

Answer to the European Commission public consultation on the early challenges regarding the "Internet of Things"

Please indicate your preference (use a X):

- I agree that this document is made public
 I want this document **not to** be made public

If you are replying on behalf of an organisation, please indicate:

- The organisation's name: [Waag Society](#)
- The type of organisation:
 - private company
 - government/public body/international organisation
 - academic/research institution
 - non governmental organisation
 - other: [indepent media lab](#)
- Your organisation details
 - o location: [Amsterdalm](#)
 - o size: [50](#)
 - o scope of activities (max 3 sentences): [creative technology for social innovation](#)
 - o website: www.waag.org
- Contact person: [Rob van Kranenburg](#)
- Contact person' telephone: [0031 6 419 30 235](#)
- Contact person's email: rob@waag.org

Please start replying on the next page

Insert here your organisation name (or your own name if replying on your own behalf)

Where we are now:

RFID technology is at a crucial point, in terms of standards and policies, regulations and deployment and services. As technology becomes ever more deeply embedded in everyday life and the experienced economies, it can no longer see design as a front-end tool, nor as a social and cultural issues as a sphere that has to mold itself around new technologies. On the contrary, as we see so clearly with RFID one has to hardcode these issues into the systems architecture and see them not as problems, not as drawbacks but as challenges to overcome at all levels of a successful introduction of new technologies.

Inevitable as technology, so

We need to move to debate further from this seemingly deadlocked polarised state it appears we are at now. Distributing yourself as data into the environment has been the revolving wheel of progress for our conceptions and applications of technology. Location-based, real-time – services, applications to strengthen communities, and the capacity to generate high quality data in information overload, these are all possibilities within a wired connected environment that need serious exploration and research.

But ontologically important, not only logistically (there is no return from the IOT but through a crash/catastrophe)

Unless we find new ways of scripting new forms of solidarities with digital technology, it seems like we can envisage two roads that both lead to less dialogue, less communication, less innovation, less business opportunities, less sustainable options. The one focuses on control in a fundamentally flux wireless environment. The other focuses on hiding the technological complexity behind ever more simple user friendly interfaces. In both cases there is no learning by citizens on how to function within such a system, thereby, opening up all kinds of breakdown scenarios.

TCP/IP is the set of network communication protocols – the language - of the Internet (Transmission Control Protocol/Internet Protocol) that ran officially on the ARPA network (the precursor of the internet) in 1983. Because of the military and academic background of the internet, the world wide web was made possible in 1993 with the browser' Mosaic. Had it been a commercial operation, we would be living in a world where we paid for a subscription to the Sony web to deliver an email to a friend in Japan from Philips Netherlands web.

It has allowed citizens to become professional managers of their lives through the internet, 3G and GPS and the ever growing possibilities of social networking applications and sites. The solidarities that still exist within the legislative frameworks and mental maps of citizens are rapidly being broken down by the inability of national states to deal with the current financial crisis, the rising oil and gas prices, climate change and the changing power shift towards the East. These national states have outsourced and privatised everything from their currency to their ability to make law and are de facto empty shells that function only as tax receiving institutes. Taking the Netherlands as an example, we see that as one the highest developed and technology saturated nations it has the highest rate of emigration in the EU, even higher then Poland.

Insert here your organisation name (or your own name if replying on your own behalf)

It is not hard to predict that this situation cannot last. To reiterate: you cannot equip citizens with tools and expect these not be actually used. But if we look around the situation actually seems quite stable, even quite calm. This is because the logic of Ambient intelligence sets forth not only its own disappearance as success, but in doing so builds its own foundation as being ‘natural’, and inevitable. If as a citizen you can no longer fix your own car – which is a quite recent phenomenon - because it is software driven, you have lost more than your ability to fix your own car, you have lost the very belief in a situation in which there are no professional garages, no just in time logistics, no independent mechanics, no small initiatives.

Who are going to distribute themselves into such an environment? An environment that you are being reminded constantly of that is unsafe, and insecure? The mobile industries 3G and 4G PowerPoint presentations highlight a person surrounded by power stations that connect nodes that should give this person more agency. The security industries presentations highlight exactly the same but in their case the agency lies in the nodes, not in the person. For both the systems logic is the same: to distribute yourself, your data - into the environment. The key themes, the cultural and political views that shape the environment are insecurity, un-safety, and fear.

The current dangers of this cultural/political axiom to highlight safety/insecurity as if there could ever be a safe default position, only leads to more fear, more distrust, more anger as incidents will inevitably happen and you will take the blame for not having been able to prevent them. The fear policy goes directly against the call for more and more innovation, whilst innovation needs a risk friendly environment. If you scare your population, very few risks will be taken.

So the main question is which institutions are going to finance and guarantee the stability of the IOT in the current credit crisis?

If it is not carried fully by citizens it is unlikely to be build, so the best option is to start a bottom up open and open source infrastructure, taking the lead in being a real testbed for ambient services that is sustainable, not a hype.

DIFR network:

DIFR has 46 members, meeting bimonthly at Waag Society in Amsterdam and A+R RFID Lab in Den Haag. At its heart lies the “trust paradox”. The paradox asks this question: how can we design our way out of a situation where people need to trust the environment in order for Ambient intelligence to deliver what it promises, while they are being told at the same time that they cannot trust that environment?

The members range from the group of Radboud Nijmegen, who hacked and cloned the Mifare card; Jaap Henk Hoepman; Tijmen Wisman from RFID Platform; Yolande Kolstee from KABK (AR+RFID Lab), Hein Gorter de Vries from GS1, Ben Schouten of Fontys Ambient intelligence; Christian van ‘t Hof from Rathenau Institute, Pieter Rotteveel from Medialab Amsterdam, and Paul Geurts from Hello My Name is E (an application for swapping business cards). In short: an assembly of a group who between them hold all the crucial positions on RFID.

Vital for the success of such a network is the existence of a network of independent

Insert here your organisation name (or your own name if replying on your own behalf)

spaces that are not originating emanating from a university (which in my opinion remain too restricted by its traditional output of research papers and PHDs), nor from a companies (which clearly betray conflicts of interests) or a government (too many different agenda's within different ministries) or individuals (can not guarantee continuity).

In Holland the only place that could host such a network is Waag Society, a media lab that has grown out of the Digital City and Hacktic in the nineties, concerned then with Public Domain on the Internet. Now the society is concerned with Public Domain in the Internet of Things, and as such has a lot of professional expertise in how to connect and frame the differences and oppositions. Most importantly it is a space is able to bring the outer ends of the spectrum; the hackers and the industry together. In 2005 Gill Wildman (Plot) and Rob van Kranenburg hosted a relatively successful seminar on RFID at the Design Council in London which we titled the The Elephant in the Room: Bringing Innovation into RFID Applications.

We talked about how there was no no doubt that RFID has the potential to be a paradigm-shifting technology, we stated and everyone is pleased when they get the technology to work, and that is difficult enough, but they are not building into the pilots the human dimensions that could make the pilots beneficial in a wider way. Rob focused on moving from privacy to privacies, which acknowledged that in a hybrid environment we leave different traces and might want to build temporary personalities around these traces, not exposing our entire personalites all the time. One of the concrete applications we focused on one the idea of having privacy levels on your mobile phone, as we guessed it would have an RFID reader soon. In industry terms you would have a lifestyle manager, in privacy activist terms you would have the equivalent of Melanie Rieback's RFID Guardian – a firewall.

In DIFR we are seeing the first real implementations of looking at RFID from the perspective of citizen empowerment. Using the RFID Guardian, the Radboud vision on revocability and ideas from Moboubiq and foremost from Christian van 't Hof as real and mental models of allowing certain tags to pass and blocking others we can negotiate with the standard organizations and the people who run logistics, pilots in open infrastructures: A consumer sets his privacy preferences in a profile stored on his mobile phone. If he holds the phone close to a product in a shop containing an RFID tag, the phone will read the tag number from the tag. It will then query (over the Internet, either through GPRS, UMTS or WiFi) the backoffice to retrieve the privacy policy corresponding to the tag number. It will then match the tag policy with the consumer policy, and present the result of the match to the consumer on the display of the mobile phone in an intuitive and appealing manner.

See DIFR Demo (funded by open source funder nl.net) at <http://www.difr.nl>

As a starting point we believe it is vital to scale this network to EU level.

Insert here your organisation name (or your own name if replying on your own behalf)