete the contemplated transaction.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a web site, thus effectively eliminating any need for default rules.

Access: Access is the third core principle. It refers to an individual's ability both to access data about self - i.e., to view the data in an entity's files - and to contest that data's accuracy and completeness.

Security: The fourth widely accepted principle is that data be accurate and secure.

Enforcement: It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.

EU Proportionality and Transparency: One of the privacy concerns most often expressed by the public are the IoT will be used to secretly track individuals. There is fear the technology will allow collection of personal data without the individual's knowledge or consent. In order to address this privacy concern, the European principles of “proportionality” and “transparency” should be applied to the IoT. “Proportionality” in this context requires a balanced analysis of assessing risk and mitigating risk based upon threat to privacy. If the implementation is “proportionate”, then the implementing entity should provide “transparency” thereby ensuring the IoT is not secretly used to collect data.

Reasonable and Adequate Notification: In order to achieve transparency, individuals should receive reasonable and appropriate notification of the type of data collected and how the data will be shared and used. Achieving “reasonable” and “appropriate” notification should vary based upon the type of data collected.

IoT implementation should consider whether the ability to be disabled at some point (e.g., the right to be forgotten)[33] or the right to the silence of the chips.[34] Both these concepts are being reviewed within the context of the on going review of the EU Data Directive. The determination to disable should be made by focusing on whether disabling (e.g., a kill tag) is necessary to mitigate real risks to individuals. For example, an RFID tag in an item which an individual will carry with them consistently (e.g., a watch) may provide less risk, if it allows the individual to disable the tag. Conversely, a tag placed in product packaging which an individual will discard quickly; there is likely little need for the disable function.

4.3 Apply Existing Data Collection Privacy Requirements and Frameworks to the IoT

Like other technologies that collect personal data (e.g., behavioral advertising), the focus should be on ensuring only data related to achieving the stated business objective will be collected. Moreover, data collectors should make certain collected data will be protected with the same rigorous privacy standards applied to personal data collected from other sources.

This policy position shifts the focus away from the IoT and turns the focus to the broader issue of ensuring there are rigorous privacy data protection policies in place to protect all individual privacy data, regardless of the source of that data. Typically, these broader policy standards apply to how the data is stored and protected on the back-end, such as the database, where the data is stored, the processes used to manage and protect the collected data, and how the data is protected when shared with authorized third parties. For instance, many press articles have focused on risk scenarios that are unlikely or impossible (e.g., networks of readers which will track the location of individuals). Education can help reduce this fear. The IoT discussion should also be expanded beyond privacy issues to the broader societal benefits the IoT can deliver.

4.4 Unintended Consequences

Governmental regulations mandating the type of acceptable IoT technology have the potential to retard innovation and competitiveness in a global economy. Rather, the focus should be on a world-wide comprehensive approach to generate general privacy standards, rather than on regulating IoT technology. These standards should protect stored personal data, and controlled use of that data, regardless of the source. Finally, regulations should focus on punishing inappropriate behavior when an individual, company, or agency violates regulations that protect personal data and its use.

[33] Dou, Eva, Internet Privacy and "the right to be forgotten", Reuters March 17 [Internet] Available from: http://www.reuters.com/article/2011/03/17/us-eu-internet-privacy-idUSTRE72G48Z20110317 [Accessed 02 December 2011]

[34] 'Right to the silence of the chips' in the new EC Communication 1 July, 2009, EDRI-gram - Number 7.13, 1 July 2009 [Internet] Available from: http://www.edri.org/edri-gram/number7.13/right-silence-of-the-chips Accessed 02 December 2011]

4.5 Challenges in an IoT world

The application of these areas of policy raises a series of crucial questions. How will the principles of notice and choice apply? What does transparency mean and what is the right level? The challenges of providing access are especially pronounced if there is not a direct interaction with a particular device. How do we incorporate privacy by design into the initial design and manufacturing phase to consider/alleviate many of the privacy issues that connected devices might present? Can industry self-regulation and the FIPPs work for the IoT to form the foundation of global privacy laws and regulations?

4.6 Questions to Consider

- How will the principles of notice and choice or consent apply?
- What does transparency mean?
- How do we provide notice appropriate to circumstances to individuals when data is collected that may be associated with that individual?
- How do we avoid IoT specific government mandates to ensure continued technological innovation in the marketplace?

5 Scope and Impact

The above sections have demonstrated the importance of the IoT and its role in social life. In this section, we look more specifically at the current scope and potential impacts of the IoT. Weber argues that the increasing ubiquity of the IoT requires new regulatory approaches to ensure privacy and security. He asks "for a heterogeneous and differentiated legal framework that adequately takes into account the globalist, verticality, ubiquity and technicity of the IoT" (Weber, 2010). More specifically, some starting points come from a recent presentation at the Expert Group on IoT from the European Commission by Rudolf van der Berg of the OECD. According to van der Berg who spoke his personal opinions, there are several issues to consider in the near future:

- **Competition especially in the mobile wireless market:** Today, connectivity is provided by an oligarchy of operators, resistant to new players and often engaged in 'cosy competition' practices. Opening this sector to new and emerging players can empower the role of customers and provide a new class of services for the end users. For example, the role of customers is changing with car companies now managing more devices than there are citizens in some OECD countries. To foster competition, it would be good that these car companies can enter the wholesale market independently and buy and sell national and international roaming independently of operators.

- **Spectrum Policy:** The Internet of Things is here for the long haul. This also means it locks in spectrum use in the long run. IoT smart objects may not have an maximum expected operational life of 5 years not like consumer electronics. Some objects can last up to 30 years. Policy makers need to be aware of the long term effects.

- **Standardization:** Currently, the standardisation domain in the IoT field is fragmented. For example, there are also no uniform ways of connecting devices to gateways. We should avoid that bad, *de-facto* standards will take the lead over well superior technologies, because of commercial considerations.

- **Privacy:** IoT together with the cloud is about information. That information is about us, the way we interact with others. This information is stored and processed at different actors and layers than before. If you do not want your mobile phone to track you, you leave it at home. If you do not want your implanted pacemaker to tell where you are, you may have a problem. Your car will communicate the moment you turn it on.

- **Numbering policy:** A much overlooked area, but it determines who can get numbers and who can play in the market.

- **Public/private sector information:** With more information and better correlation everyone could become wiser, under what terms is data shared?

To these we can add:

- **Funding research:** Public funding can help streamline research, which is important as many of the application opportunities and technologies remain to be explored.

- **Governance:** Public authorities may wish having a say in the governance of the IoT. It remains however to be demonstrated that additional governance schemes are necessary.
- **Safety:** The main concern of end users might be the possible impact of IoT technologies on their health. Existing laws and regulations may be sufficient but it needs to be shown they exist and are adequate regarding electromagnetic frequencies.
- **Education:** There is a role for public authorities to educate businesses, public bodies and citizens about IoT, its constraints and benefits.
- **Dissemination:** Public authorities can promote IoT at large but more specifically the applications that can potentially bring the bigger benefits. This can be done by sponsoring pilots, events and documentation.
- **Recycling:** It remains to be proven whether the increasing use of tags and sensors deserves a special attention and the IoT's environmental impact needs to be considered in the long view with an aim towards biodegradable or recyclable components.
- **Global cooperation:** Needless to say, the large majority of IoT applications has and will have a global dimension. Public policies should always consider the big picture before addressing national and regional needs.

These categories can and should be the focus of attention by policy-makers as well as developers themselves. In the section below, we call attention to the current developmental approaches to the IoT, using China, the EU, and the US as examples. We follow this up with a general categorization of these and similar approaches, claiming that more proactive forms of governance and policy setting are required. We end with some conceptual arguments from the growing field of *infrastructure studies* which provide guidance for a more nuanced attention to the complexities of the IoT policy space, and one use case: privacy.

5.1 Development Approaches

A quick analysis of the current state of IoT globally shows three approaches aiming to build - more or less - governance reference architectures that offer a framework for decision making, as well as collaborative governing, tax systems, generic infrastructure, legal frameworks and resilience. These are:

1. An **integrated approach**, for example in China, is able to steer on broad investments in infrastructure, smart cities, software, applications and services. The 2006 RFID white paper was released by a total of 15 Ministries and Commissions, including Ministry of Science and Technology of PRC. Premier Wen Jiabao proclaimed the city of Wuxi as China's IoT capital and called for the rapid development of internet of things technologies. Therefore, the IoT can be claimed in the Chinese notion of "Sensing Planet" as "original" as any other vision available. It is able to integrate IoT fully into its technical architecture of the future internet. There are on going sensor projects in Wuxi and the

city's mayor proclaimed the 530 Project with his aim to bring 30 IoT entrepreneurs to Wuxi within five years. Start-ups are supported and given free office spaces in Wuxi to promote growth in the region and on IoT. It is interesting to see the interest in China for a bottom-up approach with regard to facilitating discussion at local levels; deliberative democracy. How this could be linked to the Sensing Planet idea is uncertain. "Whether widespread Deliberative Polling would contribute to democratization in China is an open question [. . .] But it can promote the notions that government can be responsive to public needs and that citizens can voice their views in a context of equality and mutual respect." (Fishkin, 2006).

2. A **stakeholder approach** in the EU favors public-private partnerships and vertical investments through four-year programme plans. This organizes internal competition, even between its own flagship projects, while aligning major IoT projects with Future Internet is not yet a dedicated goal. This approach aims to bring a broad adoption of potentially privacy-invading and business disruptive IoT as a set of applications. These should bring convenience, safety, and cost efficiency to the domains of health, automotive, smart energy grids, and the home. In order to do this, the EU has set up risk assessment procedures (Privacy Impact Assessment for RFID, Internet of Things Impact Assessment forms IoT) with a broad and wide variety of stakeholders (the RFID and IoT Expert Group).

3. An **opportunity investment approach** in the US is driven by short to mid-term return on investment. It is pushed by smart energy, smart cities, and RFID fuelled by Department of Defence and Wal-Mart. Big data, the cloud and the growing synergies of B2B and B2C, through social media networks, lead to a convergence of back-end and real services and applications: location-based services and augmented reality (e.g., Facebook buying Nextstop, smart energy to the home and community applets (LogMeIn buying Pachube), (NFC) handheld device integration (Google buying Motorola). There is no US wide federal policy, nor an EU style stakeholder debate. Large opportunities exist at local and city level where local decision power is harnessed, and there is an appreciable amount of 'buzz' in this area.

The above approaches each have strengths and weaknesses. They each balance important issues of technical stability, security and privacy, with the need to maintain and extend innovative programs. However, it is not clear to what extent the three approaches listed above currently incorporate and make use of new peer-to-peer developments. To what extent do the approaches all fail to take the citizen - the end user - into account as a new systemic force? Key research questions center around the changing roles and power relations between informed citizens and institutions of governance. Just as novel socio-technical development such as crowd-sourcing and commons-based peer production have had dramatic effects on previous expert communities and their products (e.g., encyclopedias, software, media production,) so too such practices and communities could have a dramatic effect on the development of the IoT (Benkler, 2006).

In addition, how do these approaches address the growing importance of open data, particularly by SMEs, and by regional and municipal governments, some of the most important customers for the IoT? The Open Data movement aims to open up data that have been collected, acquired and stored by public funds and means is growing. "Take data that you and I have already paid a government agency to collect, and post it online in a way that computer programmers can easily use. Then wait a few months. Voilà! The private sector gets busy, creating Web sites and smartphone apps that reformat the information in ways that are helpful to consumers, workers and companies" (Thaler, 2011).

In the past eighteen years of the browser, we have seen a trend towards collaboration and sharing. We have gone from text and images towards building new operating systems, open hardware (OpenBTS, OpenBSC, Oswash) and even an open Global Village Construction Set (50 tools for building post-scarcity, resilient communities). It is hard to find one city that is not involved in open government projects or open data schemes. So far these open projects have required little resources, but we are now reaching a milestone where this technology will be used to transform future cities. IBM's City Forward is a philanthropic donation of services and technology urging citizens to "use data and visualizations to come up with new ideas and share them with others." Eduardo Paes, Mayor of Rio de Janeiro, has asked IBM to build a 'Single City Operations Center' that would allow him to ”monitor, command, & forecast critical events across the city[35].” Guru Banavar of IBM's Smarter Cities group says: “This is a very special thing for IBM, because we're seen as a trusted adviser by the mayor - not a vendor, not even a partner.“ Addressing the need for open data by many of the potential customers of IoT systems is an important priority, but presents privacy risks.

One of the main research questions in the next decade involves the exploration of citizenship in a digitally-enabled world. How can we help existing institutions and power nodes to transform into a networked form of a variety of heterogeneous forms of organisation that need mediation? Might we not be able to facilitate citizens with the individual and community tools that are necessary to perform the functions of current institutions and democratic processes: slow down, mediate, negotiate, educate, take a long term perspective[36].

5.2 Moving Beyond a Reactive Approach to Governance

From the previous chapters we can look towards IoT from 4 different perspectives:

1. A value chain where all objects can be tracked, logged and traced.
2. A service layer will be built on this, currently mostly by mobile operators who will be offering filtering layer deals to customers just as they do now with sms/gsm.
3. On top of this layer - and currently interwoven in it through the public private partnerships - we find the smart city layer.
4. The ultimate limit and scope of the Sensing Planet notion is to capture natural processes by globally distributed sensor grids to have counterpart in the cloud.

[35] Arkenberg, Chris 2011 Rio de Janeiro partners with IBM to build a smarter city [Internet] Available from: http://www.psfk.com/2010/12/rio-de-janeiro-partners-with-ibm-to-build-a-smarter-city.html Accessed 02 December 2011]

[36] Nold, C. van Kranenburg R. (2011) The internet of people for a post-oil world. New York: Architectural League of New York.

In each and every one of these layers, key issues are or have emerged. In the value chain, the debate is about the possibility of a global value chain at all, who should facilitate and provide governance, what technical protocols could form this ecology. Tentative solutions have also emerged, such as federated EPC Global ONS trials in France (cf. Chapter 2). Privacy and security are the main issue in the applications and services domain. The Privacy Impact Assessment (PIA, below) is a unique combination of industry led and policy backed instrument that was negotiated by a wide variety of stakeholders in the RFID expert group. Then smart city concept is the actualization of the need of different layers of governing (EU, national, and regional) to find funding for infrastructural work with sensor based infrastructure. Maintaining control and governance in a fuzzy, dynamic environment is the key driver behind the Sensing Planet idea and FP7 Security. This has led to a broader diffusion of the Open Data movement in contrast to the control notion that builds closed systems.

At this time, it is possible to take one or two differing approaches to governance and investments, a reactive approach or a proactive one.

The *reactive approach* takes a defensive approach and sees Internet of Things as a manageable technological series of developments. Addressing the issues from the current economic and socio-cultural realities, it aims to manage the ’extra’ connectivity that IoT brings, assuming that this ’extra’ will not change the basic elements of the economic, socio-cultural and political realities. Against such an approach, Santucci argues that "the main problem today, and especially tomorrow, is not only to determine if and how we’ll preserve our right to privacy but what will be the place of human beings in a society in which the largest population will be the one made of smart objects enabled by ICT with the attributes of "subjects" (Santucci, 2011).

Alternatively, a *proactive approach* confronts Internet of Things as an existing and rapidly innovating set of devices, protocols and systems which works back from that situation to the current political, economic and socio- cultural realities. Based on this idea, it becomes obvious that individuals as well as social groups need to be educated into the realities involved in sharing decision-making with autonomous M2M operations. Possible results include the failures of existing business types as well as the development of new business opportunities. Current democratic processes could be severely disrupted and/or new approaches to political participation may be engendered. Here, the main question is whether or not the current groups studying global IoT Governance and specifically the Dynamic Coalition on IoT are able to act pro-actively to shape the scope and import of IoT[37] In this final section, we explore the cornerstones for a proactive approach seeing these as involving attention to inclusive designs for IoT services for the home, transportation and energy, and the city. We will then describe relevant work on the nature of infrastructure that provides some guidance towards a useful analytic model of IoT and end with an example of such an analysis focusing on privacy.

[37] The Global Standards Initiative on Internet of Things (IoT-GSI) promotes a unified approach in ITU-T for development of technical standards (Recommendations) enabling the Internet of Things on a global scale. ITU-T Recommendations developed under the IoT-GSI by the various ITU-T Questions - in collaboration with other standards developing organizations (SDOs) âĂŞ will enable worldwide service providers to offer the wide range of services expected by this technology.ÂăGSI alsoÂăaims to act as an umbrella for IoT standards development worldwide.

5.3 Inclusive Designs for IoT Services

The need for a proactive and inclusive approach to the IoT is clear. Three examples are given below of its importance, each of which emphasizes different needs and issues.

Home: The house will be the key focus for eHealth and the ageing European population. It will become an ’actor’ trying "to maximise the comfort of each of its inhabitants by learning the individual preference profiles" (Internet of Things 2020 Roadmap). The biggest challenge is that of balancing security with convenience for such uses and at-risk users. The number of general- and specific-purpose devices connected to the internet, either directly or through a gateway is growing exponentially.[38] One can only wonder how to adequately share and sort through the devices and their data reliably and conveniently, yet securely. This is even more of a challenge when considering the countless respective individual and corporate needs. This situation requires a flexible and Open Source combination of hardware, software and protocols to be designed and implemented.

Transportation: Rudolf van der Berg of the OECD proposes that car companies will enter the wholesale market independently and buy and sell national and international roaming independently of operators. Social and mobile technologies will transform the car ownership experience. (Toyota press release, 2011). Again, security will be a key focus. Another impetus is electrified vehicles (EV) for application in the urban environment; research should focus on the development of smart infrastructures, and innovative solutions which will permit full EV integration in the urban road systems while facilitating evolution in customer acceptance" (2011 FP7 Call GC.SST.2012.1-2. Smart infrastructures and innovative services for electric vehicles in the urban grid and road environment). In September 2011, the Commission adopted the first measure towards the mandatory introduction of eCall. It will dial 112 for you automatically when the sensors detect a serious accident, sending a so-called "Minimum Set of Data" with key information about the incident. The study report on automated driving, cooperative driving, and autonomous driving concludes that "a more concrete standardization program will certainly help the industry, the regulators, and the road infrastructure owners to take the right decisions in due time and avoid thereby undesired costs introduced by uncertainties in their business models" (SMART 2010/0064).

City: The Nikkei Business Publications estimates that smart city market will be a cumulative total of 3.1 trillion Euro for the next 20 years (Smart Connected Communities, 2011).

[38] For example, the Herma box will bridge home-based data providers to roaming users and global consumers, like smart-grid platforms. It will be a ’gatewall’: it will act like a firewall when necessary and a gateway by default. It aims to provide different APIs depending on the consumer, be it a home appliance or a corporate environment, including ISPs or energy and media suppliers (probably ’one’ service layer in the near future). The box developed in this project can also be a base for an IoT label, which could in turn be extended to other Things. With this working it would provide a gateway to a more industrial, yet open, hackable and eco-friendly home environment, as a potential plug to other dedicated services and open hardware modular items: washing machines, coffee machines, power monitoring tools to share locally and globally. For technical details: [Internet] Available from: http://herma.duekin.com/Accessed 02 December 2011] /

According to Intelligent Community Forum, more than 500 cities globally have been introduced with 'smart' technologies. For example, the following cities being created are: Neapolis, Cyprus; Songdo and Incheon, South Korea; King Abdullah Economic City, Saudi Arabia; GIFT, Lavasa, and Nano City, India; Wuxi, Huishan and Meixi, China; Masdar, UAE; Living PlanIT Valley, Portugal; and Skolkovo, Russia. However, it is not clear how cities will adopt new IoT infrastructures. As Bruce Katz argues in Smart Cities USA:

> *"Instead of cashing in on what could be a $1.2 trillion industry, our patchwork collection of local, city, and state governments fight over who should pay to update our infrastructure. This needs to stop. The United States would seem tailor made for this market transformation. One of the most urbanized countries in the world; cities and metropolitan areas house over 83% of the population and generate 90% of national GDP. US companies (and the US military) have been innovative leaders in the invention of technologies critical to making cities smart. Despite these natural advantages, the US lags rather than leads the move towards smart cities technologies at scale when supported by strong public policies." at the national scale. [. . .] The most important barrier; however, to US leadership may be institutional fragmentation. [. . .] An excess of municipal governments (and the general absence of metropolitan governments) means that there is no 'one stop shop' for the application of innovative technologies in American cities and metropolitan areas*[39]

Alex Bassi, in developing the term 'cityness', claims that in order to develop a coherent, synergistic vision of the cities of tomorrow we need to have a multi-stakeholders approach: cities will have to be places where people not only live but enjoy to live, where work, leisure, residential, commercial areas will merge in harmony. The vision must be developed together by urbanites, sociologists, artists, and technology people. Therefore, we need a multi-cultural and multi-stakeholders approach, to start a movement that aims to the identification of sustainable development paths for our cities.[40]

5.4 How to Analyze IoT - Some Conceptual Guidance

How might policy-makers, technology developers, and interested citizens parse the IoT in a way that allows them to address its complexity? While technical values such as functionality and ease-of-use can guide initial development, social values more associated with political action and citizen rights may be more appropriate in the longer term. We can imagine that values such as transparency, interoperability and openness will be important, just as they have been for the development of the internet itself.

[39] Katz, Bruce, Why the U.S. Government Should Embrace Smart Cities [Internet] Available from: http://www.brookings.edu/opinions/2011/0726_cities_katz.aspx/Accessed 02 December 2011] /

[40] Alex Bassi, Cityness [Internet] Available from: http://www.theinternetofthings.eu/content/alessandro-bassi-cityness Accessed 02 December 2011].

Some assistance can be gained by consulting a new and growing field of social research. Infrastructure Studies, a cross-disciplinary research area includes researchers from Information, Sociology, Political Science, and Computer Science. Together these researcher's goal is to develop case studies on infrastructure as well as novel methods for unpacking its importance for social life. Three insights from this field are most relevant here:

- Infrastructure is relative: one person's helper is another's hindrance.
- Infrastructure is socio-technical and made up of technical apparatus, institutions and social groups, as well as individual practices.
- There is both a tendency for infrastructures to become invisible as well as the simultaneous need to reveal them, given their importance.[41]

First, it is important to recognize that infrastructures are not experienced the same by all individuals and groups. This relativity was first noted by Star and Ruhleder[42] who described the ways in which infrastructures are learned by individuals as they become members of particular communities. For members of these groups, infrastructures become naturalized, for newcomers and strangers, they are encountered at best as unfamiliar objects to be learned and at worst as barriers to activity.

Second, infrastructure is best considered as a hybrid of social practices, institutions and communities, as well as technical objects, Here, infrastructure scholars leverage work from Science and Technology Studies[43] to unpack the complexly interwoven nature of infrastructures in daily lives. Any attempt to understand and govern the IoT as an infrastructure should start from a similar understanding.

One of the main questions in IoT research in the next decade will be of informing the intellectual, technological and cultural elites to formulate in inter-subjective and pragmatic ways: How can we help existing institutions and power nodes to transform into a networked form of a variety of heterogeneous forms of organisation that need mediation? Might we not be able to facilitate citizens with the individual and community tools that are necessary to perform the functions of current institutions and democratic processes: slow down, mediate, negotiate, educate, take a long term perspective...?

There is thus great value in considering the IoT from the perspective of infrastructure. It is obviously experienced 'relatively' with some users finding it easy or even invisibly assisting them, while others will have more difficulty. The IoT is also socio-technical rather than 'purely' a technical apparatus. Lastly, the IoT is both necessarily and problematically invisible. In fact, if we consider the rhetoric associated with the trajectory from Ubiquitous Computing to Pervasive Computing to Ambient Intelligence, to the Internet of Things, it appears to involve

[41] For more readings in this area, a good starting point is Bowker, G., Baker, K., Milerand, F., Ribes, D., Hunsunger, J., Allen, M., & Klasrup, L. (2009). Towards Information Infrastructure Studies: Ways of Knowing in a Networked Environment. Springer Verlag.

[42] Star, S. L., and Ruhleder, K. 1996. Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. Information Systems Research, 7, 111-133.

[43] Here, the work of scholars such as Susan Leigh Star, Geoffrey Bowker, Steve Shapin, Simon Schaeffer, Bruno Latour, Trevor Pinch, and many others in particularly relevant. For an introduction to some of this work, see Sismondo, S. (2009). An Introduction to Science and Technology Studies (2nd ed.). Wiley-Blackwell.

the movement of computational resources more and more into the background, with less and less human involvement in the processes of computational decision-making and environmental sensing and control. One way to consider the IoT is as a paradigm for computing in which humans have left the scene entirely. As Nold and van Kranenburg have argued, this is an incorrect vision.[44] Overcoming and replacing this vision with one that emphasizes open standards, shared development, and inclusive designs will encourage innovation while maintaining the social values which have informed the development of the internet requires human attention.

[44] Christian Nold and Rob van Kranenburg (2011) The Internet of People for a Post-Oil World, Situated Technologies Pamphlets 8: Spring 2011.

6 Use case: Privacy

“We cannot innovate in a bubble if citizens are not coming along for the journey”, Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, stated in her opening for the High-level Internet of Things conference ’As the IoT matures into the connected society’, Budapest, 16th May 2011:

> *“Whether it is Smart Cities, eHealth and Assisted Living, Intelligent Manufacturing, Smart Logistics and Transport, or Smart Metering, 21st century machines are now sensing, anticipating, and responding to our needs; and we can control them remotely [. . .] We cannot have a policy or create the impression that the Internet of Things would create an Orwellian world. Our goal, and our commitment, should be to create a vision that focuses on providing real value for people.”*[45]

Policy, industry and democratic institutions have to face the consequences of growing groups of media and sensor literate individuals being able to organize themselves through the internet and through data gained from inexpensive sensors in the IoT. Balancing security and resilience with end user programming, convenience and innovation is a challenge to them all. Key research questions center on the changing roles and power relations between informed citizens and institutions. Which new notions of quality and formats of data, information and knowledge will inform decision making, governing and leadership? In the case of privacy these questions converge into an ever more growing debate that will dominate the level of public adoption of IoT.

A debate in the Netherlands on privacy and data protection was sparked by the introduction of the OV card, the RFID chip travel card - after it became known that the Mifare chip it contained was hacked, this did not stop the project. In 2009, the minister of economic affairs, Maria van der Hoeven, backed down from making the ’smart energy meter’ compulsory in the Netherlands after consumer groups raised privacy concerns[46]. However, Florian Michahelles and Andrea Girardelle discuss TwiPhone, a mobile app that posts mobile phone event data, such as time and caller ID, as well as SMS communication, including text contents, to Twitter. According to Girardello, this "essentially meaningless application, which seems nightmarish for privacy advocates, has surprisingly been downloaded by several thousand Android users". It is used by several hundred people whose conversations can be publicly retrieved on Twitter using the #twiphone hashtag: “Do users not care about privacy anymore, or are they just unaware? Is privacy becoming an optional feature?” (Michahelles and Girardelle, 2010).

[45] [Internet] Available from: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=7008 [Accessed 02 December 2011]

[46] [Internet] Available from: http://vorige.nrc.nl/international/article2207260.ece/Smart_energy_meter_will_not_be_compulsory [Accessed 02 December 2011]

Working Group	Dilemma	Stakeholders	Path
1	What is IoT? General public does not know IoT	Society (user) & IoT community	Participation and user driven innovation
2	IoT is killing (simple/unskilled) jobs (self checkout)	Businesses & State/Society	Education
3	Sustainability/Energy	Manufacturers & User	IoT label (this is good for Energy, Home ...)
4	Privacy user is not aware of what is collected	Users & Data collectors	Circles of Trust & Transparency
5	Value = (benefit - cost) is very difficult to quantify	Government & Citizens	Open access to data & Self-education
6	Acceptance of IoT (10-15yrs ahead) & incentives	End users & Business	Making clear it's not just for tech people
7	Danger of losing control of your environment	End user & Business	Education & Respect

Table 3: Outcome of Workshop Groups 2011

In the IoT-Forum[47] Working Group Societal the following issues were the result of a brainstorm session among IoT experts. Privacy is affecting all layers and stakeholders:

6.1 A Reactive Approach: Issues to be Addressed

If we consider these outcomes and the IoT domain in its entirety, there are several risks to be addressed. Architectural and modelling issues such as addressed in Infrastructure Studies for the IoT are extremely important for its success. Internet became the global phenomenon we know today when a single technology, based on a very simple and straightforward architecture, became the standard: the TCP/IP protocol stack (Kale, 1991).

Without a clear communication model, it is doubtful that we would have had the internet revolution. Currently, we are in a situation similar to the internet infancy: the presence of vertical solutions, conceived to work in isolation for a specific application, is generating interoperability issues and slowing down the uptake of IoT technologies.

Orchestration, management and monitoring of devices are a very important field of research, as the number of interconnected objects is supposed to reach several hundred bil-

[47] [Internet] Available from: http://www.iot-forum.eu/events/launch event/programme/preliminary-programme [Accessed 02 December 2011]

lions (Jefferies 2007 and Clark, Partridge, Braden, Davie et al, 2005). Regarding security and privacy aspects, we can list at least two major ones, and explore the policy implications in detail further in this chapter.

In the IoT general domain, the collection of data and profiling are both demonstrable facts (Hildebrand, 2010; Langheinrich, 2009). We can interpret this as an intrusion in private life, implementing a kind-of "big brother" control, which gives a very negative perception. The intentions of data collection might be positive, as social sorting enables governments and companies to more efficiently provide services and to better target citizens who might be at risk. However, an excessive use of these technologies will inevitably lead to practices for commercial or other purposes, leading to exclusion of people from accessing services. Like re-purposing of data and mission creep, using information for purposes that go beyond the original reason for collecting them, social sorting is an increasing temptation with increasing data collection. Consumers groups targeted because they offer better commercial prospects inevitably means that other consumers are ignored or marginalised.

Social sorting enables many enterprises, such as insurance companies or airlines, to provide some deals to their valued customers and not to others. In the long run, social sorting risks damaging notions of equality and democracy.

Profiling and data mining within any IoT scenario is massively increased as a potential harm to individuals due to the ease to which data can be collected, stored, shared and analysed. Over-reliance on the content of databases (such as security related ones) may likewise be problematic in instances where mistakes are made. Individual access to remedy incorrect data being stored should be seen as a key goal yet it represents a challenge given the wide range of potential databases that might be in existence with the widespread implementation of IoT technologies and systems.

Furthermore, computer network infrastructure or process failures can lead to a major paralysis of the overall automated IoT vision of the future. This includes both the wired and wireless infrastructure as well as critical components such as routers or back-end servers. Many, if not all, sensors and readers require wired or wireless infrastructure to deliver their data. Additionally, any system may require network access to back-end servers. The current internet infrastructure is an integral part of providing future IoT services. Depending on the degree of computing network infrastructure failure, the impact to any kind of service, including life-threatening ones, could be severe.

An important factor that makes this failure even more severe and more likely is the excessive reliance on the technological infrastructure that is characteristic of this new envisaged environment. There may be an over-reliance on smart devices as the foundation of future IoT services. This can become evident in the event of an overall system failure due to compromise of these smart devices and loss of functionality due to wireless/IT infrastructure failure, equipment/reader malfunctions, theft, devices’ weak access control, jamming, and social engineering or cyber attacks.

Over-reliance may also become apparent with paralysis and interruption of the future process resulting from malfunction of critical technology components such as barcode scanners, RFID tags and RFID readers due to electro-magnetic interference, vibration and age. As in the case of authentication via biometric authentication, fingerprint and iris scanners may be ineffective to, say, elderly passengers or people with finger injury or damage. Such risks arise from non-malicious ’malfunction’ of biometric sensors and are facts of technology limitations. Manual processes have to be devised to address them.

Hard failures could result from hardware such as kiosks, terminals, readers, RFID malfunctions, virus attacks, denial-of-service/flood attacks or drive-by downloads of malicious code. Also, for portable devices, the battery could be discharged rendering the device useless.

Many of tomorrow’s facilities can and will be integrated with IoT of the future. For example, air conditioning/heating systems, as well as plumbing systems, can be integrated with various temperature, vibration or pressure sensors at strategic locations. Data from these sensors could be read or accessed through mobile RFID readers or smart phones. Under such circumstances, the physical failure of the facilities is tightly linked with the management of the IoT devices, in addition to risks arising from structural, electrical or terrorist causes.

Successfully addressing and prioritizing the above issues in a multistakeholder approach that tries to assess the disruptive qualities of emergent technologies such as IoT has been demonstrated in the EU process that led to the Privacy Impact Assessment of RFID.

6.2 Policy and Self Regulation: The RFID Privacy Impact Assessment Case

As we look into ways to address the Internet of Things from a political perspective, we do not need to go very far back in time to find a truly disruptive positive policy approach to technology developments and most importantly, to the resulting user applications. One example of that is the recent European policy approach to Radio Frequency Identification (RFID).

In 2006, Information Society Commissioner Vivian Reding announced the Commission’s intention to scrutinize RFID, identify its benefits and the societal and economic challenges it would pose[48]. The Commission opened a very broad and exhaustive debate on different policy aspects such as security, health, privacy, standardisation, environment, etc. The debate was highly publicized in the press, and all stakeholders had the opportunity to give their opinion through a public consultation and a series of workshops. At this stage, the policy positions were extremely reactive ones.

As a result of the intense debate, the European Commission developed it structured policy thinking around the subject, already outlining some sense of political direction on the matter through a Commission Communication.[49] The most effective guiding points of the Communication was the support for deepening the dialogue with all relevant stakeholders, best expressed through the creation of an RFID experts group, including representatives from governments, data protection authorities, companies, standard organizations consumer group

[48] Viviane Reding Member of the European Commission responsible for Information Society and Media RFID: Why we need a European policy EU RFID 2006 Conference: Heading for the Future Brussels, 16 October 2006 Reference: SPEECH/06/597 Date: 16/10/2006 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/06/597

[49] Recommendation on RFID European Commission
http://ec.europa.eu/information.../rfid/.../recommendationonrfid2009.pdf 12 May 2009 - The Commission Communication of 15 March 2007 ’Radio Frequency Identification. (RFID) in Europe: Steps towards a policy framework’2.

and privacy advocates. The focus on stakeholder dialogue was a key to turn a highly reactive debate into a proactive/constructive one. Stakeholder dialogue will be a constant through the years to follow and even today, as the RFID Experts Group evolved into a renovated Internet of Things Experts Group in 2010.

Looking back at those days of intensive exchanges of opinions, awareness raising and learning from each other's concerns and proposals, one can see why the Commission services in charge of the dossier decided not to sanction the results of the RFID dialogue into a one single binding piece of legislation, but came close to self-regulatory approaches by adopting a non-binding Recommendation in 2009[50]. The Recommendation on Privacy and Security Aspects of RFID was addressed to Member States, like previous recommendations, but included very precise instructions to industry and other stakeholders.

The RFID Industry's Privacy Impact Assessment Framework is the first result of that Commission Recommendation. It is a co-regulatory instrument supported by the European Commission, the National Data Protection Authorities and the Article 29 Working Party. Party[51]. It is the first instrument in the EU that includes a harm based approach, in other words, it does not focus on the technology itself but on the use of the technology and the ”likely” privacy risks (as opposed to the ”possible” risks) it entails in the context of the application of usage at stake; it is sufficiently flexible to be future proof and relies on making privacy principles enshrined in the current EU privacy regime effective.

6.3 A Proactive Approach: Issues to be Addressed

Taking into account the current innovation going on in IoT, we see a mismatch between the policy and legal frameworks on privacy and personal data and the actual design practices by the about 20 startups already providing real building blocks for IoT.[52]

The Information Society “can only be reliable if it is capable to construct, connect and nourish these rooms where doubting the promises of, ambient intelligence (AmL), is a habit. Being aware of the redesign of borders is a necessary act for creating diversity in interaction rooms - where people and society can choose how the invisible and visible can interact, where they can change their status, where the invisibility could be deconstructed” (Cecile Crutzen, 2006). Privacy Enhancing Technologies (PET) and ’privacy by design’ are thus proactive tools. The Privacy Coach, produced by a small Dutch consortium of RFID experts, is an application running on a mobile phone that supports customers in making privacy decisions when confronted with RFID tags (Broeninjk et al, 2011). It functions as a mediator between customer privacy preferences and corporate privacy policies, trying to find a match between the two, and informing the user of the outcome (Fischer-Hübner, 2011). However, more work needs to be done to educating citizens as to the problems and the benefits of IoT. A potential starting point is current media education initiatives at the secondary and post-secondary levels (if not before) and innovative curriculum that blends technical work and social insight (Ratto & Hoeckema, 2009; Ratto, 2011).

[50] http://euroalert.net/en/news.aspx?idn=10271

[51] For all relevant policy documents see http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm

[52] [Internet] Available from: Postcapes, tracking the internet of Things, platforms; http://postscapes.com/internet-of-things-platforms [Accessed 02 December 2011]

Gary Wolf, one of the founders of the Quantified Self with Kevin Kelly, explains in Data Drive Life[53] argues that until a few years ago, it would have been pointless to seek self-knowledge through numbers:

> *"Although sociologists could survey us in aggregate, and laboratory psychologists could do clever experiments with volunteer subjects, the real way we ate, played, talked and loved left only the faintest measurable trace. Our only method of tracking ourselves was to notice what we were doing and write it down. But even this written record could not be analysed objectively without laborious processing and analysis. Then four things changed. First, electronic sensors got smaller and better. Second, people started carrying powerful computing devices, typically disguised as mobile phones. Third, social media made it seem normal to share everything. And fourth, we began to get an inkling of the rise of a global super-intelligence known as the cloud."*

As end users have shaped the direction of the internet, end users like Gary Wolf might become highly influential in moving debates on privacy as a concept under threat, to a debate on self awareness and self knowledge.

Professor Mireille Hildebrandt of Radboud University, Nijmegen in the Netherlands works on profiling technologies on human identity and legal subjectivity. This involves issues of liability, causality, data protection, privacy, non-discrimination and intellectual property. Her article, 'A Vision of Ambient Law' addresses many legal issues relevant to the IoT. Her work on the hidden complexity of smart environments raises a number of issues, notably concerning fundamental human rights that are constitutive for the rule of law, such as privacy, non-discrimination and due process. For instance, fundamental questions she raises include: "which rights and options does one have if a smart environment implicitly takes a decision that affects my life, based on statistical profiles; which options does one have to protect personal data and/or to control its usage by smart environments; how can one possibly contest such decisions?" (Hildebrandt, 2010).

In a proactive approach, we need to move away from catchy slogans like the 'silence of the chips' since such thinking leads to many missed opportunities. The on going review of the EU Data Directive and the OECD privacy guidelines coupled with proposed base line legislation in the United States creates a unique transatlantic opportunity to redefine privacy protection and effective enforcement mechanisms. When dealing with issues surrounding privacy, one must assure to take into account both existing regulatory and policy constructs as well as technology solutions, which enable further security and privacy. There are many examples of the benefits of the IoT including: the smarter planet, smart grids, smart transportation, and transforming global transportation to name but a few. Privacy by design, privacy impact assessments, and privacy enhancing technologies should all be considered as a means to promote trust and confidence in this new medium. These new concepts must

[53] Wolf, Gary. The Data Driven Life, April 28 2010. http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?pagewanted=2

be allowed to develop. The focus needs to be on actions that are the most damaging and most likely to occur. Processes need to be developed to assess and mitigate risk to identify things of highest concern, e.g., actions that threaten one's most sensitive information and then designing effective enforcement mechanisms.

Mireille Hildebrandt states that “we may need to develop an Ambient Law that is embodied in the algorithms and human machine interfaces that support AmI and for this we will have to break through our paralysis, ready to become literate in terms of a new script” (Hildebrandt 2006a). Gérald Santucci, Head of EU Unit RFID, stressed the importance of the concept ’from privacy to privacies’ at the Brussels May 2009 Conference on the Internet of Things. What does it mean? An individual sets his or her privacy policies for every daily activity. Privacy is thus splintered up into a large set of privacies. These policies correspond with their digital counterparts in a distributed network of databases. In this way, your entire identity is not needed in order to service you on a particular activity. The distributed network of databases forms the next layer of smart connections. These are the results, hints, advice that is played back to you. The first always puts you into contact with real people in your neighborhood. If that is not possible, the second offer goes global immediately and will suggest relations and connections that might be far away physically.

In the reactive approach that assumes IoT as a digital layer on top of analogue identity, institutions, and services, agency lies in legal and multi-stakeholder consensus that might be embedded in devices and service provider infrastructure. The proactive approach recognizes that object to object and object to human communication will realistically mean that human identities no longer can be in full control and consent of all their actions and idiosyncratic communication. Here also agency lies in embedding consensus at protocol level in devices and service provider infrastructure.

References

[1] Bell, G. & Dourish, P. (2007). Yesterday's tomorrows: notes on ubiquitous computing's dominant vision. Pers Ubiquit Comput 11: p 133-143.

[2] EG Conference, 2007. Monterey, CA (2007). The next 5000 days of the web, Kelly, K. [Internet] Available from www.ted.com/index.php/talks/kevin_kelly_on_the_next_5_000_days_of_the_web.html [Accessed 17 September 2011].

[3] Gershenfield, N. (1999). When things start to think: The nature of mathematical modelling, the physics of information technology, and fab, the coming revolution on your desktop - from personal computers to personal fabrication. Henry Holt and Co: New York.

[4] Roberto de Almeida Amazonas, J. (2010) Opportunities, Challenges for Internet of Things Technologies.

[5] van Kranenburg, R. (2011). Moscow FuturoDesign Lab Co-create Urban Intelligence. Designing Smart Interfaces Between People and City. [Internet] Available from http://www.theinternetofthings.eu/ [Accessed 17 September 2011].

[6] Weiser, Mark (1991). The computer for the 21st century. Scientific American September Issue [Internet] Available from: http://www.ubiq.com. [Accessed 18 August 2011].

Chapter Two

[7] Albrecht, K. (2005). Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID. First edition. Edition. Thomas Nelson.

[8] Arduino (2011). Arduino. [Internet] Available from http://www.arduino.cc

[9] Ashton, K. (2009). That 'Internet of Things' thing. RFID Journal, 22 July. [Internet] Available at: http://www.rfidjournal.com/article/view/4986 [Accessed 18 August 2011].

[10] Bono, S. et al. (2005). Digital Signature Transponder In Proceedings of the Usenix Security Symposium, pp. 97-114. Usenix: Berkley, CA.

[11] Borden, E. (2010). No more secrets: Open data pioneer unlocks government radiation datasets. Pachube 25 July. [Internet blog]. Available from: http://blog.pachube.com/2011/07/no-more-secrets-open-data-pioneer.html [Accessed 17 September 2011].

[12] Burleson Consulting (2007). A brief history of database disk storage. [Internet] Burleson Consulting. Available from <http://www.dba-oracle.com/t_history_disk.htm> [Accessed 19 August 2011].

[13] Chui, M., Löffler, M. and Robets, R. (2010). The Internet of Things. McKinsey and Company: Chicago.

[14] Cute, Brian. (2011). The Public Interest Registry. blog on CircleID. [Internet] October 16. Available from: http://www.circleid.com/posts/7101616_the_internet_of_things_governance/ [Accessed 19 August 2011].

[15] Caprio, Dan. (2010). US View on the Technological Convergence Between the Internet of Things and Cloud Computing.

[16] CERP-IoT (2011). Strategic Research Agenda [Internet] Available from: ec.europa.eu/information_society/policy/rfid/documents/in_cerp.pdf [Accessed on 18 September 2001].

[17] Casagras Newsletter, February 2009 (http://www.rfidglobal.eu/userfiles/documents/CASAGRAS26022009.pdf) [Accessed 18 August 2011].

[18] Clark, D. Partridge, C., Braden, R. T., Davie, et al. (2005). Making the world (of communications) a different place. SIGCOMM Comput. Commun. Rev. 35, 3 (Jul. 2005), 91-96. [Internet] Available at: http://doi.acm.org/10.1145/1070873.107088 [Accessed 18 August 2011].

[19] EPoSS. (2011). The Internet of Things- EPoSS. [Internet] Available at: http://www.smart-systems-integration.org/public/internet-of-things. [Accessed 18 August 2011].

[20] Flavio D. et al,. (2011). Dismantling MIFARE Classic. [Internet]. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.142.4402. [Accessed 18 August 2011].

[21] Gannes, L. (2010). With Foursquare Out of the Picture, Facebook Buys Nextstop. [Internet] Available from: http://gigaom.com/2010/07/08/with-foursquare-out-of-the-picture-facebook-buys-nextstop/ [Accessed 19 August 2011].

[22] Gladwell, M. (2000). The Tipping Point: How little things can make a big difference. Little Brown: New York.

[23] IBM (2011). IBM announces new innovation lab dedicated to technology services [Internet] Available from: <http://www-03.ibm.com/press/uk/en/pressrelease/35148.wss [Accessed 19 August 2011].

[24] Information Security Group (2011). [Internet] Available from: http://www.avoine.net/rfid/index.php. [Accessed 18 August 2011].

[25] IPSO Alliance (2011). Enabling the Internet of Things. [Internet] Available at: http://ipso-alliance.org. [Accessed 18 August 2011].

[26] ITU (2005). The Internet of Things [Internet] Available at: http://www.itu.int/osg/spu/publications/internetofthings/ [Accessed 19 August 2011].

[27] Jefferies, N. (2011). About the Forum - Wireless World Research Forum. [Internet] Available from: http://www.ww-rf.org/. [Accessed 18 August 2011].

[28] Kale, J. (1991). RFC 1180 - TCP/IP tutorial. 2011. [Internet] Available at: http://tools.ietf.org/html/rfc1180. [Accessed 18 August 2011].

[29] Sourcemap (2011). Soucemap. [Internet] Available from http://stage.sourcemap.org [Accessed 19 August 2011].

[30] Streitz, N. (2001). Augmented reality and the disappearing computer. In Smith, M, Salvendy, G., Harris, D., Koubek, R. (eds) Cognitive engineering, intelligent agents and virtual reality. p 738-742. Lawrence Erlbaum: London.

[31] Talbot, D. Phones that Rule Everything (2011). MIT's Technology Review. Vol. 114/ No. 3. June 2011. p. 78 - 79.

[32] Uckelmann, D.; Harrison, M.; Michahelles, F. (2009). Architecting the Internet of Things. Springer [internet]. Available from http://www.springer.com [Accessed 18 August 2011].

[33] Vermesan, O. (2009). CERP-IoT Strategic Research Agenda. [Internet]. 1, All. Available at: http://ec.europa.eu/information_society/policy/rfid/documents/in_cerp [Accessed 18 August 2011].

Chapter Three

[34] Architecture of the World Wide Web, (2004). Volume One, W3C Recommendation, 15 December. [Internet] Available from: http://www.w3.org/TR/webarch/#URI-scheme [Accessed on 18 September 2011].

[35] Ashton, K. (2009). That 'Internet of Things' thing. RFID Journal, 22 July. [Internet] Available at: http://www.rfidjournal.com/article/view/4986 [Accessed 18 August 2011].

[36] Ashton, S. (2009). ZigBee Technology Overview [Internet] Available at: http://www.ZigBee.org/imwp/idms/popups/pop_download.asp?contentID=16561 [Accessed on 18 September 2011].

[37] Bridge project (2011). [Internet] Available from: http://www.bridge-project.eu/ [Accessed on 03 September 2011].

[38] Dempo, H. and Yoshida, M. (2010). CUBIQ: Cross UBIQuitous platform Architecture, 2010 10th Annual International Symposium on Applications and the Internet, Seoul, Korea, July.

[39] Devarapalli, V. Wakikawa, R. Petrescu, A. and Thubert, P. (2005). Network Mobility (NEMO) Basic Support Protocol , Request for Comments 3963, Internet Engineering Task Force, January.

[40] Dou, E. (2011). The right to be forgotten. Reuters [Internet] 07 March. Available from <http://www.reuters.com>[Accessed 18 August 2011].

[41] Dialog Project (2011). [Internet] Available at: http://dialog.hut.fi/ [Accessed on 18 September 2011].

[42] Edri.com. (2009). The right to silence the chips. Edri.com [Internet] 01 July. Available from: <http://www.edri.org/edri-gram/number7.13/right-silence-of-the-chips>[Accessed 18 August 2011].

[43] EPCglobal. (2005). The EPCglobal Architecture Framework - Version 1.0, March. [Internet] Available: http://www.epcglobalinc.org/standards/architecture/architecture 1 0-framework-20050701.pdf. [Accessed on 18 September 2011].

[44] Fielding, Roy (2000). Architectural Styles and the Design of Network-based Software Architectures, Doctoral dissertation, University of California, Irvine.

[45] Hildebrandt, M. (2010): An Ecosystem of Legal and Technological Protections, on: Trusted e-services for the citizen session, ICT Event, Brussels.

[46] IoT-A Public documents. (2011). [Internet] Available from: http://www.iot-a.eu/public/public-documents [Accessed 03 Sept 2011].

[47] Johnson, D. Perkins, C. and Arkko, J. (2004). Mobility Support in IPv6, Request for Comments 3775, Internet Engineering Task Force, June.

[48] Langheinrich, M. (2009). Privacy in Ubiquitous Computing, in: Krumm, J (ed.): Ubiquitous Computing, Chapman & Hall / CRC Press, Sep. 2009.

[49] Mindteck (2009). WirelessHART Overview, [Internet] Available at: http://www.mindteck.com/resourcelibrary/Technical-Papers/WirelessHART-%20Overview.html [Accessed on 18 September].

[50] Moskowitz, R. and Nikander, P. (2006). Host Identity Protocol (HIP) Architecture, Request for Comments 4423, Internet Engineering Task Force, May.

[51] Much-Ellingsen, A. (2011). D.3.4 - End to End Networking and Management, Sensei Public Deliverable D.3.4, 2010. [Internet] Available: http://www.sensei-project.eu/ [Accessed on 18 September 2011].

[52] Garcia-Morchon, O. (2011). Security Considerations in the IP-based Internet of Things. Datatracker [Internet] Available at: <http://datatracker.ietf.org/doc/draft-garcia-core-security/> [Accessed 17 August 2011].

[53] Gilmore, G. (2011). What you should know about the EU's new 'internet of things' privacy framework. Business2Community [Internet] 17 June. Available from: <http://www.business2community.com/social-media>[Accessed 18 August 2011].

[54] IPSO Alliance (2011). Enabling the Internet of Things. IPSO Alliance. [Internet] Available at: http://ipso-alliance.org. [Accessed 18 August 2011].

[55] Kale, J. (1991). RFC 1180 - TCP/IP tutorial [ONLINE] Available at: http://tools.ietf.org/html/rfc1180. [Accessed 18 August 2011].

[56] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Background. 2011. [Internet] Available at: http://www.oecd.org/document/20/0,3746,en_2649_34255_15589524_1_1_1_1,00.html [Accessed 19 August 2011].

[57] Perkins, C. (2002). IP Mobility Support for IPv4, Request for Comments 3344, Internet Engineering Task Force, August.

[58] Schuster, E. Allen, S. Brock, D. (2007). Global RFID: The value of the EPCglobal network for supply chain management, Berlin and Heidelberg: Springer; 1st ed.

[59] Sun Spot World (2011). [Internet] Available from: http://www.sunspotworld.com/ [Accessed on 18 September].

[60] Song et al.(2008). WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control, IEEE Real-Time and Embedded Technology and Applications Symposium.

[61] Stewart, R. et al. (2000). Stream Control Transmission Protocol, Request for Comments 2960, Internet Engineering Task Force, October.

[62] uID Center Web Site, (2011). What is an ucode? [Internet] Available: http://www.uidcenter.org/learning-about-ucode/what-is-ucode [Accessed on 18 September 2011].

Chapter Four

[63] Albrecht, K. (2002). Supermarket Cards: The Tip of the Retail Surveillance Iceberg. Denver University Law Review, Summer 2002, Volume 79, Issue 4, pp. 534-539 and 558-565.

[64] Albrecht, K. and Starrett, M. (2003). Boycott Benetton. [Internet] Boycott Benetton. Available from http://www.boycottbenetton.com [Accessed 19 August 2011].

[65] Albrecht, K. (2005). Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID. First edition. Thomas Nelson.

[66] Arduino (2011). Arduino. [Internet] Available from <http://www.arduino.cc>

[67] Burleson Consulting (2007). A brief history of database disk storage. [Internet] Burleson Consulting. Available from <http://www.dba-oracle.com/t_history_disk.htm> [Accessed 19 August 2011].

[68] Council (2010). Arrayent: Internet-connect-your-product-in-a-day DevKit. [Internet] Available from: http://www.theinternetofthings.eu/content/arrayent-internet-connect-your-product-day-devkit [Accessed 19 August 2011].

[69] Foresman, C. (2011). Wired US. How a Security Researcher Discovered the Apple Battery ’Hack’ [Internet] Available from: http://www.wired.com/threatlevel/2011/07/apple_battery [Accessed 19 August 2011].

[70] Gannes, L. (2010). With Foursquare Out of the Picture, Facebook Buys Nextstop. [Internet] Available from: http://gigaom.com/2010/07/08/with-foursquare-out-of-the-picture-facebook-buys-nextstop/ [Accessed 19 August 2011].

[71] IBM (2011). IBM announces new innovation lab dedicated to technology services [Internet] Available: <http://www-03.ibm.com/press/uk/en/pressrelease/35148.wss [Accessed 19 August 2011].

[72] Open NFC (2011). Open NFC. [Internet] Available from: <http://www.open-nfc.org [Accessed 19 August 2011].

[73] Open Picus (2011). Open Picus. [Internet] Availble from http://www.openpicus.com/cms [Accessed 19 August 2011].

[74] Microsoft (2003). The Disappearing Computer by Bill Gates. Press release, 2003. Available at: http://www.microsoft.com/presspass/ofnote/11-02worldin2003.msp [Accessed 19 August 2011].

[75] MacManus, R. (2011). Pachube Acquired: Why Did It Sell So Early? July 20 [Internet] Available from: http://www.readwriteweb.com/archives/pachube_acquired.php [Accessed 19 August 2011].

[76] Physorg (2011). Minority rules: Scientists discover tipping point for the spread of ideas [Internet] Available at: <http://www.physorg.com/news/2011-07-minority-scientists-ideas.html [Accessed 19 August 2011].

[77] Schmidt, E. (2009). Speaking at a forum jointly hosted by Google and the Pittsburgh Technology Council in Pittsburgh, PA. 23 September 2009.

[78] Streitz, N. (2001). Augmented Reality and the Disappearing Computer. In: Smith, M., Salvendy, G., Harris, D., Koubek, R. (Eds.), Cognitive Engineering, Intelligent Agent and Virtual Reality., Lawrence Erlbaum, 2001. pp. 738-742.

[79] Streitz, N. and Nixon, P. (2005). The Disappearing Computer. Guest Editors’ Introduction to Special Issue. Communications of the ACM, Vol. 48, March 2005. pp. 33-35.

[80] Streitz, N. and., Kameas, I. Mavrommati (Eds.) (2007). The Disappearing Computer: Interaction Design, System Infrastructures and Applications for Smart Environments. State-of-the-Art Survey, Springer LNCS 4500.

[81] Thai, T. (2010). Terragotchi demonstration video. [Internet] Available from: http://vimeo.com/groups/cmdgenk/videos/12508917 [Accessed 19 August 2011].

[82] Weiser, Mark. (1991). The computer for the 21st century. Scientific American September Issue [Internet] Available from: http://www.ubiq.com. Accessed 18 August 2011].

Chapter Five

[83] Arthur, C. (2011). Sony suffers second data breach with theft of 25m more user details. Guardian. [Internet] Available at: http://www.guardian.co.uk/technology/blog/2011/may/03/sony-data-breach-online-entertainment. [Accessed 17 August 2011].

[84] Auto-ID Labs. (2011). RFID Announcements of the ETH. [Internet] Available from: <http://www.autoidlabs.org> [Accessed 17 August 2011].

[85] BEUC/ANEC: (2008). The European Consumers Group (BEUC) & The European Consumer Voice in Standaridsation (ANEC)'s joint consultation: "Internet of Things: Commission Staff Working Paper on Early Challenges regarding the 'Internet of Things"'. SEC (2008) 2516.

[86] Cavoukian, A. (2011) Privacy by Design. [Internet] Available from: <http://www.ipc.on.ca> [Accessed 19 August 2011].

[87] Cole, J. (2011). The Tenth Study by the Digital Future Project Finds High Levels of Concern about Corporate Intrusion in Personal Lives. University of Southern California (USC). Annenberg School for Communication & Journalism. Center for the Digital Future. [Internet] Available from: http://www.digitalcenter.org/pdf/2011_digital_future_final_release.pdf [Accessed 19 August 2011].

[88] Cute, Brian (2011). The Public Interest Registry. blog on CircleID. [Internet] October 16. Available at: http://www.circleid.com/posts/7101616_the_internet_of_things_governance/ [Accessed 19 August 2011].

[89] China Communication Network (2010). Experts say standardization of Internet of Things is urgent [Internet] Available from http://www.cn-c114.net/583/a567633.html [Accessed 19 August 2011].

[90] China Communication Network (2011). Ericsson launches cloud based service for M2M communication [Internet] Available from http://www.cn-c114.net/2502/a580768.html [Accessed 19 August 2011].

[91] China Communication Network (2011). Sprint hopes to make money off machine-to-machine conversations [Internet] Available <http://www.cn-c114.net/2502/a576424.html> [Accessed 19 August 2011].

[92] China Communication Network (2011). NFC and mobile payment to spearhead M2M development. [Internet] Available from http://www.cn-c114.net/2502/a585330.html [Accessed 19 August 2011].

[93] Dada, A. and others (2010). The Potential of the EPC Network to Monitor and Manage the Carbon Footprint of Products [Internet] Available from: http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-BIZAPP-054.pdf [Accessed 19 August 2011].

[94] Doria, Avri (2010). Socio-Economics of the Network of the Future Workshop. Lulea University of Technology. [Internet] Available at: http://ec.europa.eu/information_society/events/cf/fnc6/item-display.cfm?id=4883 [Accessed 19 August 2011].

[95] Dillow, C. (2011). Rebuilding tsunami-wrecked Japan as smart towns. [Internet] 22 June. Available at http://www.urbangateway.org/content/news/rebuilding-tsunami-wrecked-japan-smart-towns. [Accessed 17 August 2011].

[96] Dutton, W. (2006). Cybertrust: The tension between privacy and security in an e-society. Oxford Internet Institute. [Internet] Available at: http://www.oii.ox.ac.uk/research/projects/?id=5 [Accessed 19 August 2011].

[97] Fairtracing (2011). Impact! Exhibition: “Does It Smell Like Fair Trade?” images & video clips. [Internet] Available at http://www.fairtracing.org [Accessed 19 August 2011].

[98] Galante, G. (2011). Sony Network Breach Shows Amazon Cloud’s Appeal for Hackers - BusinessWeek. [Internet] Available at: http://www.businessweek.com/news/2011-05-16/sony-network-breach-shows-amazon-cloud-s-appeal-for-hackers.html. [Accessed 17 August 2011].

[99] HP. (2001). Shell to use CeNSE for clearer picture of oil and gas reservoirs. [Internet] Available at: http://www.hpl.hp.com/news/2009/oct-dec/cense.html [Accessed 19 August 2011].

[100] Guinard, D. (2010). Auto-ID Lab White Paper. Mobile IoT Toolkit: Connecting the EPC Network to Mobile Phones. Auto-ID Lab [Internet] Available from: http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-SWNET-026.pdf [Accessed 19 August 2011].

[101] Hudson, A. (2011). Are there Criminals Hiding in the Cloud? BBC Click. [Internet] 8 May Available at <http://news.bbc.co.uk/2/hi/programmes/click_online/9477968.stm> [Accessed 19 August 2011].

[102] IERC. (2011). Identifying IoT Technology Research Challenges. IERC. [Internet] Available from: <http://www.internet-of-things-research.eu/> [Accessed 19 August 2011].

[103] IoT Expert Group 022. (2011). Meeting Minutes of IoT Expert Group of 19 April 2011. Brussels. European Commission, Information Society and Media Directorate-General, Converged Networks and Services, Networked Enterprise & Radio Frequency Identification (RFID). May 2011.

[104] Jakobs, K. et al (2011). Project Report: "Standardising the Internet of Things- What the Experts Think." RWTH Aachen University. CoSc Department, Informatik 4 and Research Group on Electronic Business. 2011. [Internet] Available from: https://www.comsys.rwth-aachen.de/fileadmin/papers/2011/2011-kai-JITSR.pdf [Accessed 19 August 2011].

[105] Lopez, T. (2010). Supply Chain sensor support by integrating the OGC Sensor Web Enablement and the EPC Network architectures. Auto-ID Labs. [Internet] Available from: http://www.autoidlabs.org/rssdetail/dir/article/1/335/ [Accessed 19 August 2011].

[106] Naone, E. (2011). Turning Your Phone into a Wallet. MIT's Technology Review. Vol. 114/ No. 3. June 2011. p. 76.

[107] Nasca. (2009). Wuxi's Economic Situation In 2009. Nasca. [Internet] Available from: http://www.nacsa.com/archives/files/wuxi_event_20100526.pdf [Accessed 19 August 2011].

[108] Near Field Communication Forum (2011). [Internet] Available from: http://www.nfc-forum.org/aboutnfc

[109] Sensing Planet. (2011). Smart device and sensor network management (2011). Available from: <http://sensingplanet.net/sensingplanet/> [Accessed 19 August 2011].

[110] Smart Connected Communities. (2011). [Internet] Available from <http://www.smartconnectedcommunities.org/community> [Accessed 19 August 2011].

[111] Smart Connected Communities. (2011). IBM'S Smarter Planet & Cisco's Smart + Connected Communities. [Internet] Available from <http:// http://www.smartconnectedcommunities.org/message/1670> [Accessed 19 August 2011].

[112] Syslog. (2011). The Philosophy of Trust and Cloud Computing. April 5/6, 2011, Corpus Christi, Cambridge, Sponsored by Microsoft Research.

[113] Wood, D. (2011). The Four Horsemen of the Apocalypse, Class of 2011: The Cloud.Law.com [Internet] Available at: http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202503787967. [Accessed 17 August 2011].

[114] van der Veer, H. et al (2008). ETSI White Paper No. 3: Achieving Technical Interoperability - the ETSI Approach. Third edition, April 2008.

[115] Von Reischach, F (2008). A Ubiquitous Product Rating System. Pervasive [Internet] Available from: http://www.pervasive2008.org/Papers/Workshop/w4-01.pdf [Accessed 17 August 2011].

[116] Weber, R. (2011). Accountability in the Internet of Things. Computer Law & Security Review. Vol 27 2011. p. 133-138. [Internet] Available from: http://www.guarder.net/euro-nf/weber.pdf [Accessed 17 August 2011].

[117] Wireless Sensor Networks Blog (2011). Core chips of Sensor Network see breakthrough in China. [Internet] Available from: http://www.wsnblog.com/2010/11/03/core-chips-of-sensor-network-see-breakthrough-in-china [Accessed 17 August 2011].

A Note On The Authors

Rob van Kranenburg wrote *The Internet of Things. A critique of ambient technology and the all-seeing network of RFID,* (Foreword by Sean Dodson), Network Notebooks 02, Institute of Network Cultures, in 2007. Although the arguments lined out are very critical he was asked to join the Expert Group of the European Commission. He moderated the business and policy focused Internet of Things Forum Brussels three years in a row. He founded Council, a think tank for the Internet of Things (www.theinternetofthings.eu) in 2009, which has currently 80 members ranging from artists and designers, to Creative Directors at Philips and academics such as Liam Bannon, Matt Ratto, Ben Schouten, Francesca Bria, Karmen Franinovic, and Florian Michahelles. His latest project is involving the Dutch Belastingsdienst, from the Ministery of Finances. They are interested in IoT as it enables more or even full traceability and transparency that could lead to new and different tax ’apps’. A second reason for them to be interested in IoT is that they see the need to accommodate the current call for openness and accountability by citizens. The UK has set up http://wheredoesmymoneygo.org/ "trying to make government finances much easier to explore and understand - so you can see where every pound of your taxes gets spent." The Dutch pilots, apps and scenarios for ministerial and senior management levels that Council will be involved in are considering participatory budgeting (allowing you to spend some amount of your taxes locally) and a rethinking of VAT. He is involved in a Paris based start up called CKAB. He is a member of the Expert Group on Internet of Things (EG IoT) for the European Commission.

Erin Anzelmo earned her master’s degree in International Law (LL.M.) with research focus on the Internet and international law. Erin has worked with a think-tank, the Global Trust Council (GTC), in Malmo, Sweden on eIdentification, consulting on human rights in the digital realm. Erin served as assistant to the Secretariat of the European eSkills Association (EeSA) in Brussels, as well as volunteered with ISOC to form the ISOC Rwanda Chapter. She is published in The Brussels Journal of International Relations on Cyberspace and International Law.

Despite being tempted by other disciplines, **Alex Bassi** decided to explore the esoteric world of computer science, mainly because of his tension between creativity and mathematical rigour. He enjoyed his stay in Milan, where he attended its world famous University, and became passionate of artificial intelligence, soft computing and software engineering. After serving his duty in the army, as many of us, he lent his abilities to the private sector, and joined Amadeus in 1997, to become -against his will- an expert of Unisys OS 2200 assembler. He then managed to unchain his spirit again and joined the University of Tennessee in summer 2000, where he was involved in the seminal work and development of the Internet Backplane Protocol. After surviving "Nax-vul" for 18 months, he managed to get back to Europe, and in particular to Lyon, where he had a position as Research Visitor at the Ecole Normale Superieure. For two years, he developed the relationship between the novel storage concepts and active networking. He then worked for RIPE NCC, working on project regarding the whois database such as the AfriNIC creation, and after one year of rainy A'dam in November 2004 he moved to the sunny south of France, to integrate the Hitachi Sophia Antipolis Labs. There he got involved in various projects, regarding Grid and Cloud (with particular regards to data aspects), Autonomic Communications and RFID. In 2007 he became chair of the then RFID (now Internet of Things) Working Group of the EU Technological Platform EPoSS, and from 2010 he started his own company, Alessandro Bassi Consulting, acting as a Technical Coordinator for the Internet of Things Architecture (IoT-A) FP7 IP project for Hitachi. He is a member of the Expert Group on Internet of Things (EG IoT) for the European Commission.

Dan Caprio brings over 25 years of experience on legal and policy issues involving the convergence of internet, telecommunications, and technology. He has substantial knowledge and experience in the areas of privacy, cyber security, information security and the Internet of Things, a term used when everyday objects are connected to the Internet. Mr. Caprio works with clients to define and capitalize on public policy strategies in the United States and Europe. From 2004 to 2006, Mr. Caprio served as Chief Privacy Officer and Deputy Assistant Secretary for Technology Policy for the U.S. Department of Commerce (DoC) where he advised the Secretary of Commerce and the White House on technology policy and privacy protection. While at the DoC, he oversaw activities related to the development and implementation of federal privacy laws, policies, and practices. He served as Chairman of the DoC RFID working group and Co-Chairman of the Federal RFID interagency working group In 2007, Mr. Caprio was appointed by the Secretary of the Department of Homeland Security to serve on the Data Privacy and Integrity Advisory Committee. In 2010, Mr. Caprio was appointed as a transatlantic subject matter expert for the European Commission's Internet of Things formal expert group. Prior to his tenure at the DoC, Mr. Caprio served as Chief of Staff to a Commissioner at the Federal Trade Commission. In 2002, he was appointed to represent the United States in revising the OECD guidelines on information systems and networks. Dan holds an active security clearance for classified matters. He is a member of the Expert Group on Internet of Things (EG IoT) for the European Commission.

Sean Dodson is a senior lecturer in journalism at Leeds Metropolitan University. He is also a journalist and writer and has been covering the social uses of technology for over 10 years. He has also worked as an assistant producer at the Guardian and a researcher for the Sunday Times, as well as contributing to a wide range of titles including Wired, Design Week, UK Press Gazette, The South China Morning Post and the Melbourne Age.

Matt Ratto is Assistant Professor, Faculty of Information University of Toronto. Ratto received his PhD from the University of California, San Diego in 2003, writing his dissertation on the social organization of the Linux development community. Following this, he completed a 2 year post-doc at the Netherlands Institute for Scientific Information (NIWI) and in 2005 helped create the Virtual Knowledge Studio for the Humanities and Social Sciences in Amsterdam (VKS-KNAW). In 2005, he was awarded a Netherlands Science Foundation (NWO) grant to study the use of computer simulation and modeling technologies in Archaeology and in 2007 was given a 1 year fellowship in the HUMlab, an innovative digital humanities laboratory located at the University of Umea, Sweden. He moved to the University of Toronto in 2008. His current research focuses on how hands-on productive work - making - can supplement and extend critical reflection on the relations between digital technologies and society. This work builds upon the new possibilities offered by open source software and hardware, as well as the developing technologies of 3D printing and rapid prototyping. These technologies and the social collectives that create, use, and share them provide the context for exploring the relationship between ’critical making’ and ’critical thinking’. Ratto is currently director of the Toronto Thing Tank Lab (formerly DDiMIT), a private-public-academic consortium interested in investigating, exploring, and building capacity around new developments in tangible interfaces, smart objects, and digital infrastructures. Departing from the traditional model of the hackerspace, Thing Tank is an ’digital economy trading zone’, a virtual and physical space where Ontario companies, academic institutions, and community organizations can leverage their joint knowledge and skills in order to support each other in doing novel research, creating innovative products and services, and fostering creative and engaging work in the Internet of Things.