Communications in Mobile Computing
a SpringerOpen Journal

ORIGINAL SUBMISSION Open Access

IoT Challenges

Rob van Kranenburg[1*] and Alex Bassi[2]

* Correspondence: kranenbu@xs4all.nl
[1]IoT-A.eu/Internet of People, Tentoonstellingslaan 22, 9000 Gent, Belgium
Full list of author information is available at the end of the article

Abstract

In this short text the authors claim that the challenges posed by Internet of Things cannot be managed with the current policy tools and research programs, as these are too slow and too instrumental. These challenges are: a) global cooperation and standards, b) new business models and new currencies, c) ethics, control society, surveillance, consent and data driven life, and d) technological challenges driven by the need to save energy. These lead up to the urgency to co-design decision making formats that aim at finding the perfect balance between top down planning and bottom up innovation.

Keywords: Internet of things, Cloud versus edges, Ethics, Disruptive, Collaboration

Introduction

The term "IoT" was initially used by Kevin Ashton in 1999, and became of widespread 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's a general agreement that IoT involves objects and connectivity, the precise wording is still to be found [1]. A decade after its conception the Internet of things is an emerging technology yet to reach the consciousness of the masses. And yet it has a surprisingly long, even illustrious history. It 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. Currently we can discern two main blocks of thought on IoT. The first is a reactive framework of ideas and thought that sees IoT as a layer of digital connectivity on top of existing infrastructure and things. This position sees IoT as a manageable set of convergent developments on infrastructure, services, applications and governance tools. It is assumed that, as in the transition from mainframe to Internet some business will fail and new ones will emerge, this will happen within the current governance, currency end business models. The second is a proactive framework of ideas and thought that sees IoT as a severely disruptive convergence that is unmanageable with current tools, as it will change the notion of what data and what noise is from the supply chain on to 'apps'. In both these approaches we find the same challenges. The difference will be in the solutions and approaches. From our perspective as a citizen and enduser we can fully accept the consequences of going fully for the solutions in the proactive framework. From the perspective of a corporation with vested assets and business inteests and from the perspctive of a government that has to ensure continuity and harmony it is realistic to assume that they both will find solutions within the reactive

framework. No doubt solutions there will be found, but as that framework has its roots in the pre digital transition it cannot inspire nor create viable businessmodels that take the current reality into account.

Challenge 1: Global cooperation

A quick analysis of the current state of IoT globally shows three approaches:

1. An integrated approach 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. Since then Chinese Premier, Wen Jiabao, has mentioned IoT several times in official speeches, the city of Wuxi has been named premier location for IoT. 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. 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 an important topic for further research. In recent publications the central government argued for a focus on IoT but that the regions should wait with infrastructural works under its national direction.
2. A stakeholder approach in the EU that favors public-private partnerships and vertical investments through four-year program plans. This organizes internal competition, even between its own flagship projects. The Cloud is an enabler for IoT, not the other way around. The approach until now aimed 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, the home. In order to to do this, the EU has set up risk assessment procedures (PIA for RFID, IIA for IoT) with a broad and wide variety of stakeholders (the IoT Expert Group). It is the only major political block in the world that has done so, so far. Others however will reap the real rewards of these efforts if IoT does not become the clear and unequivocal focus of EU R&D, investments and driver for changing decision making systems at the highest level.
3. An opportunity investment approach in the US that is driven by short to mid-term return on investment. It is pushed by smart energy, smart cities, and RFID fueled by Department of Defense 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) hand held device integration (Google buying Motorola). No US wide policy, no stakeholder debate. Large opportunities at local and city level where local decision power is harnessed. There is an appreciable amount of 'buzz' in this area, but it is still very much about the Cloud.

What set of principles is able to align these perspectives?

Challenge 2: Business models, new currencies in IoT and trust

Nick Appleyard, head of digital at the UK Technology Strategy Board believes IoT will lead to new "processes and innovative business models." According to Alessandro Bassi, one model could be based on the idea of borrowing and lending objects instead of buying them: A drill can be pretty expensive, so given the fact that you may in total use it for about 10 minutes in its lifetime makes for quite a high price per minute. Renting one in your local DIY store is quite a hassle, so imagine embedding a chip into the drill and being able to track it and borrow it through some kind of community service instead." In fact, he adds, we need to get away from the idea of adding something to objects to enable interconnectivity. A key area of research lies in building procedures and protocols for decision making that are not based on the premise of speed. In a real-time world there is no longer gain being the "first" to have the data. Instead, the internet of things favors a daily situation of full traceability. There is so much contextual information about what you are wearing – this jacket or this pair of jeans – that neither the customer nor the merchant, require a Point of Sale/Point of Transaction as a "closure". And yet "closure" is of great importance to us as human beings, as it signals the "right" kind of feedback in a procedure enhancing levels of trust. It may be the case that IoT will favor a situation where different forms of currencies, standards of banking and money will exist together [2].

Challenge 3: Ethics, control society, surveillance, consent and data driven life

Privacy was named by the originator of ubicomp, Mark Weiser, the late chief scientist at Xerox Parc as a key issue (Weiser, 1991) [3]. Machina Research, in association with Latitude, Council and Info.nl – a trio of web 2.0 consultancy companies – recently ran an web survey, polling views on the future internet of things. One of the questions was related to concerns that people may have about living in a future connected environment. Privacy was mentioned by a clear majority as a key challenge. Privacy Enhancing Technologies (PET) is a partial solution. The Privacy Coach, [4] 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 and others, 2011). It functions as a mediator between customer privacy preferences (Fischer-Hübner, 2011) and corporate privacy policies, trying to find a match between the two, and informing the user of the outcome. Gérald Santucci (head of unit Knowledge Sharing), key IOT architect at the European Commission explains: "in the future, the right to privacy, whatever we do to implement it with technology and/or regulations ("right to be forgotten", "right to oblivion", "right to silent chips", etc.), will become a subset of ethics. The future is (largely) about ethics-by-design" [5].

Challenge 4: Technological challenges

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, 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.

- Zero-Entropy systems (energy harvesting, energy conservation, energy usage): Energy will be a major technological challenge in the next five to 10 years, and research must be conducted in order to develop systems that are able to harvest energy from the environment and not waste any under operation.
- Scalability: IoT will be composed of trillions of devices. While it is unlikely that all devices will be connected in a mesh, but rather organized in hierarchical sub domains, the number of interconnected object will outnumber by several orders of magnitude the current internet.
- Security and privacy: The issue of having sufficient security on devices with limited capabilities has to be addressed and solved convincingly. As well, technological architectures preserving the respect of privacy have to be developed and used as a basis for any future development.
- Communication mechanisms: The situation in today's IoT domain resembles to the one at the very beginning of the Internet: several communication mechanisms were used, and only the convergence on a particular reference model allowed the development of the web.
- Integration of smart components into non-standard substrates: The use of non-silicon substrates for developing smart components will reduce the dependency to silicon with all related problems, like packaging and recycling.

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 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. First of all, 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 (Ipso, 2011), 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). 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 nanorobot 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, 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.

Challenge 5: Finding the perfect balance between top down planning and bottom up innovation

IoT applications should be aimed to help the current institutions and public bodies to transform peacefully into a networked model of open data [6], direct feedback on where money goes, participatory budgeting models (say 25% for innovation in your street and neighborhood). IoT could be extremely relevant in making direct feedback visible in street and city furniture, and mobile applications. The internet of things can be a layer of data, open to all, through which individuals can decide for themselves what they are willing to pay for, get direct feedback from their voluntary donations, coordinate community spending that has a direct bearing to their needs through participatory budgeting [7,8].

Conclusion

What becomes clear in these challenges is that IoT cannot be managed with the current policy tools and research programs. They are too slow and too instrumental. There is too little sense of urgency; of the larger picture of Climate Change that should be the one issue the main umbrella research questions are parsed to, and of the upcoming breakdown in managing societal drivers in an inclusive way.

Author details
[1]IoT-A.eu/Internet of People, Tentoonstellingslaan 22, 9000 Gent, Belgium. [2]IoT-A.eu/Internet of People, 3 Avenue de Cannes, 06160 Juan-les-Pins, France.

Received: 9 August 2012 Accepted: 13 August 2012
Published: 28 November 2012

References

1. Anzelmo E, Bassi A, Caprio D, Dodson S, van Kranenburg R (2011) Matt Ratto (Internet of Things, Discussion/ Position Paper. Institute for Internet and Society, Berlin, commisioned
2. Bassi A, Anderson S (2011) We need a killer business model. Council. Available at: http://www.theinternetofthings.eu/content/alessandro-bassi-interviewed-stig-andersen-we-need-killer-business-model. Accessed on 22 April 2011
3. Weiser M (1993) Some computer science issues in ubiquitous computing. Communications of the ACM 36(7):75–84, July
4. Broenink G, van Kranenburg R et al (2011) The Privacy Coach: supporting customer privacy in the internet of things. TNO. Available at: http://arxiv.org/pdf/1001.4459. Accessed 21 August 2011
5. Santucci G (2010) Speech at Internet of Things Europe 2010. Cordis cordis.europa.eu/fp7/ict/enet/documents/. . ./iot-europe2010.pdf
6. Wolf G (2010) The Data-driven life. NY Times Magazine, April 28. Available from: http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html. Accessed 21 August 2011
7. Nold C, van Kranenburg R (2010) Situated technologies pamphlets 8: The internet of people for a post-oil world. The Architectural League of New York, New York
8. van Kranenburg R (2007) The Internet of Things. A critique of ambient technology and the all-seeing network of RFID, Network Notebooks 02. Institute of Network Cultures. Available from: http://networkcultures.org/wpmu/portal/publications/network-notebooks/the-internet-of-things. Accessed 21 August 2011

doi:10.1186/2192-1121-1-9
Cite this article as: van Kranenburg and Bassi: **IoT Challenges.** *Communications in Mobile Computing* 2012 **1**:9.