Fact sheet- Ethics Subgroup IoT - Version 4.0¹

Jeroen van den Hove Delft University of Technology Chair Ethics Subgroup IoT Expert Group

Table of contents

Introduction	. 2
What is IoT?	. 2
What are the defining features of IoT?	. 4
Key issues	. 6
Social justice & (Digital) Divides	. 6
Trust	. 8
Blurring of contexts, in particular the distinction Private vs. Public	12
Non-neutrality of IoT metaphors	13
Agency: social contract between people and objects?	14
Autonomy: Informed consent vs. obfuscation of functionality	17
Policy objectives	19
Avoid the emergence of social injustice	19
Establish trust in the IoT	19
Ensure the adequateness of IoT metaphors	19
Creating a social contract between people and objects	19
Allow for informed consent	19
Policy Recommendations	20
Transparency – Vendor Regulation and Certification	20
Transparency – Public Information	20
Research	21
Regulating access	21
Public debate and continuous citizen oversight	21

¹ Contributions to this document have been made by a number of people on the basis of the work of the ethics subgroup of the IoT Expert Group of DG Connect and a number of discussions with a variety of experts in the IoT Expert Group. Contributions were made by Rolf Weber, Ângela Guimarães Pereira, Francien Dechesne, Job Timmermans, Rob van Kranenburg, and Hendrik vom Lehn.

Introduction

The Internet of Things (IoT) can be described as objects around us being connected in order to provide seamless communication and contextual services². In IoT any physical thing can become connected to other things, using and widening the scope of the Internet. IoT is a fabric of numerous connections between things and between humans and things and is thus potentially more complex and dynamic than the Internet. The Internet is already the most complex artefact man has made, IoT goes beyond that. Moreover IoT alters the modes of interaction of humans with things, devices, artefacts and natural objects.

The development towards an IoT is likely to give rise to a number of ethical issues and debates in society many of which have already surfaced in connection with the current Internet and ICT in general, such as loss of trust, violations of privacy, misuse of data, ambiguity of copyright, digital divide, identify theft, problems of control and of access to information and freedom of speech and expression . However, in IoT, many of these problems gain a new dimension in light of the increased complexity.

This paper aims to shed light on this complexity and the ethical and social issues associated with a fully fledged IoT. Although there is a general agreement of what IoT entails in a broad sense, not unlike other emerging ICTs, much of its concepts are still much debated. This lack of conceptual clarity makes it difficult to analyze IoT from an ethical perspective. As IoT is a radically distributed technology, ethical concepts therefore should not be viewed in isolation but in contextualized form to incorporate the dynamics and complexity of time and place independent connections of subjects and objects.

In order to evaluate ICTs ethically in a fruitful way, we use an approach used in the ethical analysis of emerging ICT's that was proposed in the EU funded FP-7 project ETICA³ which aims to deal with complexities and uncertainties inherent to emerging ICTs. Instead of trying to start from a strict definition of a technology, we start from a set of defining features – characteristics uncontroversially associated with a technology. This starting point of ethical evaluation can accommodate the unavoidable conceptual vagueness, disagreement and interpretative flexibility that are typically associated with new and emerging technologies

In this paper, we first give a description of the defining features of IoT, by analyzing the current conceptualizations and prevalent discourse on IoT. This is followed by a short delineation of the ethical analysis. Afterwards, six key ethical issues are discussed. For each of the ethical issues its relation with the defining features is established and an exemplary case is discussed. Building on this, the issue is evaluated from an ethical point of view. Based on these key issues, we point out policy objectives that should be aimed at. We finish this paper, by elaborating on policy recommendations that contribute to these objectives.

What is IoT?

In 2000 the Auto-ID Center and its director Kevin Ashton and collaborators⁴ envisioned "a world in which all electronic devices are networked and every object, whether it is physical or electronic, is

 ² G. Lee, 2012. The Internet of Things – Concept and Problem Statement. Internet Draft, Internet Research Task Force. http://tools.ietf.org/html/draft-lee-iot-problem-statement-05
³ ETICA: "Ethical Issues of Emerging ICT Applications", GA 230318, www.etica-project.eu
⁴ Sarma, S., Brock, D. L., Aston, K. 2000. The Networked Physical World. Proposals for Engineering the Next Generation of Computing, Commerce & Automatic-Identification. White Paper of the Auto-ID Center at the MIT, Cambridge, MA.

electronically tagged with information pertinent to that object. We envision the use of physical tags that allow remote, contactless interrogation of their contents; thus, enabling all physical objects to act as nodes in a networked physical world. The realization of our vision will yield a wide range of benefits in diverse areas including supply chain management and inventory control, product tracking and location identification, and human-computer and human- object interfaces."

Despite disparate definitions of the expression "The Internet of Things", all the different definitions of it have in common that it is related to the integration of the physical world with the virtual world of the Internet⁵. IoT can be broadly defined as a global network infrastructure, linking uniquely identified physical and virtual objects, things and devices through the exploitation of data capture (sensing), communication and actuation capabilities⁶⁷⁸. The underlying infrastructure of virtually represented "things" in an Internet-like structure includes existing and evolving Internet and network developments³. Emerging services and applications will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability³. Potential uses of IoT include the home environment, smart city and health monitoring devices. The RFID technology is at the basis of these developments, but the IoT concept has been considerably extended to a vision that envisages a plethora of heterogeneous objects interacting with the physical environment. "In order to realise the vision of Ambient Intelligence in a future network and service environment, heterogeneous wireless sensor and actuator networks (WS&AN) have to be integrated into a common framework of global scale and made available to services and applications via universal service interfaces."⁹ Amongst the building blocks technologies that play an important role in IoT developments, the following are commonly listed: RFID, Near Field Communication, 2D bar codes, wireless sensors/actuators, Internet Protocol V. 6 and ultra-wide-band or 3/4G¹⁰.

The IoT puts forward a great deal of challenges with regard to its governance, technological options, societal impacts including ethical aspects, which requires it to be thoroughly investigated. In Europe an initiative ¹¹ aiming at a EU policy framework in this domain has started a broad research programme called European Research Cluster on IoT¹², which delivers several studies and a continuous dialogue amongst different stakeholders. Amongst those the European Commission has established an expert group on ethics and IoT to discuss governance, architecture, security, privacy and other ethical issues.

In 2011, Santucci⁷ argued that "the IoT does not concern objects only; it is about the relations between the everyday objects surrounding humans and humans themselves" which requires that an urgent extended debate to all sectors of the society is started on the ethics of IoT. In their opinion on

⁵ Haller, S. 2011. The Things in the Internet of Things. Poster paper presented at *Internet of Things Conference 2010*, Tokyo, Japan. http://www.iot2010.org/

⁶ CASAGRAS report...

⁷ Internet of Things. Wikipedia. Available at: http://en.wikipedia.org/wiki/Internet_of_things

⁸ Miorandi D., Sicari, S., De Pellegrini, F. and Chlamta, I. 2012, Internet of things: Vision, applications and research challenges, Ad Hoc Netw. (2012), http://dx.doi.org/10.1016/j.adhoc.2012.02.016

⁹ From SENSEI project (IoT-A report)

¹⁰ See COM(2009) 278. Internet of Things – An action plan for Europe.

¹¹ See Santucci, G. The Internet of Things: the Way ahead.

¹² http://www.internet-of-things-research.eu/

Ethics of Information and Communication Technologies¹³, the European Group on Ethics in Science and New Technologies asserts that IoT will change *"radically the relationship between humans and the interconnected autonomous objects, giving to the last ones autonomy towards the interaction with human beings"*. The kinds of ethical issues that these types of technology raise are related to autonomy (of things and humans), security (dual use; freedom, liberty), equity / equality / justice / fairness (access; treatment; discrimination / discriminatory interfaces) and others. Commissioner Neelie Kroes has welcomed this opinion, in particular that investments should be made to undertake research on ethical, legal, social and environmental aspects of ICT, specifically mentioning the "Internet of Things"¹⁴.

The aim of this document is therefore to present and to explore on the basis of present day conceptions of relevant values, rights and norms, what are the "ethical issues" arising from the research, development and deployment of IoT. These issues will be illustrated with cases from the literature and the media.

What are the defining features of IoT?

Here we list the characteristics of the Internet of Things relevant to discussions concerning the ethical issues arising from its development and deployment:

- (1) Ubiquity and pervasiveness. The user is engulfed and immersed by IoT and there are no clear ways of opting out of a fully fledged IoT, except for a retreat into a pristine natural and artifactless environment, which will be hard to come by in the remainder of the 21st century.
- (2) Miniaturization and invisibility. The desk top computer as we know it will gradually disappear or will stop to serve as the paradigm case of a computing device. Computing technology will become translucent and has the tendency to disappear from human sight. So although the functionality is prominent and ubiquitous, it will for a good part be inconspiciuous or invisible. This calls for special design measures to make the technology visible and amenable to inspection, audit, quality control and accountability procedures.
- (3) Ambiguity and ontology. The distinctions between natural objects, artefacts and human beings tends to blur as a result of the facile transformation of entities of one type into the other by means of tagging, engineering and absorption into a networks of artefacts. We will have to deal both practically and conceptually with ambiguous criteria of identity and system boundaries.
- (4) Identification: Electronic identity of things and objects achieved by tagging and networking of objects. We will have to get used to the fact that – apart from special and cherished objects and artifacts, many more and seemingly insignificant objects and artifacts will have unique identities. This feature is crucial for the idea of IoT. Who gets to assign, administrate and manage these identities, will access to them and to what they entail in a globalizing world is a non-trivial governance issue.
- (5) Connectivity: High and unprecedented degree of connectivity between objects and persons in networks. High degree of production and transfer of data.
- (6) Mediation and autonomous agency: The IoT environment provides ways of extending and augmenting human agency, even to the point that it may exhibit artificial and spontaneous and emerging agency. IoT environments may present spontaneous interventions in the course of human events which are not directly caused by human agents or operators and

¹³ See Opinion 26 of the 22/2/2012. Available at: http://ec.europa.eu/bepa/european-group-

ethics/publications/opinions/index_en.htm

¹⁴ See Commissioner N. Kroes blog: http://blogs.ec.europa.eu/neelie-kroes/ict-ethics/

which are unforeseen and unexpected. Human beings will act in IoT environments together and in concert with artefacts, devices and systems, thus constituting hybrid systems.

- (7) Embedded intelligence and extended mind: Smart and dynamic objects, with emergent behaviour, embedding intelligence and knowledge function as tools and become (external) extension to the human body and mind. As is already the case to a certain extent with traditional computing artifacts, access the intelligent and data carrying IoT environment may come to be considered as necessary for human agents to get around. Similar to the info available through a mobile phone, and access to your Social Networking Site, people would feel cognitively and socially handicapped.
- (8) Seamless transfer: Interaction, information flow with IoT context will be effortless, with potentially very low transaction and information cost.
- (9) Distributed control: The locus of control and governance of IoT will not be a central one, because of its vast amount of nodes, hubs and data. It will see emergent properties and phenomena, and will have to be governed and monitored in ways adequate for its distributed nature. This has implications for the locus of accountability.
- (10) Big Data: IoT is the locus of tremendous data generation, storage and flow and processing at Exabyte level and beyond.
- (11) Unpredictability and uncertainty: Incremental development of IoT will lead to emerging behaviours without the user having full or even relevant knowledge of the IoT environment.

These defining features individually and collectively give rise to a panoply of ethical issues and are used here in the ethical analysis of IoT to describe the connection of technology to moral and social issues.

Delineation

Not unlike other emerging ICTs, the concept of IoT still is much debated. The boundaries as to what IoT precisely entails are fuzzy and have many overlaps with adjacent technologies such as the Future Internet, Cloud Computing, Mobile Computing and Ambient Intelligence. By focussing on the defining features that are generally accepted among experts and which distinguish IoT from related and enabling ICTs, the ethical analysis can be further narrowed down.

Privacy and Security

Privacy and security issues are considered to be the most important set of ethical issues raised by IoT. As a result they are debated and addressed in depth by the other subgroups of the IoT expert group. To avert redundancy in this factsheet these issues will merely be touched upon.

Key issues

Based on the defining features of IoT, we identified six key ethical issues: social justice, trust, the blurring of contexts, non-neutrality of IoT metaphors, agency, and autonomy. The prominent privacy aspects are discussed in a separate. In the following sections we will relate each of these issues to the defining features, illustrate it by using an example or case and discuss the ethical implications.

Social justice & (Digital) Divides

There are many different conceptions of social justice, yet based on the vast available literature it is most helpful here to focus on fair distribution of benefits and burdens and equal opportunity to access the advantages that IoT may offer. Social justice and equality are enshrined in human rights, freedoms and economic and legal principles worldwide. In this section we look at how defining features may impact our think and acting upon the values of equality and justice The main defining features relevant to the ethical issue of social justice is the new connectivity which arises from device networking, "machine to machine" communication, wireless sensors and the convergence of these with the Internet. The "digital intelligence" embedded in the emerging connectivity of IoT is that of its developers and industry, hence, it does not necessarily include the ordinary user's point of view or representing her chosen lifestyles. The way the network is shaped affects the information position of users and citizens. There is no democratic institutional framework that evaluates the way networks distribute benefits, how it may discriminate and provide differential access. Given the ubiquity, pervasiveness and invisibility of data transactions by the objects of IoT will prevent many from realising how much their lives are shaped by what may become ordinary networked life. Unless investment in transparency and openness of the design and development of IoT is encouraged and realized only an educated elite will grasp, and utilize the types of operations and allocations of information and information positions with IoT.

The levels of promised interconnectivity not only imply high numbers of interacting objects but also a high numbers of actors and institutions involved. Such a situation cannot be grasped by all – see for example the issue of Agency, where Orwell's "big brother" idea is replaced by an abstract "some brother". The fact that there is complex technology that cannot be grasped by lay people is something that we are used to. Next generation nuclear power plants, large hadron colliders cannot be easily explained to citizens, but these are unlike the IoT since they do not make up and shape the the everyday living environment of individual citizens.

Problems arising from unwanted data transfers and processing may result into user distress and even legal appeals as far as accountability is concerned. These IoT defining features may bring about divides that go beyond what is normally described as "digital divide" between the haves and have not's. This will not only happen due to accessibility differences among different segments of the population, but also due to geographical and cultural differences, social structure, institutionalised inequalities, as well as generational gaps in technology appropriation and user agency. However, even if the more sophisticated IoT benefits may be unevenly distributed within the income geography, the dividing issue is likely to arise from other types of access. If no special measures are taken it may be the case that only an educated knowledgeable elite will be actually empowered to make sense, to take informed decisions and to control the (Smart) data transactions that will take place among the myriad of objects of IoT or even to be able to protect those devices. As this is a knowledge divide, the inequalities that will be created being of a different order.

Case/example

A useful analogy could be found in the financial sector. The financial sector has developed in tandem with computing technology. The infrastructures, products and services of financial markets are **a** hard to understand for the average citizen and as it turns out for many financial experts as well. Only after the financial crisis did we come to realize the extent to which we have been depending on complex financial products and services, computer models that gauge the risks, high frequency, high volume and computer supported trading, that could become instable in fractions of seconds give rise

to flash crashes that can lead to loss of thousands of billions dollars in less than a second. The positional arms races in shortening the transmission times between computers and data centers, the understanding with the help of computational and mathematical technology of the risks and opportunities has become a world where equality of opportunity is an empty notion. IoT would generalize in a sense this world of an intransparent computational and artifactual world, that is intelligible only to extremely qualified experts, who are the first to reap the benefits it has to offer.

Ethical analysis

In the analysis that follows, it is assumed that access to the Internet of Things is beneficial for people and that preventing or complicating access to it may cause disadvantages and unfairness as far as knowledge, empowerment, economic prospects and other vital resources for people's well-being, such as education and healthcare are concerned. For the sake of simplicity, we will examine here two types of divides that may arise from IoT deployment. They represent the two sides of the same coin; on the one hand as with other ICT, the possibility of a digital divide, usually referring to differences in group (ethnicity, age, income, education, gender, and other demographic factors) access or usage of ICT within single nations or across nations; and a more paradoxical divide which we will call a "knowledge divide", arising from the progressive disempowerment and deskilling provoked by the ubiquitous and invisible (smart) automation of data transactions, management of such transactions among objects and associated activities that IoT promises.

The Digital Divide¹⁵ concept emerged during the 1990's with the realisation that many did not have access to the Internet and therefore were left out from a burgeoning place of data and information transactions, knowledge creation, etc.

The Internet and data networking has increased interdependencies of actors and dependency on means to govern such interdependencies; so, as with the Internet, will IoT raise social integrity? Or will it contribute to social disparities and increase potential conflicts and raise the digital divide, instead?

The "digital divide" is seen as one of the challenges for the development of IoT at policy level. Although, a great deal of this technology will be imposed onto people (a good example of this fact, being the "smart" *movement*, such as small and large scale applications like Smart Cities and Smart Grids, Intelligent Transport, eHealth, Intelligent Manufacturing), the diffusion of and access to IoT technologies will be different according to global geography and is likely to permeate and transform work and leisure patterns, engagement in civic and political activities and people's quotidian, at different paces, even in Europe. It must be noted that this is not likely to be about the "objects" per se but about equal access to health, education, and other vital resources. The actual possession of "things" is probably the least relevant.

IoT could easily end up reinforcing the divide between capable users and those intimidated or outpaced by new technology. In here, we will go beyond the commonly described "digital divide", describing other diffuse divides that the unauthorised and unquestioned automations, seamless transfers and unnoticed ubiquity featured by IoT may create due to overwhelming consent demands. The divides in this case are not exclusively related to lack of skill, but also to what we could call "consent fatigue". If ever asked, the ordinary user may not have the time to keep pace with all consent activities she needs to respond to. This is even more serious for the individuals that have reduced autonomy such as "special needs people", children and the elderly.

With IoT, where the kinds of promised interconnectivity involve billions of "objects" and transactions for which mechanisms of authentication and consent need to be put in practice, much attention has to be put on this issue. So, those who are knowledgeable and skilled enough and empowered to

¹⁵ The commonplace definition of "digital divide" comes from the US National Telecommunication and Information Administration's (NTIA) "Falling Through the Net" policy report series issued during the Clinton administration.

control the working of the technology will be able to protect themselves against abuse, and to choose amidst the technological offer or opt-out if they deem it necessary. Hence, the rising divides in these cases have, paradoxically, implications for knowledge production, skills development and empowerment. Those who cannot keep the pace with the pervasiveness will progressively become deskilled, disempowered and less knowledgeable. This latter situation, however dramatic it may sound, already occurs today with objects as mundane as home appliances, cars, etc. where sophisticated electronics have progressively prevented ordinary users from resolving even small malfunctions. Some have described this trend of substitution as the *incompetence trap*¹⁶: when technologies do what people could do themselves, de-skilling people and make people more dependent on experts and tools. It appears as though that after a flourishing democratisation of knowledge production momentum especially with social media, IoT could become the epitome of control and disempowerment: the space for knowledge co-production and creativity could be more controlled and confined with IoT. Therefore, there is an urgent need for a wide debate that involves all stakeholders to understand by what values present and future generations will like to live and what kinds of knowledge production need to be protected. Additionally, the IoT developments should ensure openness to avoid these types of divide.

Moreover, the diffused control of IoT raises issues of responsibility and also of accountability – the latter dealt with in this Fact Sheet. Those with resources may be able to trace what data and where their data is being processed and in which transaction is participating and act accordingly. Again, this divide arises as a "knowledge divide".

As for Internet and computer access today, it is still a small fraction of the population that has knowledgeable and regular access to it; or put in other words, benefiting from the whole set of opportunities that Internet access offers. Although, the character of the IoT is heralded as ubiquitous, not all people will have access to all promised functionality, given the divides described above. And if that is so, the inevitable question is, what is that that people are missing when they do not benefit from access to the IoT? What kinds of alternatives are put in place in order to guarantee that those that voluntarily (or not) are not engaged in the web of device communications and sensing do not get hampered with their lifestyles, hindered with personal endeavours or even excluded from their communities?

Other ethical issues may arise from violation of specific rights. IoT can potentially set the grounds for violations of Article 21 of the European Charter of Human Rights on "non-discrimination", since as we have seen with other ICT developments, phenomena like *profiling* and *target advertisement* are at the basis of seemingly discriminations already. Article 8 "protection of personal data" where "[...] data must be processed fairly for specified purposes and on the basis of the consent of the person concerned [...]" could be vulnerable to the issues discussed above on "knowledge divide".

It should also be important to see how core IoT features such as seamless transfers and distributed control deal with the recently proposed provisions for rectification and erasure in the proposal for a new legal framework for the protection of personal data in the EU (COM(2012) 11 final), which includes the "famous" right to be forgotten and to erasure (Article 17).

Trust

Another major concern with IoT is public trust in the technological system. When boundaries between public and private spaces get blurred, and are invisible, users would feel a sense of unease: they do not know what information they actually share with whom, which raises the question of trust. The fear of privacy infringement, the idea of an omnipresent network, and reliability issues challenge trust in IoT. Therefore, IoT and its applications should be designed to be trustworthy. This includes effective technical functioning, protection of personal data against attacks and theft,

¹⁶ In Crabb, P. B, 2010. Technology traps: who is responsible? Technoethics. 1(2).

ensuring privacy and providing usable security management. This should be taken into account right from the beginning of the development rather than as add-on features. As Jim Clarke pointed out, *"the failure to enhance trust [...] may result in suspicion and eventual rejection of new technology [...]*^{*17}.

IoT generally is depicted as building on the Internet we have today and therefore raises similar trust issues. But IoT also has distinct features that diverge from the current Internet and that influence the assessment of trust. IoT promises to be highly distributed, dynamic and ubiquitous (everything communicates and interacts; no boundaries, new entities can enter the IoT at all times) which makes establishing trust among entities essential, but also difficult as entities will have to engage, relate and negotiate with unfamiliar entities. Furthermore non-human entities are predicted to display some form of smartness or autonomy and behave in undetermined ways. Together with the lack of homogeneity and the hierarchical structure of Iot networks, this calls for an evaluation of what it means to trust a thing, person or service in an IoT context.

Case/example

The Netherlands has learned interesting lessons about ethics and innovation in the first decade of the 21st century. A first instructive case was the attempt to introduce smart electricity meters nation- wide. In order to make the electricity grids more efficient and meet the EU CO2 reduction targets by 2020, every household in The Netherlands would have to be transformed into an intelligent node in the electricity network. Each household could thus provide detailed information about electricity consumption and help electricity companies to predict peaks and learn how to "shave off" the peaks in consumption patterns. After some years of R&D, a plan to equip every Dutch household with a smart meter was proposed to parliament. In the meantime however, opposition to the proposal by privacy groups had gradually increased over the years¹⁸. The meter was now seen as a 'spying device' and a threat to the personal sphere of life, because it could take snapshots of electricity consumption every 7 seconds, store data in a database of the electricity companies for data mining, and provide the most wonderful information about what was going on inside the homes of Dutch citizens. With some effort it could even help to tell which movie someone had been watching on a given night. By the time the proposal was brought to the upper house of the Dutch parliament for approval, public concern about the privacy aspects was very prominent and the upper house rejected the plan on data protection grounds. The European Commission, being devoted to the development of smart electricity grids in its member states, feared that the Dutch reaction to this type of innovation would set an example for other countries and would jeopardize the EU wide adoption of sustainable and energy saving solutions in an EU market for electricity¹⁸.

Ethical analysis

Concept of Trust

Trust is a concept that carries different meanings in different disciplines. One definition of trust is the "accepted vulnerability to another's possible but not expected ill will (or lack of good will) toward one" ¹⁹. Thus, we trust when we are vulnerable to harm from others, yet believe these others would not harm us even though they could. It is generally accepted that a climate of trust eases cooperation, cuts transaction cost and fosters reciprocal care-taking. The resources—physical,

¹⁷ Clarke, J., (2008) Future Internet: A Matter of Trust: eMobility Newsletter,

http://www.tssg.org/eMobility_Newsletter_200811.pdf accessed 27th July, 2010.

¹⁸ AlAbdulkarim, L., Lukszo, Z., & Fens, T. Acceptance of Privacy-Sensitive Technologies: Smart Metering Case in The Netherlands. In Third International Engineering Systems Symposium CESUN 2012 (June 2012).

¹⁹ Baier, A.C. (2004) "Demoralization, Trust, and the Virtues," in Calhoun (ed.) 2004. Friedman, B., Khan, P.H., Howe, D.C (2000) Trust online. Commun. ACM 43, 12 (December 2000)

emotional, economic—that would otherwise be consumed guarding against harm can be directed toward more constructive ends. E-trust, any instance of trust between people involving online communication, has been the focus of many recent studies²⁰. Examples of e-trust include trusting as true what is said on a website or blog, trusting that the operators of an e-commerce site will deliver the promised goods, trusting that a person has described themselves accurately on a dating site, trusting that sponsored results to a search engine enquiry are highlighted as such ,or trusting that an email is from whom it appears to be.

Reliability vs. Trust

Pettit²⁰ analyses 'trust' to be a species of the more generic phenomena 'reliance'. This theoretical difference²¹ is interesting with respect to IoT, because it helps to distinguish between thing-person interactions and mediated person-person interactions both supported by IoT. "Relying on [something or] someone to display a trait or behaviour is just acting in a way that is shaped by the more or less confident belief that they will display it." (p. 162) Relying can be either interactively static or interactively dynamic. Only in the second instance it amounts to trust. Interactively dynamic presupposes that: the entity on whom a person relies is aware of that fact that that person relying on that entity to display a certain trait or behaviour and that in revealing his reliance in this manner, the person relying must be expecting that it will engage the disposition of the trusted entity, giving it an extra motive or reason for being or acting as is expected²⁰. In the foreseeable future these conditions only will be met by actual persons thereby excluding things from being trustworthy. A reliance relation with a thing in these terms is always interactively static as the trusted entity has no awareness and is not able to engage a disposition or be motivated like a person. This suggests the limits to establishing trustworthiness amongst people via IoT. Only in a mediated sense of online identities can such relationships be established. The three requirements that need to be fulfilled in case IoT should offer a milieu or context in which relations of trust can help developing such a milieu online. The discussion on reputation systems below can be viewed in this light. Furthermore, in object-object interactions and in object-person interactions that lack fulfilment the dynamic interaction conditions only a certain level of 'generic reliability' is attainable. Reliance then is a measure or level of confidence a person or thing displays towards another thing or person acting in a certain way.

Confidence vs. Trust

Another distinction that is insightful in analyzing trust in relation to IoT is between confidence and trust. The disappearance of physical boundaries between systems enabled by technology most notably the Internet, calls for the establishment of explicitly designed virtual boundaries between (sub-) systems. Building on the work of system theorist Luhmann, this will lead to paradigm shift in conceptual terms as well: from passive to active insulation of data and systems, from danger (not manmade) to risk (manmade) and from confidence (no alternatives) to trust (with alternatives). Again, a more pro-active stance is being called for as trust and risk stem from human (design-) choices, and thus suggest taking responsibility for the consequences of those choices.

Trust negotiation

An analysis of trust issues in IoT can also be based the more narrow definition of trust as referring to 'security policies regulating access to resources and credentials that are required to satisfy such policies'²⁵. In that way secure interaction requires the establishment of a process of credential exchange that 'allows party requiring a service or a resource from another party to provide the necessary credentials in order to obtain the service or the resource.'²⁵ Only after a successful trust

²⁰ Pettit, P. (2008) Trust, Reliance and the Internet. In Information Technology and Moral Philosophy(2008), Jeroen van den Hoven and John Weckert (Eds.). P 322-353

²¹ In literature- also the literature reviewed in this article- the distinction between trust and reliance suggest in this section is not used. Trust and reliability are often not that clearly demarcated or even used interchangeably.

negotiation in which digital credentials have been exchanged and verified, mutual trust can be established. The dynamic and distributed nature of IoT makes trust negotiation very challenging as compared to the classic centralized and static approaches as no trust relationship is defined a priori²⁵. Furthermore, just as it is the case on the Internet, globally accepted certification authorities need to be established that facilitate the certification process on the IoT²⁵.

Impact of IoT

IoT technology can be used ubiquitously encompassing persons, things, plants and animals^{22 23}. As a result malfunctioning IoT technology may entail a much greater impact than traditional Internet services would have. Whereas consequences of a virus or hack in traditional Internet applications would mainly have a negative impact on the virtual realm, for instance corrupting data, a virus or hack in a IoT can directly impact the physical realm, have consequences in the 'real life' of people. A hack of a personal computer may lead to an intrusion into someone's privacy, but a hack into the control system of a smart car can mean that the passengers' safety is at risk. These real life risks imply that reliability and trustworthiness are important matters for IoT, even more so as compared to traditional Internet applications. Only when trust and reliance criteria are satisfied, end-users can be expected to be open to adaptation of such disruptive new technology.

Design-time vs. run-time

More and more things in the IoT are predicted to display automated or even autonomous behaviour²⁴. Context awareness and adaptation in combination with Artificial Intelligence enable things to act without human intervention at run-time in ways that cannot be predicted beforehand during design-time. Devices such as mobile telephones, 'wearables' like intelligent accessories and textiles, for instance, are able to interact with their environment by automatic recognition and autonomous processing of repetitive tasks without user intervention²³. Decision-making, instead of being centralized becomes decentralized with the objects interacting autonomously in heterarchical structures²⁴.

This not only raises responsibility issues but also further questions whether things or networks of things can be trusted or relied upon to function in ways users expect them to function. What is more, users may experience a loss of control due to systems autonomous behaviour. Although they are dependent on a system users are not able, aware, or lack the technical expertise to interfere with the system. As a result users may experience loss of control and accompanying feelings of helplessness that undermines their trust in the system (Bohn et al., 2005 in Friedewald, 2010).

Open vs. closed

IoT will enable dynamic configuration of networks of objects supporting changing relationships amongst things and services working together. It can therefore be assumed that no trust relationship is defined a priori among the entities in the system²⁵. This dynamic and distributed nature of IoT makes addressing trustworthiness very challenging indeed. With objects also displaying autonomous behaviour, the establishment of trust relationships among human and objects surrounding them needs therefore be prioritized²⁵. Dynamic configuration is only feasible when entities that interact are able to reach a level of trustworthiness that they are confident about the consequences of them engaging in some form of interaction. What's more, obfuscation of things common in IoT together with the enormous diversity of objects exacerbate difficulties for entities to know with whom they

²² Weber, R.H. (2010) Internet of Things – New security and privacy challenges, Computer Law & amp; Security Review, Volume 26, Issue 1, January 2010, Pages 23-30

²³ Friedewald, M. Raabe, O. (2011) Ubiquitous computing: An overview of technology impacts, Telematics and Informatics, Volume 28, Issue 2, May 2011, Pages 55-65

²⁴ Uckelmann, D., Isenberg, M., Teucke, M., Halfar, H. (2010) Autonomous Control and the Internet of Things: Increasing Robustness, Scalability and Agility in Logistic Networks, 163-181

²⁵ Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I. (2012) Internet of things: Vision, applications and research challenges, Ad Hoc Networks, Volume 10, Issue 7, September 2012, Pages 1497-1516

are communicating/interacting in changing network configurations. In order to provide its service to an end-user, a thing may come to rely on other services and things that over time may be different from the ones that are known to the end-user and/or without the end user being aware of this. Again establishing trust relations in IoT is further complicated while at the same time the need to enhance trustworthiness increases, as control of end-users over the services diminishes.

Reputation systems

A proven way for supporting the establishment of trust relations on the Internet in a dynamic context with rapid changing interactions is the use of reputation systems. In his analysis of trust, Pettit²⁰ argues that three forms of evidence are needed to be able to engage in the dynamic interaction needed to establish real trust amongst persons. Reputation systems such as can be found on Amazon, Slashdot or E-bay provide a possible technical solution to fulfil this condition by supplying sources of 'evidence' of behaviour or performance of other users as well as a reason for those users to live up that evidence as preservation of their online reputation depends on it.

Research should be conducted on how reputation systems can contribute to establishing reliability and trust in an IoT world. The distinct features of IoT however pose additional challenges. The open and distributed character of IoT as opposed to the closed and centralized character of existing reputation systems such as that on E-bay, pose additional challenges.

One domain which has to cope with similar difficulties are Peer-to-Peer (P2P) systems. In P2P filesharing applications, the problem of free-riding led to the development of distributed protocols which establish trust-relationships between the peers²⁶. But also for Wireless Sensor Networks (WSNs), trust and reputation schemes have already been developed²⁷, leading to first results for the domain of the IoT²⁸. Existing work within these two areas might therefore serve as a starting point when developing distributed reputation systems for the IoT.

Blurring of contexts, in particular the distinction Private vs. Public

A characteristic feature of the IoT is that it contributes highly to the degree of mediation by (information) technology of our interaction. Mediated environments such as your kitchen, your living-room, our shopping malls, the streets of old villages, websites, schools or p2p networks, are new beginnings as they reformulate our sense of ourselves in places, in spaces, in time. Our everyday environments are effectively the interface and we must learn anew how to make sense.

We must investigate the possibility that IoT generates authentically new situations and experiences in which the notions of privacy and data protection can no longer do all the moral work. In a mediated environment – where everything is connected to everything - it is no longer clear what is being mediated, and what mediates. What is the meaning of autonomy and responsibility of the human individuals acting on their own or jointly in such an environment?

IoT promises to be a highly dynamic, bottom-up technology, which allows for changing configurations. In order to enable this, the objects need to carry identities which are somehow stable

²⁶ Cohen, Bram. "Incentives build robustness in BitTorrent." Workshop on Economics of Peer-to-Peer systems. Vol. 6. 2003.

²⁷ Boukerche, Azzedine, and Xu Li. "An agent-based trust and reputation management scheme for wireless sensor networks." *Global Telecommunications Conference, 2005. GLOBECOM'05. IEEE.* Vol. 3. IEEE, 2005.

²⁸ Chen, Dong, et al. "TRM-IoT: A trust management model based on fuzzy reputation for internet of things." *Computer Science and Information Systems* 8.4 (2011): 1207-1228.

and context independent. Integrity can be defined as the accuracy of one's actions, which implies that actions are carried out in accordance with the norms and agreements that hold in a certain context.

Case/example

IoT, by its extreme interconnectedness, enables devices to communicate across the boundaries of the contexts we are used to and within which we have agreements on interaction and information norms. The notion of context and contextual integrity are central in the analysis of the notion of privacy in relation to information technology. In particular, the dividing line between what is public and what may assumed to be private, runs the risk of gradually shifting to reduce the private sphere. This is demonstrated for example in the case of smart metering, which concerns the public good of energy: the smart meter can both be seen as part of the private sphere -physically within the home, behind the closed doors, storing information on private behaviour- and of the public sphere: the information is increasingly necessary for fast, efficient and reliable distribution of electricity.

Ethical analysis

We see that boundaries between contexts, that have grown explicitly or implicitly over decades, disappear: the perimeter of a context, keeping certain information or actions restricted to the boundaries of a particular restricted type of interaction, may silently disappear by technology that is as ubiquitous and interconnective as IoT.

Such de-perimeterisation associated with converging technologies²⁹ challenges the checks and balances associated with the separation of powers in our democracy.

Non-neutrality of IoT metaphors

To deal with the complexity of the IoT technology, and uncertainties on how it will develop, IoT is explained through analogies with existing systems and metaphors. This steers the perception of the technology by the public and the (direct) stakeholders, and may even impose an ideology: the terminology in which IoT is (speculatively) presented to policy makers and the public is not neutral.

As in general with emerging technologies it is a challenge to characterize the technology while it is still emerging. This is an epistemic problem: to which extent is it even possible to know what we are talking about? It should be carefully monitored whether the analogies used, the `framing', remain adequate as the technology develops. One should also prevent that the power of the metaphors is used by any of the stakeholders to hamper the possibility to form an autonomous and well-informed judgment. In particular, one should be careful not to treat expectations for IoT as facts, nor have concerns people raise with respect to IoT definitively dismissed, on the basis of the current narrative we use to get a grip the uncertain future development.

The way in which we frame IoT determines to a great extent how we will develop IoT governance. Standardization issues require a centralistic (top-down) approach, while a perception of IoT in terms of smart interconnected objects suggests a strong decentralization, which requires policies fit for such bottom-up, dynamically evolving system.

Many metaphors used to describe the IoT revolve around the question of how this emerging technology will ease everyday life. Central from this point of view is the ubiquity with which IoT technology is expected to be embedded in regular living spaces, thereby connecting virtual and real

 ²⁹ Wolter Pieters, André van Cleeff (2009). The Precautionary Principle in a World of Digital Dependencies. In Computer, vol.
42, no. 6, pp. 50-56, May 2009, doi:10.1109/MC.2009.203

realms. As the embedded intelligence helps to fulfil everyday tasks in a fully automatic fashion, a hybrid agency on behalf of the user comes into being.

Case/example

In the case of IoT, it is particularly important to keep distinguishing whether the `things' can be considered to be actors (rather than passive objects), and if so, to which extent they can act autonomously. In particular, the combination with the term `smart' raises expectations as to the status of the things in the interaction with its environment, including people. Can these things be attributed some form of responsibility or accountability? How to regulate that?

An example for this is the 'smart' refrigerator, which is often used to illustrate the advantages of the IoT³⁰. The refrigerator knows what is stored in it and automatically orders new products on behalf of the user. This metaphor nicely illustrates the conveniences that the IoT may bring. Many important aspects, such as the user's privacy, the dependence on this technology or possible financial liability for wrongly ordered products, are, however, not discussed in most of the descriptions.

Ethical analysis

To broaden the boundaries of reflection and to be able to frame the issues surrounding IoT, a new ontology must be constructed that affords to discuss and evaluate the issues raised in this document, rather than incorporating a particular viewpoint on them.

So, amongst other things, it should enable capturing a 'new self' of users encompassing both their analogue and virtual selves. The boundaries between traditional entities such as end-users, government agencies and corporations are blurring. Hybrid entities will occur sharing a selection of qualities from different traditional entities. As a consequence ownership of data and systems becomes less straightforward and may be institutionalized via leasing constructions instead of ownership. Also the western individualistic outlook may come under pressure as IoT seems to have a more collectivistic outlook. An important development that contributes to and further instigates these developments is the development of open standards in IoT, both in terms of data, software and hardware design.

The new ontology must also be able to support the articulation of both current as well as future values that come into play. A network approach can be used to depict different realms that intersect as IoT takes shape. Besides a local area network (LAN), e.g. around a refrigerator as a hub, a wide area network (WAN), e.g. with a car as a hub also a Body Area Network must be taken into consideration supported by a medical device for instance an smart hearing aid. Within this approach questions arise how the networks intersect and how and where they are fenced off from the outside. A balance should then be struck between synergy and freedom with and across networks on the one hand and security and privacy on the other.

Agency: social contract between people and objects?

In this section, we will look at two interrelated aspects of human agency in an environment where objects act and decide in invisible but intentional ways, on behalf of human users. Agency becomes an ethical issue when the intentionality of delegated actions is not fully controllable by the user, does not identify with the user's identity and compromises her integrity and eventually her freedom.

The main defining features of interest to this ethical issue include the high degree of connectivity, which implies that a myriad of entities are interconnected and interacting; this is not only about

³⁰ Kominers, Paul. "Interoperability Case Study: Internet of Things (IoT)." *Berkman Center Research Publication* 2012-10 (2012).

objects but also about actors and institutions involved. Such a situation (which may not be grasped by all – see digital divide issue) amounts to a replacement of Orwell's "big brother" idea by an abstract "some brother" ³¹ concept. The pervasiveness and ubiquity, invisibility, seamless transfers and strong mediation features of IoT imply delegation of actions and decisions by users. It moreover leads the user to stop noticing presence, transactions, and eventually actions are taken on her behalf. This situation sets the grounds for loss of control, disempowerment and potential unauthorised actions. Who the agent (user or object?) is, becomes object of controversy. After all, objects become agents of their developers' worldviews and morals. *Unpredictability*, described as unpredictable emergent behaviours due to potentially accessible IoT infrastructure from anywhere at any time³²; as there will always be incremental developments and deployments, leading into emerging relationships and behaviours without the user having full realisation, unpredictability remains a key feature as far as the discussion on agency is concerned.

Case/example

Again, the smart refrigerator³⁰ illustrates this aspect. Since the refrigerator autonomously orders products on behalf of the user, one can speak of a social contract between the user and the refrigerator. But when exactly does the refrigerator place a new order? Without limiting the user's convenience by having her configure a complex configuration-system, the user will likely not know the exact details of how and when products are ordered, unless specific design measures are taken to design an over-ruling option, an opt-out or a particular default setting determined by the user. Standardization battles and debates are to be expected here as are now going on about privacy setting for Social Networking Sites.

Ethical analysis

In this analysis we are assuming that values, moral and human rights sustain ideas of autonomous choice and action, which inherently characterise human beings as still cherished by all citizenry. Therefore, we will look at how some defining features of IoT may interfere with the ethical issues, autonomy and agency of both humans and the "things" of the IoT. Human autonomy and agency are constitutional human values being explicitly enshrined in the European Charter of Human Rights and European purposeful regulation about digital life.

IoT defining features include strong mediation, through both embodiment and hermeneutic relations between humans and artefacts³³. In the former, the "artefacts" are incorporated by users, becoming extensions of the human body or mind enhancing the interface between humans and the environment (a most common example are glasses); in this type of relations the artefacts are not perceived. Hermeneutic relations on the other hand refer to relations where the artefacts provide a representation of reality requiring interpretation; decisions being taken based on such interpretation (e.g. a thermometer). With IoT both types of relationships are emphasised and hybridised; users are likely to stop "noticing" the artefacts (sensors, RFID, etc.) that communicate among themselves in *autonomous* ways, and at the same time many of these artefacts encapsulate representations of reality through the algorithms and models driving their activity. This latter condition, amounts to a deeper form of not "noticing" technology; it is not only about the artefact but also, more importantly, about the invisibility of the interaction itself (data transfers, decision and action). Voluntarily or not, the user will need to rely on models and technology to achieve the chores that technology is meant to help her with³⁴.

³¹ Mannermaa, M. 2007. Living in the European Ubiquitous Society. Journal of Future Studies 11(4):105-120.

³² In Wrigth et al. (EDS). 2008. Safeguards in a World of Ambient Intelligence.

³³ In Verbeek 2006, quoting D. Ihde. Verbeek, P-P. 2006. Materializing Morality. Design Ethics and Technological Mediation, Science, Technology & Human Values. 31(3). Pp. 361-380.

³⁴ Stahl, Bernd Carsten. 2011. IT for a Better future: how to integrate ethics, politics and innovation. Journal of Information, Communication & Ethics in Society 9(3). Pp. 140-156.

Hence, the strong mediation inherent to IoT developments, will lead eventually to shifting or delegation of human autonomy and agency to the objects of the IoT. If noticed, artefacts will act on the user's behalf; if not noticed artefacts will act on their developers' worldviews, intentionality and interests. This strong mediation poses challenges to human agency.

Profiling became the nightmare of social and legal scholars with many recent ICT developments. Profiling puts in jeopardy people's autonomy and agency, amongst others. High level of connectivity, seamless transfers and embedded intelligence of objects and machines cannot but make one think of scenarios where human autonomy about even mundane decisions and activity is put in jeopardy. Profiling is an algorithmic procedure over data; it follows the logic of identification, categorisation and clustering of those who developed the algorithms used for such purpose. But such algorithms are blind to specificities of individuals. They act with indifference with respect to context in which the data they use are collected. In Kafka's "The Trial", Joseph K. gets arrested by unspecified agents and gets entrapped in judiciary machinery without reason or due process for an unspecified crime. The loss of autonomy that IoT features could lead to a scenario where the human indifference in Joseph K.'s story is overridden by the indifference of the "things" collecting and storing our data, forming a multiplicity of 'dossiers' on our whereabouts that may be used in unexpected contexts^{35 36}. Profiling is about "being identified", but such identification is established upon the individual corresponding to lack of an individual's autonomy to establish her/his public self-image (personality, identity); with the IoT promised levels of data transactions and embedded intelligence, profiling will lead yet to another level of disempowerment: the crucial issue is not abuse, but the fact that users will have no effective means to know whether and when profiles are used or abused³⁷. So, caring, medicating, reminding, buying, selling, messaging, etc. may all stem from autonomous procedures of the IoT "things" lead by categories of identity with which potentially the user may not identify herself and which the user will most certainly not be aware of; as with Joseph K., users could be tangled on processes with which they have nothing to do and what could be worse, no one to get support from, not even from a smart object. Hence, profiling as in other developments of ICT, poses several threats to autonomy and therefore challenges human agency. In IoT we need at least the same kind of attention for the issue of data profiling as in other current and emerging ICT.

In the ubiquitous world of IoT there won't be the Orwell's "big brother" to blame or to refer to; a myriad of human and artificial agents are implied in the interconnected smart artefacts and machines promised in the IoT world view. Such developments will lead to a "*Some brother controls, knows and never forgets society*"³⁸. "Some brother" is not a single agent, but a heterogeneous "mass" consisting of innumerable social actors, e.g. public sector authorities, citizens' movements and NGOs, economic players, big corporations, SMEs and citizens.

The diffuse nature of the interactions, which inevitably results in changes of a user's agency with regards to artefact-to-artefact or machine-to-machine interactions, will imply opacity when it comes to decide on agents' responsibility, accountability and eventually agents' liability. Many scholars have used Brentham's *Panopticon* to describe how users will be constantly visible and "solicited" by invisible (and unverifiable) requests of "some brother" in the IoT world. Paradoxically, however invisibility is a defining feature of IoT; but if a *Panopticon* scenario for IoT is plausible, how will IoT developers deal with the intolerable idea of invisibility in the "things" interaction? How can we guarantee identification of all agents involved in the data transactions, veiled decisions and actions in order to ensure that attempts to violate human rights, EU legislation or other principles of our present human condition are diabled from the outset?

³⁵ De Hert, P. **A right to identity to face the Internet of Things**, p. 5 at http://portal.unesco.org/ci/fr/files/ 25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf

³⁶ M. Hildebrandt and S. Gutwirth (EDS), 2007. Profiling the European Citizen. Cross-disciplinary perspectives.

³⁷ Hildebrandt and Gutwirth, op. cit.

³⁸ Mannesmma, op. cit.

In here we would like to look at objects agency and so, we look at the intentionality implied in objects' activity and what we can call a "contract" between objects and people. The IoT defining features that interest this issue are embedded intelligence, seamless transfers and unpredictability³⁹. The roots of the ethical challenges with relevance to agency that we describe in this section are similar to those described in the earlier section "profiling yet again".

To which extent is there in the interconnected world of IoT conceptual equality between people and objects with respect to intentionality? Are people and objects just connected physically and causally, or also intentionally or symbolically? Can we attribute dignity or responsibility to objects? Numerous current examples of ICT developments include devices that take autonomous decisions (for example, in healthcare or search and rescue situations⁴⁰), the moral qualities of which are preestablished in algorithmic ways. Many automated technologies make it unnecessary and often undesirable for human users to exercise control over their own behaviour; this is what has been termed the self-miscontrol trap⁴¹, i.e. a failure of peoples' self-control when their behaviour is controlled by technological devices rather than by social and moral norms. People are often compelled to use technology as something inevitable otherwise risking to be isolated; up until recently we could argue that it is the users' appropriation of technology that dictates major categories of intentionality, responsibility and accountability. With the promised automation in IoT, this attribution can be at least questioned; in an IoT world vision, intentionality is at most shared among creators, designers and users of technology. All human agents need to be identified for their intentionality, the morals they sustain, otherwise the risk is that no responsibility can be attributed once the objects mediate and operate within an IoT.

Other ethical issues may arise from violation of specific rights related to agency and autonomy. IoT can potentially set the grounds for violations of Article 21 of the European Charter of Human Rights on "non-discrimination", since as we have seen with other ICT developments, phenomena like profiling and target advertisement are at the basis of seemingly discriminations already. Article 8 "protection of personal data" where "... data must be processed fairly for specified purposes and on the basis of the consent of the person concerned..." could be vulnerable to the issues discussed above on "intentionality" and the "some brother" concept.

The right to integrity of the person (Article 3 of the the European Charter of Human Rights), relies very much on the autonomy of the person. Challenging people's ability to take decisions and exert their agency may compromise their integrity.

Autonomy: Informed consent vs. obfuscation of functionality

IoT has a tendency – just like other infrastructures or as public utilities to become translucent⁴² and to disappear from sight, only to emerge and reappear again when they break down or fail to deliver the public goods. This applies to electricity, water, gas and telecom services. Our lives crucially depend on them and they are often taken for granted and assumed to function properly. This disappearance from sight is even more striking in the case of Internet of Things. Here the tags, sensors and micro electronics supporting the IoT move towards the nano-scale and literally disappear from sight. This amounts to a conspicuous obfuscation of functionality. If we want to make it visible for inspection again special design countermeasures need to be taken.

³⁹ Objects and services potentially accessible from anywhere at any time, may result in unpredictable emergent behaviours see for instance, Wright *et al., op. cit.* in their discussion of ambient intelligence's key characteristics.
⁴⁰ In Stahl, Bernd Carsten. 2011. *Op. cit.*

⁴¹ In Crabb, P. B, 2010. Technology traps: who is responsible? Technoethics. 1(2).

⁴² Bowker, Geoffrey C., and Susan Leigh Star. Sorting things out: classification and its consequences. MIT press, 2000.

Case/example

This translucence can occur in two forms: Everyday 'smart' objects like a toaster, the refrigerator or a car are well visible, but may be perceived by the user as an ordinary object without intelligent capabilities. Furthermore, the development of 'smart dust'⁴³ actually aims at the development of wireless sensor nodes that are rarely visible. In either case the user will probably not be aware of the functionality being present, which breaches the principle of informed consent.

Ethical analysis

The invisibility of the IoT-technology may obfuscate its exact workings to the user: there will be a dissonance between what a user knows about what happens, and what actually is happening. Different stakeholders will have different epistemic requirements with respect to interaction with the technology. It can be argued that informed consent by IoT users or indirect stakeholders can be difficult if technical knowledge is required. The question then may arise how information on the working, effects and risks of the technology should be presented. This holds especially since users form a diverse group with different choices, needs, knowledge and epistemic capabilities. Transparency might be difficult to achieve even for experts and therefore taking and assigning responsibility becomes problematic.

⁴³ Warneke, Brett, et al. "Smart dust: Communicating with a cubic-millimeter computer." *Computer* 34.1 (2001): 44-51.

Policy objectives

The key issues identified in the previous chapter each depict one or several states with regard to the development of IoT technology. While some of these states are actually desirable to happen, others should be avoided. In order to develop policies which aim at steering the development in the desired direction, we formulated a number of policy objectives based on the aforementioned key issues.

Avoid the emergence of social injustice

Future developments and the use of IoT bear the risk to lead to a societal divide between those who have and those who don't have access to IoT technology. Besides this *digital divide*, there is also the risk of a *knowledge divide* separating those who have the knowledge to master the new technology from those who are dependent on experts. One policy objective is therefore to avoid the emergence of social injustice due to a digital or a knowledge divide. Besides a fair access to IoT technology and the qualification of citizens to make use of it, it is also necessary to provide alternatives to those citizens who (voluntarily) do not want to get engaged with the IoT.

Establish trust in the IoT

Another objective for the introduction of the IoT is to design the technology in such a way that users can establish trust in it. To that end, an effective technical functioning, the protection of personal data, ensured privacy and usable security management are of importance. Only when those objectives are fulfilled, users will be able to trust and accept IoT technology surrounding them.

Ensure the adequateness of IoT metaphors

In many cases metaphors, such as the intelligent fridge, are used to explain the manifold advantages the IoT is about to bring. Researchers and industry have to ensure that these metaphors not only highlight the conveniences of the IoT, but also shed light on the dangers that come with it. Furthermore, the development of these metaphors has to keep up with the development of the technology itself.

Creating a social contract between people and objects

The issue of objects agency questions current understandings of the social contract between people and the (smart) objects surrounding them. When people use the things in the IoT, they effectively delegate actions to objects. In such a situation it is important that the actions being taken by IoT technology are actually intended by its users. Of further importance are the algorithms being used as part of the IoT: profiling algorithms may be blind towards the special needs of individuals and therefore assurance is needed that they are morally proper.

Allow for informed consent

The principle of informed consent is already of high importance when it comes to privacy in contemporary information technology. Due to the complexity that the IoT will bring with it and its purpose to act invisibly on behalf of the user, it will be even more important in this context. One way to ensure this is the option to make the otherwise invisible IoT technology visible for inspection purposes.

Policy Recommendations

In order to achieve the objectives explained in the previous chapter, the following policy recommendations should be considered:

Transparency - Vendor Regulation and Certification

A key element in achieving several of the aforementioned objectives is the openness of IoT technology vendors about the functioning of their products. Closed systems whose internal functioning is neither accessible to experts nor the regular user will lead to the undesired situations as explained earlier.

Regulating to which degree and in what form vendors have to be open about the internal functioning of their systems, may be a way to avoid a knowledge divide, establish trust in the systems and help to achieve intentionality of delegated actions. A particular focus should thereby be on the issue of data profiling.

In addition to pure regulation, the establishment of a certification system can be a valuable building block to achieve these objectives. A certificate that covers relevant values (e.g. user privacy, user autonomy, system security or system reliability) would help to establish trust of people in the objects surrounding them. Such a certification process should also cover particular elements such as the prevention of blindness of profiling algorithms, the possibility to make objects visible for inspection, the openness of the vendor about the internal functioning or the usability of security management mechanisms.

Vendors of IoT technology might see closed systems as a competitive advantage. It is therefore questionable whether the objectives will be achieved if no intervention takes place. A certification system might be, once it is established, a competitive advantage, but the development of such certification should be led by an independent party ensuring that all requirements with respect to transparency are being taken into account. A binding regulation which defines transparency criteria with an additional certification system therefore seems to be the most effective option.

Transparency – Public Information

Orthogonal to the need for transparency with respect to particular industry products is the understanding of IoT technology in its broader form.

In order to ensure that metaphors used for the IoT are adequate, a monitoring process should be established. Evaluation results should be publicly available and summarized in an easily understandable form.

To address the problem of a knowledge divide, it should furthermore be ensured that easily comprehensible information on the overall working of the IoT is available and reaches out all citizens. This action might be performed by an independent organization or an industry consortium.

The industry might see the proper implementation of such mechanisms as a non-necessary additional burden. It is therefore advisable to initiate and monitor the proper execution through a

co-regulation process. Assigning these tasks to an industry-independent organization is, however, also an option.

Research

Similar to IoT technology in itself, its embedding in a societal context is still unclear and under research. In order to meet some of the objectives it is therefore reasonable to suggest that research on particular issues should be encouraged with purposeful programs.

Further research would actually help to achieve the objectives corresponding to all of the identified key issues. In particular, research on the use of reputation systems in the context of IoT could help to establish trust between people and objects, the development of classification schemes could help to assess the moral qualities of pre-established algorithms and the development of an ontology framing the issues surrounding IoT could help to ensure the adequateness of IoT metaphors. Furthermore, alternatives for those who voluntarily opt out of the IoT have to be studied and developed.

Research on the societal aspects of IoT can be stimulated most adequately through the existing research funding organizations, on a European level through the according Framework Programmes. Although the industry is investing in research efforts within the field of IoT, it seems advisable to provide industry-independent research funding for aspects industry isn't as interested in.

Regulating access

Even though a digital divide with respect to the use of IoT is not an issue right now, it is foreseeable that this issue will become a problem over the medium term. Once the use of IoT technology reaches a sufficient state, it might therefore be necessary to regulate access to the IoT in a way that allows every citizen access to it.

Similar to the current efforts being taken to provide broadband access to the Internet for the whole European population (broadband initiative), it might be meaningful to carry out similar efforts for the access to IoT technology. In order to avoid a digital divide between EU member states, it is of importance to carry out these efforts at a European level.

Public debate and continuous citizen oversight

The ethical analysis that has been performed as part of this report revealed that a number of ethical issues might arise due to the introduction and widespread use of IoT technology. Many of the developments that are about to come will reshape parts of our society and change the way we interact and make use of technology. In that context, a debate on the future values of living is necessary.

Although this is hard to initiate in terms of a policy, it seems crucial that such a debate takes place alongside with the introduction of technology. The issues arising from the way how social networks reshape human interaction show the need for such a debate. However, in the case of social networks, such debates only take place as a downstream process after individual company's already reshaped society through their technical products.

Anticipation of possible unintended, unintentional and implausible effects of the IoT in society and the associated debate on responsibility and accountability for potential negative effects need to be participated by all concerned, above all by the European citizenry. The ethical debates should not remain confined to corporate initiative.